Lambda dual

Alberto Angurel

17th December 2025

Contents

0.1 Galois cohomology

0.1.1 Local Galois cohomology

Let R be a complete, noetherian, local principal ring with finite residue field of characteristic $p > 2$ and let $\mathfrak{m}$ denote its maximal ideal.[1] Let T be a free R-module of finite rank with an R-linear continuous action of the absolute Galois group $G_{\mathbb{Q}}$ of the rational numbers. We will denote the Cartier dual of T by $T^* = \operatorname{Hom}(T, \mu_{p^\infty})$.

For every rational prime ℓ, we fix an inclusion of the algebraic closures $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. This choice determines an inclusion $G_{\mathbb{Q}_\ell} \subset G_{\mathbb{Q}}$. We will consider the Galois cohomology group

$$H^1(\mathbb{Q}_\ell, T) := H^1(G_{\mathbb{Q}_\ell}, T)$$

Let $\mathcal{I}_\ell$ be the inertia subgroup of $G_{\mathbb{Q}_\ell}$, i.e., the absolute Galois group of the maximal unramified extension $\mathbb{Q}_{\ell,\mathrm{ur}}$ of $\mathbb{Q}_\ell$.

Definition 0.1.1. Let ℓ be a prime different form p. The *finite* cohomology subgroup $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) \subset H^1(\mathbb{Q}_\ell, T)$ is the kernel of the restriction map

$$H^1(\mathbb{Q}_\ell, T) \to H^1(\mathcal{I}_\ell, T \otimes \mathbb{Q}_p)$$

We will also denote

$$H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T) \cong H^1(\mathbb{Q}_\ell, T)/H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T)$$

Proposition 0.1.2. ([Rub00, lemma 1.3.5]) If T is unramified at $\ell \neq p$, then

$$H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) = H^1(\mathbb{Q}_{\ell,ur}/\mathbb{Q}_\ell, T^{G_{\mathbb{Q}_{\ell,\mathrm{ur}}}}) = \ker\left(H^1(\mathbb{Q}_\ell, T) \to H^1(\mathcal{I}_\ell, T)\right)$$

For certain primes, the finite cohomology group helps to describe the whole cohomology group.

Definition 0.1.3. Fix a natural number $k \in \mathbb{N}$. Let $\mathcal{P}_k$ be the set of prime numbers ℓ satisfying the following assumptions:

- (P1) $\ell \equiv 1 \mod p^k$.
- (P2) $T/(\mathfrak{m}^k, \mathrm{Frob}_\ell - 1)T$ is a free $R/\mathfrak{m}^k$-module of rank 1, where Frob_ℓ is te¡he arithmetic Frobenius at ℓ.

The set of square-free products of primes in $\mathcal{P}_k$ will be denoted by $\mathcal{N}_k = \mathcal{N}(\mathcal{P}_k)$. For every $n \in \mathcal{N}_k$, we write $\nu(n)$ for the number ofx primes dividing n.

In order to make the computations of the primes $\mathcal{P}_k$ in the particular example described in §**??**, it is interesting to define $\mathcal{P}_k$ relative to an extension $F/\mathbb{Q}$.

Definition 0.1.4. Let $k \in \mathbb{N}$ be a natural number and let $F/\mathbb{Q}$ be a Galois extension. Define $\mathcal{P}_{k,F}$ as the subset of primes ℓ in $\mathcal{P}_k$ such that

- (P3) ℓ splits completely in $F/\mathbb{Q}$.

[1] Some results are valid only when R is artinian. In those cases, we will state the result for $R/\mathfrak{m}^k$ for some positive integer k.

Remark 0.1.5. Let L be the field associated to the kernel of the map $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p^k])$. By the Chebotarev density theorem, if $\mathcal{P}_k$ is non-empty and $L \cap F = \mathbb{Q}$, then $\mathcal{P}_{k,F}$ is an infinite set.

Lemma 0.1.6. ([MR04, lemma 1.2.1]) Assume ℓ satisfies (P1) and denote by $\mathcal{G}_\ell$ the p-primary part of the Galois group of $\mathbb{Q}(\mu_\ell)/\mathbb{Q}$, where μ_ℓ is the set of ℓ^{th} roots of unity. Then there are canonical functorial isomorphisms:

- $H^1_{\text{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k) \cong T/(\mathfrak{m}^k, \mathrm{Frob}_\ell - 1)T$.
- $H^1_{\text{s}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k) \otimes \mathcal{G}_\ell \cong (T/\mathfrak{m}^k T)^{\mathrm{Frob}_\ell = 1}$.

For every prime ℓ in $\mathcal{P}_k$, it is possible to define the finite-singular map ϕ^{fs}_ℓ as follows. Consider the polynomial

$$P_\ell(x) := \det(1 - \mathrm{Frob}_\ell\, x | T/\mathfrak{m}^k) \in R/\mathfrak{m}^k[x]$$

Assume $P_\ell(1) = 0$. Then there is a unique polynomial $Q(x) \in R/\mathfrak{m}^k[x]$ such that $P_\ell(x) = (x-1)Q(x)$. By the Cayley-Hamilton theorem, $P_\ell(\mathrm{Frob}_\ell^{-1})$ annihilates $T/\mathfrak{m}^k T$, so $Q(\mathrm{Frob}_\ell^{-1})T/\mathfrak{m}^k \subset (T/\mathfrak{m}^k T)^{\mathrm{Frob}_\ell = 1}$. Hence we can define the map ϕ^{fs}_ℓ as the composition

$$\begin{tikzcd} H^1_{\text{f}}\left(\mathbb{Q}_\ell, \frac{T}{\mathfrak{m}^k T}\right) \arrow[r, "\sim"] & \frac{T}{(\mathfrak{m}^k, \mathrm{Frob}_\ell - 1)T} \arrow[r, "Q(\mathrm{Frob}_\ell^{-1})"] & \left(\frac{T}{\mathfrak{m}^k T}\right)^{\mathrm{Frob}_\ell = 1} \arrow[r, "\sim"] & H^1_{\text{s}}\left(\mathbb{Q}_\ell, \frac{T}{\mathfrak{m}^k T}\right) \otimes \mathcal{G}_\ell \end{tikzcd}$$

Lemma 0.1.7. ([MR04, lemma 1.2.3]) If $\ell \in \mathcal{P}_k$, then $\det(1 - \mathrm{Frob}_\ell | T/\mathfrak{m}^k) = 0$ and the map ϕ^{fs}_ℓ is an isomorphism.

Another important subgroup of the local Galois cohomology group is the transverse subgroup, which is defined via the cohomological inflation

$$H^1_{\text{tr}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k) = \mathrm{Im}\left(\mathrm{Inf} : H^1(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell, T/\mathfrak{m}^k) \hookrightarrow H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^k)\right)$$

Lemma 0.1.8. ([MR04, lemma 1.2.4]) Assume ℓ satisfies (P1). Then there is a functorial splitting

$$H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^k) = H^1_{\text{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k) \oplus H^1_{\text{tr}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$$

The most important feature about the finite local cohomology is that it behaves well under Tate duality.

Proposition 0.1.9. ([MR04, proposition 1.3.2]) Let ℓ be a finite prime. The cup product induces a perfect pairing

$$H^1(\mathbb{Q}_\ell, T) \times H^1(\mathbb{Q}_\ell, T^*) \to H^2(\mathbb{Q}_\ell, \mu_{p^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

If T is unramified at $\ell \neq p$, then

1. $H^1_{\text{f}}(\mathbb{Q}_\ell, T)$ and $H^1_{\text{f}}(\mathbb{Q}_\ell, T^*)$ are orthogonal complements under this pairing.
2. If ℓ satisfies (P1) for some $k \in \mathbb{N}$, then $H^1_{\text{tr}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$ and $H^1_{\text{tr}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$ are orthogonal complements.

Corollary 0.1.10. Given a prime $\ell \in \mathcal{P}_k$, the finite and singular cohomology groups $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$, $H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T/m^k)$, $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$ and $H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$ are free $R/\mathfrak{m}^k$-modules of rank one.

Proof. By (P2) and lemma 0.1.6, $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$ is free of rank one over $R/\mathfrak{m}^k$. By lemma 0.1.7, the finite-singular map ϕ^{fs}_ℓ is an isomorphism, so $H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T)$ is a rank one free $R/\mathfrak{m}^k$-module too.

Proposition 0.1.9 implies the following:

$$H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k]) \cong H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)^\vee; \qquad H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k]) \cong H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)^\vee.$$

Hence $H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$ and $H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T^*[\mathfrak{m}^k])$ are also free $R/\mathfrak{m}^k$-modules of rank one. □

0.1.2 Selmer structures

An important tool to study the cohomology of the global absolute Galois group is the use of Selmer structures. Assume that T is unramified outside a finite set of primes S, i.e., that for every $\ell \notin S$, the inertia group $\mathcal{I}_\ell$ acts trivially on T.

Definition 0.1.11. A *Selmer structure* $\mathcal{F}$ on T is a collection of the following data

- a finite set $\Sigma(\mathcal{F})$ of places of $\mathbb{Q}$, including ∞, p and all primes where T is ramified.
- for every $\ell \in \Sigma(\mathcal{F})$, an $R[[G_{\mathbb{Q}_\ell}]]$-submodule $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \subset H^1(\mathbb{Q}_\ell, T)$, where $G_{\mathbb{Q}_\ell}$ is the absolute Galois group of $\mathbb{Q}_\ell$. This choice is usually referred to as a *local condition* at the prime ℓ.

Definition 0.1.12. The *Selmer module* $H^1_{\mathcal{F}}(\mathbb{Q}, T) \subset H^1(\mathbb{Q}, T)$ associated to a Selmer structure $\mathcal{F}$ is the kernel of the sum of restriction maps

$$H^1(\mathbb{Q}_{\Sigma(\mathcal{F})}/\mathbb{Q}, T) \to \bigoplus_{\ell \in \Sigma(\mathcal{F})} H^1(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$$

where $\mathbb{Q}_\Sigma(\mathcal{F})$ is the maximal extension of $\mathbb{Q}$ unramified outside $\Sigma(\mathcal{F})$.

Remark 0.1.13. Given a Selmer structure $\mathcal{F}$, we will denote $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T)$ for every prime $\ell \notin \Sigma(\mathcal{F})$.

Definition 0.1.14. Let $\mathcal{F}$ be a Selmer structure defined on T. If $T' \hookrightarrow T$ is an injection, $\mathcal{F}$ induces a Selmer structure where the local conditions $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T')$ are the inverse images of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ under the natural map $H^1(\mathbb{Q}_\ell, T') \to H^1(\mathbb{Q}_\ell, T)$.
If $T \twoheadrightarrow T''$ is a surjection, $\mathcal{F}$ induces a Selmer structure on T'' where the local conditions $H^1(\mathbb{Q}_\ell, T'')$ are the images $H^1(\mathbb{Q}_\ell, T)$ under the map $H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell, T'')$.

Definition 0.1.15. Given a Selmer structure $\mathcal{F}$ on T, there is a dual Selmer structure $\mathcal{F}^*$ on T^* where, for every prime ℓ, the local conditions $H^1_{\mathcal{F}^*}(\mathbb{Q}_\ell, T^*)$ is the orthogonal complement of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ under the pairing defined in proposition 0.1.9. Note $\mathcal{F}^*$ is well defined by proposition 0.1.9

In order to compare Selmer structures, Poitou-Tate global duality is helpful.

Proposition 0.1.16. ([MR04, theorem 2.3.4]) Let $\mathcal{F}$ and $\mathcal{G}$ be Selmer structures of T such that $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \subset H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)$ for every prime ℓ. Then the following sequence is exact.

$$\begin{tikzcd}
0 \arrow[r] & H^1_{\mathcal{F}}(\mathbb{Q},T) \arrow[r] & H^1_{\mathcal{G}}(\mathbb{Q},T) \arrow[r] & \bigoplus_{\ell\in\Sigma(\mathcal{F})\cup\Sigma(\mathcal{G})} \dfrac{H^1_{\mathcal{G}}(\mathbb{Q}_\ell,T)}{H^1_{\mathcal{F}}(\mathbb{Q}_\ell,T)} \arrow[dll, rounded corners] \\
 & H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee \arrow[r] & H^1_{\mathcal{G}^*}(\mathbb{Q},T^*)^\vee \arrow[r] & 0
\end{tikzcd}$$

where the third map is induced by proposition 0.1.9.

In order to compute the structure of a Selmer group, it is helpful to make use of slightly modified Selmer structures.

Definition 0.1.17. Given a Selmer structure $\mathcal{F}$ defined on T and square-free and pairwise relatively prime integers a, b and c, we define a new Selmer structure $\mathcal{F}_a^b(c)$ given by the following data[2]

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

We now define the notion of Selmer triples

Definition 0.1.18. A *Selmer triple* is a triple $(T,\mathcal{F},\mathcal{P})$ where $\mathcal{F}$ is a Selmer structure on T and $\mathcal{P}$ is a set of rational primes disjoint from $\Sigma(\mathcal{F})$.

For technical reasons, we need to assume the following mild hypotheses in our Selmer triples:

- (H0) T is a free R-module of finite rank.
- (H1) $T/\mathfrak{m}T$ is an absolutely irreducible $R/\mathfrak{m}[G_{\mathbb{Q}}]$-representation.
- (H2) $H^1(\mathbb{Q}(T,\mu_{p^\infty})/\mathbb{Q},T/\mathfrak{m}T) = H^1(\mathbb{Q}(T,\mu_{p^\infty})/\mathbb{Q},T^*[\mathfrak{m}]) = 0$, where $\mathbb{Q}(T,\mu_{p^\infty})$ is the minimal extension of $\mathbb{Q}$ whose Galois group acts trivially on T, T^* and μ_{p^∞}.
- (H3) There is a $\tau \in G_{\mathbb{Q}}$ such that $\tau = 1$ on μ_{p^∞} and $T/(\tau-1)T$ is free of rank one over R.
- (H4) Either
  - (H4a) $\mathrm{Hom}_{\mathbb{F}_p[G_{\mathbb{Q}}]}(T/\mathfrak{m}T, T^*[\mathfrak{m}]) = 0$ or
  - (H4b) $p \geq 5$.
- (H5) There is a prime q such that $H^1_{\mathrm{s}}(\mathbb{Q}_q,T) \cong R$ and $H^2(\mathbb{Q}_q,T) = 0$.
- (H6) For every $\ell \in \Sigma(\mathcal{F})$, the local condition of $\mathcal{F}$ at ℓ is cartesian in the category of quotients of T, in the sense of [MR04, definition 1.1.4].

[2] If any of a, b or c is not explicitly written, we will assume it to be one.

- (H7) The core rank $\chi(\mathcal{F})$ is zero (see theorem 0.1.25), i.e., for every $n \in \mathcal{N}(\mathcal{P})$ and $j \in \mathbb{Z}_{\geq 0}$ there is a non-canonical isomorphism
$$H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^j) \cong H^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^j])$$

- (H8) There exists some $k \in \mathbb{N}$ and some Galois extension $F/\mathbb{Q}$ such that $F \cap \mathbb{Q}(T/p^k) = \mathbb{Q}$ and $(\mathcal{P}_{k,F} \setminus \Sigma(\mathcal{F})) \subset \mathcal{P} \subset \mathcal{P}_1$.

Remark 0.1.19. ([MR04, remark 3.5.1]) Suppose that $(T, \mathcal{F}, \mathcal{P})$ satisfies hypotheses (H0)-(H8). Then $(T/\mathfrak{m}^k, \mathcal{F}, \mathcal{P})$ also satisfies (H0)-(H8) for every $k \in \mathbb{Z}_{\geq}0$.

All of the above hypothesis except for (H5) and (H7) were imposed by Mazur and Rubin in [MR04, §3.5] to develop the basic theory of Kolyvagin systems when $\chi(\mathcal{F}) = 1$.

(H1), (H2) and (H6) are necessary to ensure that the Selmer group in the cohomology with torsion coefficient rings $H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^j)$ (resp. $H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^j])$) coincides with the $\mathfrak{m}^j$-torsion of the full Selmer group $H^1_{\mathcal{F}}(\mathbb{Q}, T)$ (resp. $H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)$). This is explained in the following lemmas.

Lemma 0.1.20. ([MR04, lemma 3.5.3]) Assume that (H1) and (H2) hold. For every $j \in \mathbb{Z}_{\geq 0}$, the inclusion $T^*[\mathfrak{m}^j] \hookrightarrow T$ induces an isomorphism:
$$H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^j]) \cong H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)[\mathfrak{m}^j]$$

Lemma 0.1.21. ([MR04, lemma 3.5.4]) Assume further that R is artinian of length k and that (H1), (H2) and (H6) hold. If π be a generator of $\mathfrak{m}$, the multiplication by π^{k-j} induces a map $T/\mathfrak{m}^j \hookrightarrow T$, which in turn induces an isomorphism in the cohomology groups:
$$H^1_{\mathcal{F}^*}(\mathbb{Q}, T/\mathfrak{m}^j) \cong H^1_{\mathcal{F}^*}(\mathbb{Q}, T)[\mathfrak{m}^j]$$

(H3), (H4) and (H8) are required to ensure there exists infinitely many Kolyvagin primes satisfying (P1) and (P2) that bound the Selmer group appropriately. Assumption (H8) is slightly weaker than the corresponding hypothesis in [MR04]. It does not suppose any inconvenience in the proofs of this reference and permits a cleaner description of the Kolyvagin primes in the example in §**??**.

(H7) is imposed because we want to generalise the theory in [MR04] to the case of core rank 0. However, those Selmer structures do not admit any non-trivial Kolyvagin systems. Therefore, (H5) is required to modify the structure in order to link it with a Selmer structure of rank one, $\mathcal{F}_q$, which the theory in [MR04] can be applied to. Note that, by local Tate duality, the condition $H^2(\mathbb{Q}_q, T)$ is equivalent to $H^0(\mathbb{Q}_q, T^*) = 0$.

Assumption (H5) can be understood in terms of the cohomology groups with torsion coefficients. The long exact sequence implies the following lemma.

Lemma 0.1.22. Assume that a prime q satisfies (H5). Then for every $j \in \mathbb{Z}_{\geq 0}$ there is an isomorphism
$$H^1_{\mathrm{s}}(\mathbb{Q}_q, T/\mathfrak{m}^j) \cong R/\mathfrak{m}^j$$

Proof. Since $H^2(\mathbb{Q}_q, T) = 0$, the long exact sequence induces an isomorphism

$$H^1(\mathbb{Q}_q, T)/\mathfrak{m}^j H^1(\mathbb{Q}_q, T) \xrightarrow{\sim} H^1(\mathbb{Q}_q, T/\mathfrak{m}^j T)$$

Since $H^1_{\mathrm{f}}(\mathbb{Q}_q, T/\mathfrak{m}^j T)$ is the image of $H^1_{\mathrm{f}}(\mathbb{Q}_q, T)$, we get that

$$H^1_{\mathrm{s}}(\mathbb{Q}_q, T/\mathfrak{m}^j T) \cong H^1_{\mathrm{s}}(\mathbb{Q}_q, T)/\mathfrak{m}^j H^1_{\mathrm{s}}(\mathbb{Q}_q, T) \cong R/\mathfrak{m}^j$$

□

Some elements in $\mathcal{N}(\mathcal{P})$ will play an important role in the theory of Kolyvagin systems.

Definition 0.1.23. 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 0.1.24. ([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 $n|m$.

The concept of core rank plays a vital role in the study of Selmer structures.

Theorem 0.1.25. ([MR04, theorem 4.1.5]) There exists some $x, y \in \mathbb{Z}_{\geq 0}$, one of which can be taken to be 0, such that for every $n \in \mathcal{N}(\mathcal{P})$ and every $j \in \mathbb{Z}_{\geq 0}$ there is a non-canonical isomorphism

$$H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^j) \oplus (R/\mathfrak{m}^j)^x \approx H^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^j]) \oplus (R/\mathfrak{m}^j)^y$$

The integer $\chi(T, \mathcal{F}) = y - x$ is said to be the *core rank* of $\mathcal{F}$.

Proposition 0.1.26. ([Sak18, corollary 3.21]) Let $(T, \mathcal{F}, \mathcal{P})$ be a Selmer triple and let $a, b, c \in \mathcal{N}_k$ be pairwise relatively prime. Then

$$\chi(T/\mathfrak{m}^k, \mathcal{F}^b_a(c)) = \chi(T/\mathfrak{m}^k, \mathcal{F}) + \nu(b) - \nu(a)$$

Remark 0.1.27. Proposition 0.1.26 is also true when $a, b \in \mathcal{N}(\mathcal{P}')$, where $\mathcal{P}'$ denotes the set of primes ℓ such that $H^1_{\mathrm{s}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)$ is free of rank one over $R/\mathfrak{m}^k$.

The key idea of this work is that we can bound the Selmer group by using appropriate primes, whose existence is known due to the Chebotarev density theorem. To be precise, we will now state the result needed.

Proposition 0.1.28. ([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 0.1.29. Let $(T, \mathcal{F}, \mathcal{P})$ be a Selmer triple satisfying (H0)-(H8) 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 0.1.20 and 0.1.21, 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 0.1.28 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 0.1.10, $H^1_f(\mathbb{Q}_\ell,T/\mathfrak{m}^j)$ 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 0.1.30. ([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

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

The above two results imply the following

Corollary 0.1.31. ([MR04, proposition 4.5.8]) Assume that $\chi(\mathcal{F})>0$ and that $H^1_{\mathcal{F}^*}(\mathbb{Q},T^*[\mathfrak{m}^k])\approx R/\mathfrak{m}^{e_1}\times\cdots\times R/\mathfrak{m}^{e_s}$ for some integers $e_1\geq e_2\geq\ldots\geq e_s$. Then there are infinitely many primes ℓ such that

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

However, the above lemma is only useful when $\chi(\mathcal{F})\geq 0$ because we can generate, due to Chebotarev density theorem, primes ℓ such that $\mathrm{loc}^{\mathrm{f}}_\ell$ is surjective. In the case $\chi(\mathcal{F})=0$, those primes might not exist but we can still get the following partial result.

Lemma 0.1.32. Assume that $\chi(\mathcal{F})=0$ and that $H^1_{\mathcal{F}^*}(\mathbb{Q},T^*[\mathfrak{m}^k])\cong R/\mathfrak{m}^{e_1}\times\cdots\times R/\mathfrak{m}^{e_s}$ for some integers $e_1\geq e_2\geq\ldots\geq e_s$. Then there are infinitely many primes $\ell\in\mathcal{P}_k$ such that

$$H^1_{\mathcal{F}^*(\ell)}(\mathbb{Q},T^*[\mathfrak{m}^k])\approx R/\mathfrak{m}^j\times R/\mathfrak{m}^{e_3}\times\cdots\times R/\mathfrak{m}^{e_s}$$

where $e_2\leq j\leq k$. In the case when $e_1>e_2$, then $j=e_2$ holds true for infinitely many primes $\ell\in\mathcal{P}_k$.

Proof. Since $\chi(\mathcal{F}) = 0$,

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

Applying proposition 0.1.28 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 $c_3 \in \mathfrak{m}^{e_1-1}H^1_{\mathcal{F}^*}(\mathbb{Q}, T[\mathfrak{m}^{e_1}]^*)$, we can find infinitely many primes $\ell \in \mathcal{P}_k \subset \mathcal{P}_{e_1}$ such that the localisation maps

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

are surjective. Since $\ell \in \mathcal{P}_{e_1}$, 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 corollary 0.1.10.

By lemma 0.1.30,

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

By lemma 0.1.20,

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

Since $\chi(\mathcal{F}^\ell) = 1$ by proposition 0.1.26, then theorem 0.1.25 implies that

$$H^1_{\mathcal{F}^*(\ell)}(\mathbb{Q}, T^*[\mathfrak{m}^k]) \approx H^1_{\mathcal{F}(\ell)}(\mathbb{Q}, T/\mathfrak{m}^k) \subset H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T/\mathfrak{m}^k) \approx R/\mathfrak{m}^k \oplus H^1_{\mathcal{F}^*_\ell}(\mathbb{Q}, T^*[\mathfrak{m}^k])$$

Therefore, $H^1_{\mathcal{F}^*(\ell)}(\mathbb{Q}, T^*[\mathfrak{m}^k])$ is an $R/\mathfrak{m}^k$-module which can be injected into $R/\mathfrak{m}^k \times R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$ and whose $\mathfrak{m}^{e_1}$-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. □

Given a Galois representation T defined over a discrete valuation ring $\mathcal{O}$, there are some natural Selmer structures that can be defined on T. The first example is called the *canonical Selmer structure.* The finite cohomology group is a well behaved local condition for primes different from p and ∞. The idea behind the canonical example is to consider the local conditions at those primes to be the whole local cohomology groups.

Definition 0.1.33. Let T be a Galois representation over a discrete valuation ring of residual characteristic $p > 0$. Then the canonical local conditions are defined as

$$\begin{cases} H^1_{\mathcal{F}^{\mathrm{can}}}(\mathbb{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) & \text{if } \ell \neq p \\ H^1_{\mathcal{F}^{\mathrm{can}}}(\mathbb{Q}_p, T) = H^1(\mathbb{Q}_p, T) \\ H^1_{\mathcal{F}^{\mathrm{can}}}(\mathbb{R}, T) = H^1(\mathbb{R}, T) \end{cases}$$

The canonical structure is the one that can be studied directly by using Euler systems. However, it is usually different to the Selmer groups that appear naturally in artihmetic geometry, because they differ in the local conditions at p and ∞. The infinite prime is usually not an issue since $H^1(\mathbb{R}, T) = 0$ when $p > 2$. At p, S. Bloch and K. Kato gave in [BK90] a definition of a local condition at p, based purely on the Galois representation T. In the most arithmetically important cases, it coincides the local condition at p defined geometrically. Their definition uses Fontaine's period rings from p-adic Hodge theory. Moreover, Bloch-Kato Selmer group is conjecturally directly related to the special values of the motivic L-function.

Definition 0.1.34. Let T be a Galois representation over a local ring of residual characteristic $p > 0$. Then the Bloch-Kato local conditions are defined as

$$\begin{cases} H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) \ \text{ if } \ell \neq p \\ H^1_{\mathcal{F}_{\mathrm{BK}}}(\mathbb{Q}_p, T) = \ker\big(H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell, T \otimes_{\mathbb{Z}_p} B_{\mathrm{crys}})\big) \end{cases}$$

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

Notation 1.1.3. 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

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

Define Cartier dual

We assume the following assumptions:

Assumption 1.1.4. 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) $H^1(K(T)_M/K, T) = H^1(K(T)_M/K, T^*(1)) = 0$.

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

Definition 1.1.5. 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 1.1.6. 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 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 1.1.7. (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 infration restriction sequence.

Definition 1.1.8. Let ℓ be a finite place of K as in Definition 1.1.7. 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 1.1.9. ([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 exists 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 1.1.10. 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]:

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

Notation 1.1.11. 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 fixes an isomorphism $H^1_s(K_\ell, T)$.

Definition 1.1.12. Let $\ell \in \mathcal{P}$. The transverse cohomology sugbgroup is defined as

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

Proposition 1.1.13. ([MR04, Lemma 1.2.4]) $H^1_{\mathrm{tr}}(K_\ell, T)$ is the image of the canonical splitting in Equation (1.1).

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 prime 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

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

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 $\Sigma(\mathcal{F})$.

In order to compare Selmer structures, Poitou-Tate global duality is helpful.

Proposition 1.2.4. ([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 0.1.9, is exact.

$$\begin{tikzcd}
H^1_{\mathcal{F}}(K,T) \arrow[r, tail] & H^1_{\mathcal{G}}(K,T) \arrow[r] & \displaystyle\bigoplus_{\ell\in\Sigma_{\mathcal{F}}\cup\Sigma_{\mathcal{G}}} \frac{H^1_{\mathcal{G}}(K_\ell,T)}{H^1_{\mathcal{F}}(K_\ell,T)} \arrow[r] & H^1_{\mathcal{G}}(K,T^*)^\vee \arrow[r, two heads] & H^1_{\mathcal{F}}(K,T^*)^\vee
\end{tikzcd}$$

local duality and dual Selmer structures.

Notation 1.2.5. Let $\mathcal{F}$ and $\mathcal{G}$ be Selmer structures. We say $\mathcal{F} \leq \mathcal{G}$ if $H^1_{\mathcal{F}}(K_\ell,T) \subset H^1_{\mathcal{G}}(K_\ell,T)$ for all places ℓ.

Local conditions propagates naturally to submodules and quotients of T.

Definition 1.2.6. (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 1.2.7. (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 1.2.8. 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.

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

Definition 1.2.9. (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 1.2.10. It is enough to check the cartesian condition for $\ell \in \Sigma(\mathcal{F})$. Indeed, if $H^1_{\mathcal{F}}(K_q, T) = H^1_{\mathrm{f}}(K_q, T)$, then $H^1_{\mathrm{s}}(K_q, T) = \mathrm{Hom}(\mathcal{I}_q, T^{\mathrm{Frob}_\ell = 1})$. Then the cartesian condition holds for q because Hom is a left exact functor.

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

Definition 1.2.11. (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 1.2.12. We will assume $\chi(\mathcal{F})$ is non-negative. Otherwise, one could swap the roles of F^* and T^* since $\chi(\mathcal{F}^*) = -\chi(\mathcal{F})$.

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 1.2.13. 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

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

1.3 Classical Kolyvagin systems

Fix the canonical homomorphism for the local cohomology

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 1.3.1. 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 1.3.2. 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

$$\mathrm{loc}_\ell(\kappa_{n\ell}) = \phi_\ell^{\mathrm{fs}} \circ \mathrm{loc}_\ell(\kappa_n) \tag{1.2}$$

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

Modified Selmer structures and finite-singular map

Remark 1.3.3. 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.

dual M^+

Definition 1.3.4. 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 1.3.5. 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 1.3.6. 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 1.3.7. 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 1.3.8. ([MR04, Theorem 4.3.3]) Under Assumption 1.3.1, $\mathrm{KS}(\mathcal{F})$ is a free, cyclic R-module.

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

Definition 1.3.9. 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 1.3.10. ([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

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

Introduce Fitting ideals

The proof of Theorem 1.3.10 is divided in the following two lemmas:

Lemma 1.3.11. Under Assumption 1.3.1, 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 1.3.12. Under Assumption 1.3.1, then

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

1.4 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 1.4.1. ([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 1.4.2. 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

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

Proof. By Proposition 1.2.4, there is an global-duality exact sequence for $\overline{T} := T \otimes k$

$$\begin{tikzcd}
H^1_{\mathcal{F}}(K, \overline{T}) \arrow[r, tail] & H^1_{\mathcal{G}}(K, \overline{T}) \arrow[r] & \displaystyle\bigoplus_{q \in \Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}} \frac{H^1_{\mathcal{G}}(K_q, \overline{T})}{H^1_{\mathcal{F}}(K_q, \overline{T})} \arrow[r] & H^1_{\mathcal{G}}(K, \overline{T}^*)^\vee \arrow[r, two heads] & H^1_{\mathcal{F}}(K, \overline{T}^*)^\vee
\end{tikzcd}$$

Since $\chi(\mathcal{F}) = 0$ and $\chi(\mathcal{G}) = 1$, Definition 1.2.11 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 1.4.3. 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 1.4.4. 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 1.4.5. 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 1.4.6. 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

$$\Theta_i^{(0)}(\kappa, \mathcal{F}) \subset \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}}(K, T)\big) \tag{1.3}$$

Moreover, if one of the following conditions is satisfied

(i) $i = \mathrm{rank}_R(H^1_{\mathcal{F}}(K,T)) =: r$

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

(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 $\Theta_i^{(0)}(\kappa, \mathcal{F}) = \mathrm{Fitt}_i^R\big(H^1_{\mathcal{F}}(\mathbb{Q}, T)\big)$.

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

Lemma 1.4.7. If $\kappa \in \mathrm{KS}(\mathcal{G})$ is a primitive Kolyvagin system and $n \in \mathcal{N}$, then

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

Lemma 1.4.8. If $\mathcal{F}$ is a cartesian

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

lemma for equality

1.4.1 Proof of Lemma 1.4.7

The proof of Lemma 1.4.7 involves comparing the indices of κ_n and δ_n, so we can then apply Lemma 1.3.11.

Lemma 1.4.9. 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 $\mathrm{ind}(\delta_n) = \mathrm{ind}(\kappa_n) \cdot \mathrm{Fitt}^{(0)}(\kappa_n)$.

Proof. Note that cite there is a non-canonical isomorphism

$$H^1_{\mathcal{G}}(K,T) \approx R \oplus H^1_{\mathcal{F}^*}(K, T^*) \tag{1.4}$$

Let (x_n, y_n) be the components of κ_n under this identification. Since $\mathrm{ind}(\kappa_n) = \mathrm{Fitt}_0^R\big(H^1_{\mathcal{F}^*}(K, T^*)\big)$, then $y_n = 0$ and x_n is a generator of $\mathrm{ind}(\kappa_n)$. The decomposition in (1.4) induces a map in R^+ defined by

$$\begin{tikzcd} R \arrow[r] & H^1_{\mathcal{G}}(K,T) \arrow[r, "\mathrm{loc}_\ell"] & H^1_{\mathcal{G}/\mathcal{F}}(K_\ell, T) \arrow[r, "\cong"] & R \end{tikzcd}$$

Let $a \in R$ be the image of one under this map, which coincides with $\mathrm{Fitt}^0(C_n)$. Therefore,

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

local coh. free of rk 1 □

Proof of Lemma 1.4.7. The exact sequence in Proposition 1.2.4 induces a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & C_n \arrow[r] & H^1_{\mathcal{F}^*(n)}(K,T) \arrow[r] & H^1_{\mathcal{G}^*(n)}(K,T) \arrow[r] & 0 \end{tikzcd}$$

We then have the identity of Fitting ideals

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

where the second inequality follows from Lemma 1.3.11 and the last one from Lemma 1.4.9. □

1.5 Old stuff

In the rest of the section, we state some lemmas from [Kim25, §5.2]. However, the convention of orders in that article is slightly different and the proofs are trickier in our case. For the sake of completeness, we also include them here.

Lemma 1.5.1. ([Kim25, proposition 5.2]) For every $n \in \mathcal{N}$, let

$$C_n := \mathrm{coker}\left(\mathrm{loc}_q^s : H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n}) \to H^1_{\mathrm{s}}(\mathbb{Q}_q, T/\mathfrak{m}^{k_n}) \cong R/\mathfrak{m}^{k_n}\right)$$

If $\mathrm{ord}(\kappa_n) + \mathrm{length}(C_n) < k_n$, then

$$\mathrm{ord}(\kappa_n) + \mathrm{length}(C_n) = \mathrm{ord}(\delta_n)$$

Otherwise, $\mathrm{ord}(\delta_n)$ is infinite, i.e., $\delta_n = 0$.

Proof. Since $\chi(\mathcal{F}^q) = 1$, we have a non-canonical isomorphism

$$H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n}) \approx R/\mathfrak{m}^{k_n} \oplus H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}]) \tag{1.5}$$

Hence we can find an element $z \in H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})$ and a submodule A isomorphic to $H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])$ such that

$$H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n}) = (R/\mathfrak{m}^{k_n})\,z \oplus A$$

By theorem **??**,

$$\mathrm{ord}(\kappa_n) \geq \mathrm{length}\big(H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\big) \tag{1.6}$$

so $\kappa_n \in (R/\mathfrak{m}^{k_n})\,z$. In particular, there is some unit $u \in R^\times$ such that

$$\kappa_n = up^{\mathrm{ord}(\kappa_n)}z \tag{1.7}$$

Assume first that $\mathrm{loc}_q^s(\kappa_n) = \delta_n \neq 0$. Then

$$\mathrm{length}\Big(\mathrm{loc}_q^s\big(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\big)\Big) \geq \mathrm{length}\big(H^1_{\mathcal{F}_q^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\big)$$

Since $H^1_s(\mathbb{Q}_q, T/\mathfrak{m}^{k_n})$ is isomorphic to $R/\mathfrak{m}^{k_n}$ by lemma 0.1.22, the above implies that

$$\mathrm{loc}_q^s\left(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right) = (R/\mathfrak{m}^{k_n})\mathrm{loc}_q^s(z)$$

By equation 1.7,

$$p^{\mathrm{ord}(\kappa_n)}\mathrm{loc}_q^s\left(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right) = (R/\mathfrak{m}^{k_n})\delta_n$$

Since $H^1_s(\mathbb{Q}_q, T/\mathfrak{m}^{k_n})$ is a cyclic $R/\mathfrak{m}^{k_n}$-module, the following equality holds true:

$$\mathrm{length}\left(\mathrm{loc}_q^s(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n}))\right) - \mathrm{ord}(\kappa_n) = k_n - \mathrm{ord}(\delta_n)$$

Since $\mathrm{length}(C_n) = k_n - \mathrm{length}\left(\mathrm{loc}_q^s(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n}))\right)$, then

$$\mathrm{ord}(\kappa_n) + \mathrm{length}(C_n) = \mathrm{ord}(\delta_n)$$

Now assume that $\delta_n = 0$. It means that $\mathrm{loc}_q^s(\kappa_n) = 0$. Using (1.7),

$$\mathrm{length}\Big(R/\mathfrak{m}^{k_n}\mathrm{loc}_q^s(z)\Big) \leq \mathrm{ord}(\kappa_n)$$

Note that

$$\begin{gathered}\mathrm{length}\left(\mathrm{loc}_q^s\left(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right)\right) = \\ \max\Big\{\mathrm{length}\Big(R/\mathfrak{m}^{k_n}\mathrm{loc}_q^s(z)\Big), \mathrm{length}\Big(\mathrm{loc}_q^s\big(H^1_{\mathcal{F}_q^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\big)\Big)\Big\}\end{gathered}$$

Hence by (1.6),

$$\mathrm{length}\left(\mathrm{loc}_q^s\left(H^1_{\mathcal{F}^q(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right)\right) \leq \mathrm{ord}(\kappa_n)$$

Therefore,

$$\mathrm{ord}(\kappa_n) + \mathrm{length}(C_n) \geq k_n$$

□

Lemma 1.5.2. ([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 0.1.9, for every $n \in \mathcal{N}$ there is an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}_q^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}]) \longrightarrow H^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}]) \longrightarrow C_n^\vee \longrightarrow 0 \tag{1.8}$$

By proposition 0.1.24, there is some $n_0 \in \mathcal{N}$ such that

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

By lemma 0.1.20,

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

Therefore, (1.8) implies that $C_{n_0} = 0$. Moreover, by lemma 1.5.1 and theorem **??**, $\mathrm{ord}(\delta_{n_0}) = \mathrm{ord}(\kappa_{n_0}) = 0$.

□

Lemma 1.5.3. Assume $\kappa \in \mathrm{KS}(T, \mathcal{F}, \mathcal{P})$ is a primitive Kolyvagin system. For every $n \in \mathcal{N}$, we have that

$$\mathrm{ord}(\delta_n) = \mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n}))$$

if the latter is less than k_n. Otherwise, $\mathrm{ord}(\delta_n) = \infty$.

Proof. Since $\chi(\mathcal{F}) = 0$, (1.8) implies thatx

$$\begin{aligned} \mathrm{length}\left(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right) = \mathrm{length}\left(H^1_{\mathcal{F}^*(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\right) = \\ \mathrm{length}\left(H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\right) + \mathrm{length}(C_n) = \kappa_n + \mathrm{length}(C_n) \end{aligned} \tag{1.9}$$

If $\mathrm{length}\left(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right) < k_n$, then lemma 1.5.1 implies that

$$\mathrm{length}\left(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})\right) = \mathrm{length}\left(H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\right) - \mathrm{ord}(\kappa_n) + \mathrm{ord}(\delta_n)$$

By theorem **??**

$$\mathrm{length}\left(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k})\right) = \mathrm{ord}(\delta_n)$$

Assume now that $\mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbb{Q}, T/\mathfrak{m}^{k_n})) \geq k_n$. By theorem **??** and (1.9),

$$\mathrm{ord}(\kappa_n) + \mathrm{length}(C_n) = \mathrm{length}\left(H^1_{\mathcal{F}^*_q(n)}(\mathbb{Q}, T^*[\mathfrak{m}^{k_n}])\right) + \mathrm{length}(C_n) \geq k_n$$

By the second part of lemma 1.5.1, $\mathrm{ord}(\delta_n) = \infty$. □

1.5.1 Fitting ideals of Selmer groups of core rank zero

Throughout this section, the concept of rank of a finitely generated module will play a role. With the aim of avoiding confusion, specially when R is artinian, we clarify this concept in the following definition.

Definition 1.5.4. Let M be an R-module. We define the rank of M as the maximium number of linearly independent elements in M. In case that R is local, principal and artinian of lenght k, this quantity coincides with the following:

$$\mathrm{rank}_R(M) = \dim_{R/\mathfrak{m}} \mathfrak{m}^{k-1}M$$

The main purpose of this section is to prove the following theorem.

Theorem 1.5.5. Assume R is a discrete valuation ring. For every $i \in \mathbb{Z}_{\geq 0}$, we have that

$$\Theta_i(\kappa) \subset \mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right) \tag{1.10}$$

where $\Theta_i(\kappa)$ was defined in definition **??**. Moreover, if one of the following conditions is satisfied

(i) $i = \mathrm{rank}_R(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee) =: r$

(ii) $\Theta_{i-1}(\kappa) \subsetneq \mathrm{Fitt}_{i-1}^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right)$

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

Remark 1.5.6. 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 1.5.5 determines the Fitting ideals of the dual Selmer group

Corollary 1.5.7. 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 1.5.5 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}:

$$m_i \leq \frac{m_{i+1} + m_{i-1}}{2} \tag{1.11}$$

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 1.5.5 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 1.5.5, would imply that $n_i = m_i$, contradicting our assumption. Therefore, $n_{i-1} = m_{i-1}$. Moreover, condition (iii) in theorem 1.5.5 cannot be satisfied since, otherwise, our assumption would not be true. Hence, the equality holds in equation (1.11) 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 1.5.5. 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

$$k \geq \mathrm{length}(H^1_{\mathcal{F}}(\mathbb{Q}, T^*)^\vee_{\mathrm{tors}}) \tag{1.12}$$

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 $\mathrm{Fitt}^R_i\left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right) = \mathfrak{m}^{\alpha_i}$. By lemma 0.1.20,

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

Since k has been chosen satisfying (1.12), then $\min\{k, \alpha_i\} = 0$ if and only if $\alpha_i = 0$.

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

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

Note the last term is a free $R/\mathfrak{m}^{k_n}$-module of rank $\nu(n)$ by corollary 0.1.10. 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 1.5.3, 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 (1.10) 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 0.1.29, 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 0.1.30, 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

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

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 0.1.32, 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 1.5.3

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

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

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

When $h_i > e_{i+1} \geq e_{i+2}$ or $h_i \geq e_{i+1} > e_{i+2}$, lemma 0.1.32 implies the existence ℓ_{i+1} such that $h_{i+1} = e_{i+2}$.

If assumption (ii) holds true, then $\Theta_i(\kappa) \subsetneq \operatorname{Fitt}_i^R(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k]))$ 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

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

1.5.2 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 (1.10) for every $i \in \mathbb{Z}_{\geq 0}$. More precisely, assume the following extra assumptions.

- (N1) $\operatorname{Hom}_{\mathbb{F}_p[G_\mathbb{Q}]}(T/\mathfrak{m}T, T^*[\mathfrak{m}]) = 0$.
- (N2) The image of the homomorphism $R \to \operatorname{End}(T)$ is contained in the image of $\mathbb{Z}_p[[G_\mathbb{Q}]] \to \operatorname{End}(T)$.

Under those assumptions, the following improvement of theorem 1.5.5 is true. Sakamoto proves the equality (1.13) 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 1.5.8. Let $(T,\mathcal{F},\mathcal{P})$ be a Selmer triple satisfying (H0)-(H8) and (N1)-(N2). Then for every $i\in\mathbb{Z}_{\geq 0}$, the following equality is satisfied:

$$\Theta_i(\kappa)=\mathrm{Fitt}_i^R\left(H^1_{\mathcal{F}^*}(\mathbb{Q},T^*)^\vee\right) \tag{1.13}$$

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

Proposition 1.5.9. ([MR04, proposition 3.6.2]) Assume that T satisfies (H0)-(H4) 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 1.5.8 is based on the following lemma.

Lemma 1.5.10. Let $(T,\mathcal{F},\mathcal{P})$ be a Selmer triple satisfying (H0)-(H8) and (N1)-(N2). 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

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

Proof. Our assumption implies that $\mathrm{length}(R)>e_1$, so we can choose some $k\in\mathbb{N}$ such that $\mathrm{length}(R)\geq k>e_1$ and $\mathcal{P}_k\subset\mathcal{P}$.

By corollary 0.1.29, 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 0.1.10, $H^1_{\mathrm{f}}(\mathbb{Q}_\ell,T/\mathfrak{m}^k)$ 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 0.1.26, we have that

$$H^1_{\mathcal{F}^b}(\mathbb{Q},T/\mathfrak{m}^k)\approx R/\mathfrak{m}^k\times R/\mathfrak{m}^{e_2}\times\cdots\times R/\mathfrak{m}^{e_s} \tag{1.14}$$

By proposition 1.5.9, 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 $\mathrm{loc}^{\mathrm{f}}_b, \mathrm{loc}^{\mathrm{f}}_\ell \in \mathrm{Hom}(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*[\mathfrak{m}^k]), R/\mathfrak{m}^k)$. 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 0.1.26, 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 1.2.4, 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 0.1.9. 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 (1.14) 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
$$H^1_{\mathcal{F}(\ell)}(\mathbb{Q}, T/\mathfrak{m}^k) = \ker\left(\mathrm{loc}^{\mathrm{f}}_\ell : \ H^1_{\mathcal{F}^\ell}(\mathbb{Q}, T/\mathfrak{m}^k) \to H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T/\mathfrak{m}^k)\right) \cong R/\mathfrak{m}^{e_2} \times \cdots \times R/\mathfrak{m}^{e_s}$$
□

Proof of theorem 1.5.8. 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 1.5.5,

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

By lemma 1.5.3, for every $i \in \mathbb{Z}_{\geq 0}$ we just need to find some $n \in \mathcal{N}$ such that $\nu(n) = i$ and $\mathrm{Fitt}^R_i \left(H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee \right) = \mathfrak{m}^{\lambda(n)}$, 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 1.5.5 and, under assumptions (N1) and (N2), lemma 1.5.10 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). □

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. □

Notation 2.1.13. 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 2.1.14. 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 2.1.15. ([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 $\mathcal{C}^{\mathbb{N}}$,

$$\begin{tikzcd} 0 \arrow[r] & (A_n) \arrow[r, "\overline{\mu}"] & B_n \arrow[r, "\overline{\varepsilon}"] & C_n \arrow[r, "0"] & 0 \end{tikzcd}$$

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

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

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

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

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

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

Lemma 2.1.16. 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 2.1.17. 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 2.1.15 and Lemma 2.1.16, 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 2.1.18. 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 2.1.19. 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 2.1.20. 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 2.1.21. 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 2.1.22. In order to guarantee that Definition 2.1.21 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 2.1.23. Definition 2.1.21 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 2.1.24. 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 2.1.25. 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 2.1.26. Note that, when $\mathfrak{u}$ is a constant ultraprime, the semidirect product $\widehat{Z}(1) \rtimes \langle \mathrm{Frob}_{\mathfrak{u}} \rangle$ 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 2.1.27. 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

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\mu"] & B \arrow[r, "\varepsilon"] & C \arrow[r] & 0 \end{tikzcd}$$

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 T be an $R[[G_K]]$-module and let $\mathfrak{u}$ be an ultraprime represented by the sequence (ℓ_n). The local patched cohomology group is defined as

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

In the local case, the local patched cohomology coincides the group cohomology of the local Galois group defined in Definition 2.1.25.

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 2.1.16.

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 □

talk about R

2.3 Patched Selmer structures

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

Definition 2.3.1. Let $\mathfrak{u}_1 = \left(\ell_k^{(1)}\right)_{k\in\mathbb{N}}, \dots, \mathfrak{u}_s = \left(\ell_k^{(s)}\right)_{k\in\mathbb{N}}$ be a finite set of (distinct) ultraprimes. Its product is defined as

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

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

Definition 2.3.2. 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 2.3.3. 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 $\mathbf{H}^i(K^{\Sigma}/K, T)$.

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

- A finite set Σ 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 2.3.5. The Selmer module of a Selmer structure $\mathcal{F}$ is

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

local duality

Definition 2.3.6. 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 $\mathbf{H}^1(K_{\mathfrak{u}}, \mathbf{T}^*)$ as the the annihilator of $\mathbf{H}^1_{\mathcal{F}}(K_{\mathfrak{u}}, \mathbf{T})$ under the local duality pairing in Proposition 0.1.9.

Proposition 2.3.7. (Global duality) Let $\mathcal{F} \leq \mathcal{G}$ be two Selmer stuctures. Then there is a global duality exact sequence

$$\begin{tikzcd} H^1_{\mathcal{F}}(K,T) \arrow[r, tail] & H^1_{\mathcal{G}}(K,T) \arrow[r] & \bigoplus\limits_{\ell\in\Sigma_{\mathcal{F}}\cup\Sigma_{\mathcal{G}}} \dfrac{H^1_{\mathcal{G}}(K_\ell,T)}{H^1_{\mathcal{F}}(K_\ell,T)} \arrow[r] & H^1_{\mathcal{G}}(K,T^*)^\vee \arrow[r, two heads] & H^1_{\mathcal{F}}(K,T^*)^\vee \end{tikzcd}$$

Proof. Let T be a finite quotient of $\mathbf{T}$ and let $\mathfrak{n} = (n_k)_{k\in\mathbb{N}}$ be the square-free product of all ultraprimes in $\Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}$.

For a prime $\mathfrak{u} = (\mathfrak{u}_i)$ in $\Sigma_{\mathcal{F}} \cup \Sigma_{\mathcal{G}}$, 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 $W_{\mathfrak{u}} \in \mathcal{U}$. For every $i \in \mathcal{N}$, define the classical Selmer structre by $\Sigma_{\mathcal{F}_i} = \{\mathfrak{u}_i : \mathfrak{u} \in \Sigma_{\mathcal{F}} \cup \Sigma_{GG}\}$ and local conditions

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

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

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

Note that $\mathcal{F} \subset \mathcal{G}$ implies that $\mathcal{F}_i \subset \mathcal{G}_i$ as Selmer structures for all i, so they induce a global exact sequence. The exactness of the patching functor implies that

$$\begin{array}{rr} \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) = \mathcal{U}(\mathrm{Sel}_{\mathcal{F}_i}(\mathbb{Q}, T)) & \mathrm{Sel}_{\mathcal{G}}(\mathbb{Q}, T) = \mathcal{U}(\mathrm{Sel}_{\mathcal{F}_i}(\mathbb{Q}, T)) \\ \mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee = \mathcal{U}(\mathrm{Sel}_{\mathcal{F}_i^*}(\mathbb{Q}, T^*)^\vee) & \mathrm{Sel}_{\mathcal{G}}(\mathbb{Q}, T^*) = \mathcal{U}(\mathrm{Sel}_{\mathcal{G}_i^*}(\mathbb{Q}, T)) \end{array}$$

□

Chapter 3

Kolyvagin systems and biduals

The results on the previous chapter were limited in two different directions: the coefficient ring R was required to be principal and the core rank was at most one. These two assumptions were relaxed in the work of D. Burns, R. Sakamoto and T. Sano. In this work, Kolyvagin systems are redefined as collections of classes in the bidual exterior powers of Selmer groups and can be used to bound the Fitting ideals of the Selmer group. However, Kolyvagin systems in this setting do not determine all Fitting ideals of the Selmer group, and one need to introduce the notion of Stark system in order to do that.

3.1 Preliminaries on exterior powers

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

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

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

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

Lemma 3.2.1. Let $\mathfrak{m}, n, r \in \mathcal{N}$ be square-free products of Kolyvagin ultraprimes such that $m \mid n \mid r$. Then

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

Definition 3.2.2. The set of Stark systems of $\mathcal{F}$ is defined as the inverse limit

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

Theorem 3.2.3. 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.

perhaps comment that $n\ell$ is also a core vertex □

3.2.1 Core vertex

Definition 3.2.4. A *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 core vertex and let $m \in \mathcal{N}$ be such that $n \mid m$. Then m is also a core vertex.

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

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

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

Assumption 3.2.6. 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 3.2.7. The module of Stark systems $\mathbf{SS}(\mathcal{F})$ is a free Λ-module of rank one.

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

Proof. By assumption 3.2.6 and proposition 3.2.5, there exists a core vertex n such that $m \mid n$, which leads to the following exact sequence

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

which induces a map

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

Since ε generates $\mathbf{SS}(\mathcal{F})$, Theorem 3.2.3 implies that ε_n generates $\bigcap^{r+\nu(n)}$. Since $\varepsilon_m = \phi_{n,m}(\varepsilon_n)$, then proposition **??** implies that the image of ε_n contains $\mathrm{Fitt}^0(\mathbf{H}^1_{\mathcal{F}_m}(\mathbb{Q}, \mathbf{T}^*))$ with finite index. □

Bibliography

[BK90] Spencer Bloch and Kazuya Kato. ‘L-functions and Tamagawa numbers of motives’. In: *The Grothendieck Festschrift, Vol. I.* Vol. 86. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[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.

[Rub00] Karl Rubin. *Euler systems.* Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000, pp. xii+227.

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

[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`.