university of groningen

faculty of science and engineering

On Howard's Kolyvagin systems for residue characteristic 2

Master Project Mathematics

July 2024

Student: R.M. van Dijk

Supervisor: T. Keller

First examiner: J.S. Müller

Second examiner: J. Top

Abstract

In [How04] Howard reformulates Kolyvagin's proof [Kol89] of the bound on the p-Selmer group of an elliptic curve in a modern style, strengthening Kolyvagin's bound on the annihilator to a bound on the length; however, Howard omits the case where $p = 2$. In this thesis we discuss Howard's proof in detail, and in an attempt to generalize his results to all primes p, study where his proofs break down when $p = 2$. We find that under the assumption of two technical conjectures, a similar but weaker bound applies to the length of the 2-Selmer group.

Contents

1 Introduction

Kolyvagin's seminal paper [Kol89] on his Heegner point Euler system made it for the first time possible to prove finiteness of the Tate–Shafarevich groups of elliptic curves and, more generally, of abelian varieties with real multiplication. However, the elementary nature of his methods has caused the proofs of his results to be inaccessible to most readers.

In [How04], Howard adapted Kolyvagin's ideas into more modern and conceptual methods to obtain a bound on not just the annihilator of the p-Selmer group, but on its length; furthermore, Howard considered a more general framework that allows his results to be applied beyond the study of elliptic curves.

Unlike Kolyvagin, however, Howard's results assume that the prime p is odd, allowing him to exploit results about fields of odd characteristic that do not hold for characteristic 2, such as the fact that 1 and -1 are distinct. Although Kolyvagin managed to overcome the discrepancy between odd and even p, the fundamentally different nature of his proof does not allow his considerations to directly be applied to modify Howard's arguments.

This thesis discusses Howard's methods in detail, and in an attempt to generalize his results to all primes p, investigate where exactly his proofs break down when $p = 2$. To that end, we find that we must make a number of conjectures whose proof is outside the scope of this thesis. With those assumptions in mind, our final result is the following generalization of [How04, Theorem A].

Theorem. *Assume that Conjectures 6.3.4 and 7.2.2 hold. Let K be an imaginary quadratic field of discriminant $D \neq -3, -4$, E an elliptic curve defined over $\mathbb{Q}$ with conductor N, and p a rational prime. Assume that D, N and p are pairwise coprime and that K satisfies the "Heegner hypothesis" that all rational primes dividing N split in K; furthermore, assume that the representation $\mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ induced by the action of the absolute Galois group of K on the p-adic Tate module of E is surjective, and if $p = 2$, that the discriminant of E is negative. Let $S_p(E/K)$ and $\mathrm{Sel}_{p^\infty}(E/K)$ denote the usual Selmer groups that fit inside the exact sequences*

$$0 \longrightarrow E(K) \otimes \mathbb{Z}_p \longrightarrow S_p(E/K) \longrightarrow \varprojlim_k Ш(E/K)[p^k] \longrightarrow 0$$

and

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E/K) \longrightarrow Ш(E/K)[p^\infty] \longrightarrow 0.$$

If $\mathrm{ord}_{z=1} L(E/K, z) = 1$, then

- ***i)*** *$S_p(E/K)$ is a free $\mathbb{Z}_p$-module of rank 1;*
- ***ii)*** *$\mathrm{Sel}_{p^\infty}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus M \oplus M$ for some finite $\mathbb{Z}_p$-module M;*
- ***iii)*** *$\mathrm{len}(2^t M) \leq \mathrm{len}(S_p(E/K)/\kappa_1\mathbb{Z}_p) + (s-t)v_p(2)$;*

where κ denotes the Heegner point Kolyvagin system and $s \geq 1$ and $t \geq 0$ are integer constants.

As part of Conjecture 7.2.2, we assume that s and t are independent of E and provide an argument why $s = t = 1$ may suffice. Naturally, the values of s and t have no significance if $p > 2$.

This thesis is structured as follows. Section 2 lists a number of results from Galois theory and Galois cohomology; these can be found in most textbooks on the subjects so we do not provide proofs. Section 3 introduces the notions of local conditions and Selmer structures, along with relevant properties and examples. Section 4 defines Kolyvagin systems, but most of its content discusses a choice of transverse local condition required for said definition. Section 5 establishes the conventions and assumptions that are used throughout the remainder of the text.

Sections 6 and 7 may be considered the technical heart of the thesis: Section 6 proves a variety of structure results in the context of modules over Artinian rings, which are then used to deduce results over discrete valuation rings in Section 7. Finally, Section 8 motivates our theoretical framework by applying it in the context of elliptic curves. We define a suitable Selmer structure on the p-adic Tate module of an elliptic curve and construct its Heegner point Kolyvagin system, ultimately yielding the theorem stated above.

2 Preliminaries

This section summarizes a variety of notions and results that will be used throughout this thesis. The reader is assumed to have a basic understanding of commutative algebra (cf. [AM69]), Galois theory [Lan02, VI], algebraic number theory [Neu99, I–III], [Ste20] and elliptic curves [Sil08]. More advanced subject matter from e.g. class field theory and the theory of modular curves will be reviewed in the main text when relevant.

2.1 Ramification of Galois extensions

Let K be a global field with a place v. We are primarily interested in a number field K, in which case v corresponds to either a prime of K, a real embedding $K \hookrightarrow \mathbb{R}$ or a pair of conjugate complex embeddings $K \hookrightarrow \mathbb{C}$. We write K_v for the completion of K at v.

If L/K is a Galois extension, we denote its Galois group by $\mathrm{Gal}(L/K)$; if L is a separable (typically, algebraic) closure of K, we write $G_K = \mathrm{Gal}(L/K)$ for the absolute Galois group of K.

Suppose that v is non-archimedean and that w extends v to L. Then the decomposition group at w is the subgroup of $\mathrm{Gal}(L/K)$ given by

$$\mathrm{Gal}_w(L/K) := \{\sigma \in \mathrm{Gal}(L/K) : w \circ \sigma = w\},$$

that is, the stabilizer of w under the action of $\mathrm{Gal}(L/K)$. If we write $\mathcal{O}_w$ for the valuation ring of w and $\mathfrak{m}_w$ for its maximal ideal, we also have the inertia group

$$I_w(L/K) := \{\sigma \in \mathrm{Gal}_w(L/K) : \sigma(x) \equiv x \bmod \mathfrak{m}_w \text{ for all } x \in \mathcal{O}_w\}$$

and the ramification group

$$R_w(L/K) := \left\{\sigma \in \mathrm{Gal}_w(L/K) : \sigma(x)/x \equiv 1 \bmod \mathfrak{m}_w \text{ for all } x \in L^\times\right\}.$$

In the local extension L_w/K_v, w is the unique extension of v, so it follows that $\mathrm{Gal}_w(L_w/K_v) = \mathrm{Gal}(L_w/K_v)$, and similarly we will write $I(L_w/K_v) := I_w(L_w/K_v)$ and $R(L_w/K_v) := R_w(L_w/K_v)$. There is a natural way in which these subgroups relate to the respective subgroups for the global extension L/K.

Lemma 2.1.1 ([Neu99, II.9.6]). *The restriction map* $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(L/K)$ *defined by* $\sigma \mapsto \sigma|_L$ *induces isomorphisms*

$$\mathrm{Gal}_w(L/K) \cong \mathrm{Gal}(L_w/K_v), \quad I_w(L/K) \cong I(L_w/K_v), \quad R_w(L/K) \cong R(L_w/K_v).$$

We will frequently make the identifications from Lemma 2.1.1, especially between the decomposition group of L/K at w and the Galois group of L_w/K_v. In particular, we will identify the absolute Galois group of K_v with the decomposition subgroup of G_K at v. The importance of the inertia group becomes apparent from the following lemma.

Lemma 2.1.2 ([Neu99, II.9.11]). *The fixed field of* $I(L_w/K_v)$ *is the maximal unramified subextension of* L_w/K_v.

In particular, if L is the separable closure of K, then the fixed field of $I(L_w/K_v)$ is the maximal unramified extension of K_v, which we denote by K_v^{unr}. By [Neu99, II.9.14] we similarly have that the fixed field of $R(L_w/K_v)$ is the maximal tamely ramified subextension of L_w/K_v, but we will have no use for that fact.

Lastly, suppose that L_w/K_v is an unramified extension and denote the respective residue fields by l_w and k_v. Since these residue fields are finite, then $\mathrm{Gal}(L_w/K_v)$ can be identified with $\mathrm{Gal}(l_w/k_v)$, which is cyclic and generated by the Frobenius map $x \mapsto x^{|k_v|}$. We denote by $\mathrm{Fr}_v \in \mathrm{Gal}(L_w/K_v)$ the automorphism corresponding to this generator, and we will also refer to it as the Frobenius map (at v). We will often confuse Fr_v with the corresponding generator of $\mathrm{Gal}_w(L/K)$ under the identification from Lemma 2.1.1.

2.2 Galois modules

Let G be a group and R a commutative ring (with multiplicative identity). The group algebra $R[G]$ is the set of formal R-linear combinations of elements of G, or equivalently the free R-module generated by the

elements of G. Addition and scalar multiplication is defined coefficientwise, and multiplication is given by

$$\left(\sum_{g\in G} c_g g\right)\cdot\left(\sum_{h\in G} d_h h\right) = \sum_{g,h\in G} c_g d_h (gh).$$

Note that this multiplication is generally not commutative. Alternatively, one could view the elements of $R[G]$ as maps $G \to R$ with finite support, given by $g \mapsto c_g$.

When the ring R is understood, we refer to a (left) $R[G]$-module as simply a G-module. Such a G-module A can be viewed as an R-module together with an action of G that is compatible with the R-module structure of A. That is, there is a map $G \times A \to A$ sending (g, a) to ga, satisfying

$$(gh)a = g(ha), \quad g(a+b) = ga + gb, \quad g(ra) = r(ga)$$

for all $g, h \in G$, $a, b \in A$ and $r \in R$. Likewise, we will often refer to $R[G]$-submodules and $R[G]$-module homomorphisms as G-submodules and G-module homomorphisms, respectively.

Remark 2.2.1. Some texts prefer to denote the image of (g, a) by a^g, but this comes with the notational inconvenience that $(a^g)^h = a^{hg}$. We will therefore avoid this notation.

The action of G on A gives rise to a representation (group homomorphism) $G \to \mathrm{Aut}_R(A)$ that sends g to the map $a \mapsto ga$. When an $R[G]$-module is given, it is understood that the notation $G \to \mathrm{Aut}_R(A)$ refers to this representation.

Example 2.2.2. Every R-module A can be regarded as a G-module by equipping it with the trivial action $ga = a$. If A is any G-module and H is a subgroup of G, then A is also an H-module.

Example 2.2.3. A Galois module is simply a G-module where G is a Galois group. For instance, any Galois extension L/K gives rise to an action of $\mathrm{Gal}(L/K)$ on the K-module L.

Example 2.2.4. Let E be an elliptic curve defined over a field K with Galois extension L. Then $E(L)$ is a $\mathbb{Z}[\mathrm{Gal}(L/K)]$-module with the action of $\mathrm{Gal}(L/K)$ defined in the obvious manner: $\sigma(x, y) = (\sigma(x), \sigma(y))$, with x and y a choice of Weierstrass coordinates for E. In particular, E itself is a G_K-module if K is a number field. Similarly, the Tate module $T_p(E)$ of E can be viewed as a $\mathbb{Z}_p[G_K]$-module.

Example 2.2.5. We typically define the action of G on R to be trivial, but we may also equip it with a more interesting action as follows. Let $\chi_p \colon G \to \mathbb{Z}_p^\times$ denote a p-adic character (group homomorphism); then, for any $g \in G$ and $x \in \mathbb{Z}_p$, define the group action by $gx = \chi_p(g)x$. If $G = G_K$ is the absolute Galois group of a number field K, then χ_p is taken to be the usual p-adic cyclotomic character. The resulting G-module is called the Tate twist of $\mathbb{Z}_p$, denoted by $\mathbb{Z}_p(1)$ to distinguish it from the G-module with trivial action.

If A is a $\mathbb{Z}_p$-module, then we define the Tate twist $A(1) = A \otimes \mathbb{Z}_p(1)$, with the tensor product taken over $\mathbb{Z}$, which effectively means that $ga = \chi_p(g)a$ for any $a \in A$ and $g \in G$. In particular, this gives rise to a nontrivial G-module $R(1)$ if R is a $\mathbb{Z}_p$-algebra.

Example 2.2.6. If R is a $\mathbb{Z}_p$-algebra, then every $R[G]$-module A has a dual $A^* = \mathrm{Hom}_{R[G]}(A, R(1))$, on which $(g\phi)(a) = g\phi(g^{-1}a) = \chi_p(g)\phi(g^{-1}a)$.

Given a G-module A, we denote its fixed or invariant submodule by

$$A^G = \{a \in A : ga = a \text{ for all } g \in G\}.$$

Let us now turn to the specific case of Galois modules: let A be a $\mathrm{Gal}(L/K)$-module for some Galois extension L/K. The kernel of $\mathrm{Gal}(L/K) \to \mathrm{Aut}_R(A)$ is a normal subgroup of $\mathrm{Gal}(L/K)$, say H, whose elements act trivially on A. The fixed or trivializing field of H is denoted by $K(A) = L^H$.

If w is a place of L and $H \subset I_w(L/K)$, then A is said to be unramified at A. Equivalently, A is called unramified if $A^{I_w(L/K)} = A$.

Example 2.2.7. Let E be an elliptic curve over a number field K, equipped with the G_K-action from Example 2.2.4. If L/K is some Galois extension and $\bar{K}$ is an algebraic closure of K that contains L, then $E(\bar{K})^{G_L} = E(L)$.

2.3 Galois cohomology

The concept of group cohomology arises from the observation that when

$$0 \longrightarrow A \xrightarrow{p} B \xrightarrow{q} C \longrightarrow 0$$

is a short exact sequence of $R[G]$-modules (that is, all terms are $R[G]$-modules and all maps are $R[G]$-homomorphisms), then

$$0 \longrightarrow A^G \xrightarrow{p|_{A^G}} B^G \xrightarrow{q|_{B^G}} C^G \tag{2.1}$$

need not be exact on the right. We can however extend (2.1) into a long exact sequence using the following.

Theorem-Definition 2.3.1 (Group cohomology; [NSW20, I.2–3])**.** *There is an (up to isomorphism) unique collection of endofunctors $H^i(G,\cdot)$ on the category of G-modules, for $i \in \mathbb{Z}_{\geq 0}$, with the following properties:*

i) *$H^0(G,A) = A^G$ for every G-module A, and if $p\colon A \to B$, then $H^0(G,p) = p|_{A^G}$;*

ii) *If*

$$0 \longrightarrow A \xrightarrow{p} B \xrightarrow{q} C \longrightarrow 0$$

is a short exact sequence of G-modules, then there is a functorial exact sequence

$$0 \longrightarrow H^0(G,A) \xrightarrow{H^0(G,p)} H^0(G,B) \xrightarrow{H^0(G,q)} H^0(G,C)$$

$$\xrightarrow{d_1} H^1(G,A) \xrightarrow{H^1(G,p)} H^1(G,B) \xrightarrow{H^1(G,q)} H^1(G,C) \xrightarrow{d_2} \cdots$$

$$\cdots \xrightarrow{d_i} H^i(G,A) \xrightarrow{H^i(G,p)} H^i(G,B) \xrightarrow{H^i(G,q)} H^i(G,C) \xrightarrow{d_{i+1}} \cdots$$

iii) *If $A \cong \mathrm{Hom}_R(R[G],M)$ for some R-module M, then $H^i(G,A) = 0$ for all $i > 0$.*

The functoriality requirement in condition **(ii)** means that if

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{p} & B & \xrightarrow{q} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{p'} & B' & \xrightarrow{q'} & C' & \longrightarrow & 0 \end{array}$$

is a commutative diagram with exact rows, then the induced diagram

$$\begin{array}{ccccccccccccc} \cdots & \xrightarrow{d_i} & H^i(G,A) & \xrightarrow{H^i(G,p)} & H^i(G,B) & \xrightarrow{H^i(G,q)} & H^i(G,C) & \xrightarrow{d_{i+1}} & H^{i+1}(G,A) & \xrightarrow{H^{i+1}(G,p)} & \cdots \\ & & \downarrow{\scriptstyle H^i(G,\alpha)} & & \downarrow{\scriptstyle H^i(G,\beta)} & & \downarrow{\scriptstyle H^i(G,\gamma)} & & \downarrow{\scriptstyle H^{i+1}(G,\alpha)} & & \\ \cdots & \xrightarrow{d'_i} & H^i(G,A') & \xrightarrow{H^i(G,p')} & H^i(G,B') & \xrightarrow{H^i(G,q')} & H^i(G,C') & \xrightarrow{d'_{i+1}} & H^{i+1}(G,A') & \xrightarrow{H^{i+1}(G,p')} & \cdots \end{array}$$

commutes as well. We will typically simply write α for $H^i(G,\alpha)$, and it should be clear from the context which induced map we are referring to; similarly, we often write d for the connecting maps d_i.

Property **(iii)** has no relevance in the rest of this text. It is simply a prerequisite to ensure that the cohomology modules $H^i(G,A)$ are essentially unique.

By definition, the 0th cohomology module is just the fixed submodule, on which the action of G is trivial. We also have an explicit description for the 1st cohomology module:

Proposition 2.3.2. *Let A be an $R[G]$-module. Define the module of 1-cochains $C^1(G,A)$ to be the set of maps $G \to A$, equipped with pointwise addition and scalar multiplication, and the group action given by $(h\xi)(g) = h(\xi(hgh^{-1}))$ for $\xi \in C^1(G,A)$ and $g,h \in G$. Define the submodules of 1-cocycles and 1-*

coboundaries by

$$Z^1(G,A) = \{\xi \in C^1(G,A) : \xi(gh) = \xi(g) + g(\xi(h)) \text{ for all } g,h \in G\}$$

and

$$B^1(G,A) = \{\xi \in C^1(G,A) : \text{there exists an } a \in A \text{ such that } \xi(g) = ga - a \text{ for all } g \in G\},$$

respectively. Then $H^1(G,A) \cong Z^1(G,A)/B^1(G,A)$*, with the* $R[G]$*-module structure inherited from* $C^1(G,A)$*.*

Corollary 2.3.3. *Let* A *be a* G*-module. Then* $H^1(G,A^G) \cong \mathrm{Hom}(G,A^G)$*.*

We will often identify elements of a cohomology module with cocycle classes.

Suppose that A is a G-module and H is a subgroup of G. Then the restriction $\xi \mapsto \xi|_H$ defines a map $C^1(G,A) \to C^1(H,A)$, which induces the restriction map $\mathrm{Res}\colon H^1(G,A) \to H^1(H,A)$. If H is a normal subgroup, then A^H may be regarded as a G/H-module, and we define a map $C^1(G/H,A^H) \to C^1(G,A)$ by sending $\xi\colon G/H \to A^H$ to the map that sends $g \in G$ to $\xi(gH)$. This induces the inflation map $\mathrm{Inf}\colon H^1(G/H,A^H) \to H^1(G,A)$. Together, these maps fit inside the exact inflation-restriction sequence:

Proposition 2.3.4 ([Rub09, 1.4.5])**.** *Let* A *be a* G*-module and* H *a normal subgroup of* G*. Then there is an exact sequence*

$$0 \longrightarrow H^1(G/H,A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A)^{G/H} \longrightarrow H^2(G/H,A^H) \longrightarrow H^2(G,A).$$

Remark 2.3.5. There are descriptions of $H^i(G,A)$ similar to Proposition 2.3.2 for $i > 1$, as the quotient of i-cocycles by i-coboundaries, which give rise to restriction maps from and inflation maps to each $H^i(G,A)$. Details of this construction can be found in [NSW20, I.2], but in this thesis we are primarily concerned with $i = 1$.

As with Galois modules, Galois cohomology simply refers to group cohomology when G is a Galois group, i.e. the group cohomology of Galois modules. If L/K is a Galois extension of fields and A is a $\mathrm{Gal}(L/K)$-module, then we will write $H^i(L/K,A) = H^i(\mathrm{Gal}(L/K),A)$; if L is a separable closure of K, then we write $H^i(K,A) = H^i(L/K,A)$. If v is a place of K, we refer to the restriction map induced by $G_{K_v} \subset G_K$ as the localization map $\mathrm{loc}_v\colon H^1(K,A) \to H^1(K_v,A)$, and the image of $c \in H^1(K,A)$ under this map is denoted by c_v.

Remark 2.3.6. Suppose that both G and A are equipped with a topology; typically, we assume that G and A both have the profinite topology, cf. [NSW20, I.1] or [Lan02, 1.10 and 6.14]. Then A is said to be a *continuous* G-module if the map $G \times A \to A$ is continuous. Together with the idea of *continuous* G-homomorphisms, this gives rise to the concept of *continuous* group cohomology, which can be described in terms of *continuous* cocycles modulo *continuous* coboundaries. Restriction and inflation is defined in the same way as before, under the assumption that the (normal) subgroup in question is *closed*.

Although this topological aspect is an important requirement for some of the results that we cite, it will not play an explicit role in our own proofs. Therefore, any further mention of G-modules, G-homomorphisms, cohomology and subgroups will refer to their topological counterpart. The relevant topologies should be clear from the context.

One important result that relies on the assumption of continuity is the following.

Theorem-Definition 2.3.7 (Local Tate duality, [NSW20, 7.2.6])**.** *Let* K_v *be a local field of characteristic* 0*, and* A *a finite (continuous)* $R[G_{K_v}]$*-module with* R *a* $\mathbb{Z}_p$*-algebra. Then there is a perfect,* G_{K_v}*-invariant,* R*-bilinear pairing, called the local Tate pairing,*

$$\langle \cdot,\cdot \rangle_v\colon H^1(K_v,A) \times H^1(K_v,A^*) \longrightarrow R.$$

In particular, if K_v *is the localization of a number field* K *at a place* v*, and* A *is a (continuous)* $R[G_K]$*-module, then the local Tate pairing is* G_K*-invariant.*

The local Tate pairing can be constructed from the cup product $H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, A \otimes B)$ [NSW20, 1.4] which exists for general cohomology modules, together with an isomorphism between $H^2(K_v, A \otimes A^*)$ and R.

Without proof, we state a property of the local Tate pairing which we will use twice. It can be deduced as a corollary of the Albert–Brauer–Hasse–Noether theorem, cf. [NSW20, 8.1.17].

Lemma 2.3.8. *If $c \in H^1(K, T)$ and $c^* \in H^1(K, T^*)$, then*

$$\sum_v \langle c, c^* \rangle_v = 0,$$

where the sum runs over all places of K.

3 Selmer structures

3.1 Local conditions

Throughout this section, let K be a number field, G_K its absolute Galois group, R a ring, and T an $R[G_K]$-module that is finitely generated over R and unramified at all but finitely many places. Given a finite place v of K, denote by k_v its residue field and by $\mathrm{Fr}_v \in \mathrm{Gal}(K_v^{\mathrm{unr}}/K_v)$ its Frobenius element.

Definition 3.1.1 (Local conditions)**.** Let v be a place of K. A local condition $\mathcal{F}$ on T (at v or over K_v) is a choice of R-submodule $H^1_{\mathcal{F}}(K_v, T)$ of $H^1(K_v, T)$.

Given an R-linear injection $f\colon S \to T$, we may propagate $\mathcal{F}$ through f by defining $H^1_{\mathcal{F}}(K_v, S)$ to be the preimage of $H^1_{\mathcal{F}}(K_v, T)$ under the map $H^1(K_v, S) \to H^1(K_v, T)$ induced by f. Likewise, we may propagate $\mathcal{F}$ through a linear surjection $f'\colon T \to S'$ by defining $H^1_{\mathcal{F}}(K_v, S')$ to be the image of $H^1_{\mathcal{F}}(K_v, T)$ under the map induced by f'. We still refer to these propagated local conditions on S and S' as $\mathcal{F}$. In particular, a local condition on T induces local conditions on all submodules and quotients of T.

Example 3.1.2. Trivially, there are the relaxed and strict conditions (at some place v of K), given by $H^1_{\mathrm{rel}}(K_v, T) := H^1(K_v, T)$ and $H^1_{\mathrm{str}}(K_v, T) := 0$, respectively. Two more interesting local conditions will play an important role in the sequel: the unramified condition

$$H^1_{\mathrm{unr}}(K_v, T) := \ker\left[\mathrm{Res}\colon H^1(K_v, T) \to H^1(K_v^{\mathrm{unr}}, T)\right],$$

where K_v^{unr} is the maximal unramified extension of K_v; and, for a maximal totally tamely ramified abelian p-extension of L/K_v, the L-transverse condition

$$H^1_{L-\mathrm{tr}}(K_v, T) := \ker\left[\mathrm{Res}\colon H^1(K_v, T) \to H^1(L, T)\right].$$

If $v \nmid p$ and T is unramified at v, then we will refer to the unramified condition as the finite condition, $H^1_{\mathrm{f}}(K_v, T) = H^1_{\mathrm{unr}}(K_v, T)$. In that case, we define the singular condition $H^1_{\mathrm{s}}(K_v, T)$ to be the cokernel of the inclusion $H^1_{\mathrm{f}}(K_v, T) \hookrightarrow H^1(K_v, T)$. We will soon see that, under some relatively weak assumptions, the singular condition is isomorphic to any L-transverse condition.

Definition 3.1.3. Let $\mathcal{T}$ be a subcategory of the category of $R[G_{K_v}]$-modules. A functorial local condition $\mathcal{F}$ over $\mathcal{T}$ is a subfunctor $T \mapsto H^1_{\mathcal{F}}(K_v, T)$ of the cohomology functor $T \mapsto H^1(K_v, T)$. A functorial local condition $\mathcal{F}$ over $\mathcal{T}$ is called cartesian if, for any injective morphism $\alpha\colon S \to T$ in $\mathcal{T}$, the functor $\mathcal{F}$ defines the same local condition on S as the local condition obtained by propagating the local condition $\mathcal{F}$ on T through α.

Remark 3.1.4. A functorial local condition $\mathcal{F}$ over $\mathcal{T}$ is cartesian precisely when, for any injection $\alpha\colon S \to T$, the diagram

$$\begin{array}{ccc} H^1_{\mathcal{F}}(K_v, S) & \hookrightarrow & H^1(K_v, S) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\ H^1_{\mathcal{F}}(K_v, T) & \hookrightarrow & H^1(K_v, S) \end{array}$$

is a pullback, i.e. a cartesian square. This is how the cartesian condition is defined in e.g. [MR04, 1.1.4].

Lemma 3.1.5. *Let $\mathcal{T}$ denote the category of $R[G_{K_v}]$-modules that are finitely generated over R, and $\mathcal{T}^{\mathrm{unr}}$ its full subcategory of unramified modules.*

- ***i)*** *The relaxed, strict, unramified and L-transverse local conditions from Example 3.1.2 define functorial local conditions on $\mathcal{T}$.*
- ***ii)*** *The relaxed and strict local conditions are cartesian on $\mathcal{T}$.*
- ***iii)*** *The unramified (hence finite) local condition is cartesian on $\mathcal{T}^{\mathrm{unr}}$.*

Proof. Both **(i)** and **(ii)** are immediate from the definitions. The third claim is [MR04, 1.1.9]: for the sake of illustrating the definitions we've encountered so far, we discuss the proof in detail.

By the definition of the singular condition, we have an exact sequence

$$0 \longrightarrow H^1_{\mathrm{f}}(K_v, T) \hookrightarrow H^1(K_v, T) \longrightarrow H^1_{\mathrm{s}}(K_v, T) \longrightarrow 0.$$

Furthermore, if we denote the inertia group of v by $I_v \subset G_{K_v}$, [Rub09, 1.4.13(2)] or [MR04, 1.1.6] state that $H^1_{\mathrm{s}}(K_v, T) \cong \mathrm{Hom}(I_v, T)^{G_{K_v}}$. Hence, if we have an injection $\alpha\colon S \to T$ of unramified modules, we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1_{\mathrm{f}}(K_v, S) & \hookrightarrow & H^1(K_v, S) & \longrightarrow & \mathrm{Hom}(I_v, S) \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\ 0 & \longrightarrow & H^1_{\mathrm{f}}(K_v, T) & \hookrightarrow & H^1(K_v, T) & \longrightarrow & \mathrm{Hom}(I_v, T). \end{array} \tag{3.1}$$

Since $\alpha\colon S \to T$ is injective and $\mathrm{Hom}(I_v, \cdot)$ is left exact, the rightmost vertical map in (3.1) is injective. Now, let $c \in H^1(K_v, S)$ be such that $\alpha(c) \in H^1_{\mathrm{f}}(K_v, T)$. The exactness of the bottom row of (3.1) then tells us that $\alpha(c)$ is mapped to 0 under the bottom right map; from the commutativity of the right square and the injectivity of the rightmost vertical map, it follows that c vanishes under the top right map, which means that $c \in H^1_{\mathrm{f}}(K_v, S)$. This shows that $\alpha^{-1}H^1_{\mathrm{f}}(K_v, T) = H^1_{\mathrm{f}}(K_v, S)$, proving **(iii)**. □

Although the L-transverse condition is generally not cartesian on $\mathcal{T}$ or $\mathcal{T}^{\mathrm{unr}}$, we will find that under additional assumptions on R, it is cartesian on a smaller subcategory:

Definition 3.1.6. For an $R[G_{K_v}]$-module T, we define the category of quotients $\mathrm{Quot}(T)$ to be the category whose objects are quotients $T/\mathfrak{a}T$ by ideals $\mathfrak{a}$ of R, and whose morphisms $T/\mathfrak{a}T \to T/\mathfrak{b}T$ are induced by scalar multiplications $r \in R$ with $r\mathfrak{a} \subset \mathfrak{b}$.

Clearly, any local condition on T as defined in Definition 3.1.1 gives rise to a functorial (but not necessarily cartesian) local condition on $\mathrm{Quot}(T)$.

Proposition 3.1.7. *Suppose that $v \nmid p\infty$, that T is unramified at v and that T is annihilated by $|k_v^\times|$. Then there are canonical isomorphisms*

$$H^1_{\mathrm{f}}(K_v, T) \cong T/(\mathrm{Fr}_v - 1)T \quad \textit{and} \quad H^1_{\mathrm{s}}(K_v, T) \otimes k_v^\times \cong T^{\mathrm{Fr}_v = 1}.$$

In particular, if G_{K_v} acts trivially on T then we have the finite-singular comparison map

$$\phi_v^{\mathrm{fs}}\colon H^1_{\mathrm{f}}(K_v, T) \cong T \cong H^1_{\mathrm{s}}(K_v, T) \otimes k_v^\times.$$

Proof. This is a straight forward generalization of [Rub00, 1.3.2], stated in [MR04, 1.2.1]. We will not give a proof here, but we do note that the first isomorphism $H^1_{\mathrm{f}}(K_v, T) \to T/(\mathrm{Fr}_v - 1)T$ is given by evaluating cocycle classes at Fr_v. □

Remark 3.1.8. By choosing a generator of $k_v^\times$, we may identify $H^1_{\mathrm{s}}(K_v, T) \otimes k_v^\times$ with $H^1_{\mathrm{s}}(K_v, T)$, so that Proposition 3.1.7 gives an isomorphism $H^1_{\mathrm{s}}(K_v, T) \cong T^{\mathrm{Fr}_v = 1}$ and the finite-singular map induces an isomorphism between $H^1_{\mathrm{f}}(K_v, T)$ and $H^1_{\mathrm{s}}(K_v, T)$. Although the arbitrary choice of generator means that these isomorphisms are no longer canonical, this does not affect any arguments in which they are used so we will frequently omit the tensor product with $k_v^\times$.

Recall from Theorem-Definition 2.3.7 that for $T^* = \mathrm{Hom}(T, R(1))$, we have the local Tate pairing

$$\langle \cdot, \cdot \rangle_v\colon H^1(K_v, T) \times H^1(K_v, T^*) \to R.$$

Given a local condition on T, this pairing allows us to obtain a local condition on T^*; typically, we will assume that $T \cong T^*$, so that we obtain a new local condition on T.

Definition 3.1.9 (Dual local conditions)**.** Let $\mathcal{F}$ be a local condition on T (at v). The dual local condition $\mathcal{F}^*$ on T^* is the orthogonal complement of $H^1_{\mathcal{F}}(K_v, T)$ under the local Tate pairing.

Proposition 3.1.10 ([MR04, 1.2.4 and 1.3.2])**.** *Assume that $v \nmid p\infty$, that T is unramified at v and that T is annihilated by $|k_v^\times|$. Furthermore, let L/K_v be a choice of maximal totally tamely ramified abelian p-extension. Then the L-transverse condition $H^1_{L-\mathrm{tr}}(K_v, T)$ projects isomorphically onto the singular condition $H^1_{\mathrm{s}}(K_v, T)$, and we have a splitting*

$$H^1(K_v, T) = H^1_{\mathrm{f}}(K_v, T) \oplus H^1_{\mathrm{tr}}(K_v, T).$$

Moreover, the dual local condition of the finite (respectively L-transverse) condition is the finite (resp. L-transverse) condition on T^*.

Remark 3.1.11. Combining Propositions 3.1.7 and 3.1.10 shows that, under the specified conditions, we have $H^1(K_v, T) \cong T \oplus T$. Also, if $T \cong T^*$, then the finite and L-transverse conditions are their own duals.

3.2 Selmer modules

Now that we've discussed the local situation, we may construct a submodule of the global cohomology module $H^1(K, T)$ by choosing a local condition at each place of K. For the resulting submodule to be useful, however, we must impose an extra condition on our local choices.

Definition 3.2.1 (Selmer structures)**.** A Selmer structure $\mathcal{F}$ on T (over K) is a choice of local condition at each place of K, also denoted by $\mathcal{F}$, such that $\mathcal{F}$ is the finite condition at all but finitely many places. The Selmer module associated to $\mathcal{F}$ is the submodule

$$H^1_{\mathcal{F}}(K, T) := \ker\left[\bigoplus_v \mathrm{loc}_v \colon H^1(K, T) \to \bigoplus_v \left(H^1(K_v, T)/H^1_{\mathcal{F}}(K_v, T)\right)\right],$$

that is, the submodule of $H^1(K, T)$ consisting of all classes whose localization at v lies in $H^1_{\mathcal{F}}(K_v, T)$, for each place v of K.

Remark 3.2.2. Equivalently, one could define a Selmer structure $\mathcal{F}$ on T to be a finite set of places $\Sigma(\mathcal{F})$ that contains the places dividing p, all archimedean places and all places at which T is ramified; at each $v \in \Sigma(\mathcal{F})$, the Selmer structure establishes a choice of local condition at v, and the associated Selmer module is given by

$$H^1_{\mathcal{F}}(K^{\Sigma(\mathcal{F})}/K, T) = \ker\left[\bigoplus_{v\in\Sigma(\mathcal{F})} \mathrm{loc}_v \colon H^1(K, T) \to \bigoplus_{v\in\Sigma(\mathcal{F})} \left(H^1(K_v, T)/H^1_{\mathcal{F}}(K_v, T)\right)\right]$$

with $K^{\Sigma(F)}/K$ the maximal extension that is unramified outside all $v \in \Sigma(\mathcal{F})$. At the places $v \notin \Sigma(\mathcal{F})$, the local condition $\mathcal{F}$ is implied to be the finite condition. In line with this definition, we use $\Sigma(\mathcal{F})$ to denote the places at which $\mathcal{F}$ does not have the finite condition. The assumption that $\Sigma(\mathcal{F})$ is finite is a critical ingredient for the following result.

Lemma 3.2.3. *Let $\mathcal{F}$ be a Selmer structure on T and suppose that T is finite. Then $H^1_{\mathcal{F}}(K, T)$ is finite.*

Proof. This is a standard result that can be found in e.g. [Sil08, X.4.3] or [Mil06, I.4.15]. □

We define a partial order on the set of all Selmer structures (on a fixed module T) by writing $\mathcal{F} \leq \mathcal{G}$ if and only if $H^1_{\mathcal{F}}(K_v, T) \subset H^1_{\mathcal{G}}(K_v, T)$ for every place v of K; it immediately follows that $H^1_{\mathcal{F}}(K, T) \subset H^1_{\mathcal{G}}(K, T)$ if $\mathcal{F} \leq \mathcal{G}$.

With Definition 3.1.9 in mind, a Selmer structure $\mathcal{F}$ on T induces a dual Selmer structure $\mathcal{F}^*$ on T^* by taking $\mathcal{F}^*$ at v to be the dual local condition of $\mathcal{F}$ at v. This is again a Selmer structure because of Proposition 3.1.10. If $\mathcal{F} \leq \mathcal{G}$, then $\mathcal{G}^* \leq \mathcal{F}^*$. This leads us to the following theorem, which will play a major role in proving our later results.

Theorem 3.2.4 (Global (Poitou–Tate) duality)**.** *Let $\mathcal{F} \leq \mathcal{G}$ be Selmer structures on T. The images of the rightmost maps in the exact sequences*

$$0 \longrightarrow H^1_{\mathcal{F}}(K,T) \hookrightarrow H^1_{\mathcal{G}}(K,T) \xrightarrow{\oplus_v \mathrm{loc}_v} \bigoplus_v H^1_{\mathcal{G}}(K_v,T)/H^1_{\mathcal{F}}(K_v,T) \tag{3.2}$$

$$0 \longrightarrow H^1_{\mathcal{G}^*}(K,T^*) \hookrightarrow H^1_{\mathcal{F}^*}(K,T^*) \xrightarrow{\oplus_v \mathrm{loc}_v} \bigoplus_v H^1_{\mathcal{F}^*}(K_v,T^*)/H^1_{\mathcal{G}^*}(K_v,T^*)$$

are each other's orthogonal complements under the sum of local Tate pairings restricted to the summands of the rightmost terms. That is, each local Tate pairing on $H^1(K_v,T) \times H^1(K_v,T^*)$ induces a pairing on $(H^1_{\mathcal{G}}(K_v,T)/H^1_{\mathcal{F}}(K_v,T)) \times (H^1_{\mathcal{F}^*}(K_v,T^*)/H^1_{\mathcal{G}^*}(K_v,T^*))$, and the images of the rightmost maps in (3.2) are orthogonal complements under the sum of those pairings.

Proof. A proof is well beyond the scope of this thesis; curious readers can find details in [Rub00, 1.7.3], [Mil06, 4.15] and [Tat62, 3.1]. □

The following applications of Theorem 3.2.4 will be useful later.

Example 3.2.5. Let $\mathcal{F} \leq \mathcal{G}$ be Selmer structures on T such that $H^1_{\mathcal{F}}(K,T) = H^1_{\mathcal{G}}(K,T)$. This need not imply that $\mathcal{F} = \mathcal{G}$; rather, this means that every $c \in H^1(K,T)$ with the property that $c_v \in H^1_{\mathcal{G}}(K_v,T)$ for all places v, in fact satisfies the stronger condition that $c_v \in H^1_{\mathcal{F}}(K_v,T)$ for all v. Under this assumption, the exactness of (3.2) implies that the image of $H^1_{\mathcal{G}}(K,T)$ is trivial. Consequently, Theorem 3.2.4 tells us that every $\mathrm{loc}_v \colon H^1_{\mathcal{F}^*}(K,T^*) \to H^1_{\mathcal{F}^*}(K_v,T^*)/H^1_{\mathcal{G}^*}(K_v,T^*)$ is surjective.

Example 3.2.6. Let $T \cong T^*$ and $\mathcal{F}$ a Selmer structure on T satisfying $\mathcal{F} = \mathcal{F}^*$. Fix a place $v \notin \Sigma(\mathcal{F})$ (i.e. at which $\mathcal{F}$ has the finite condition) and denote by $\mathcal{F}_v$ the Selmer structure that has the strict condition at v and the same local conditions as $\mathcal{F}$ elsewhere; likewise, $\mathcal{F}^v$ has the relaxed condition at v and the same conditions as $\mathcal{F}$ elsewhere. Then $H^1_{\mathcal{F}}(K_v,T)/H^1_{\mathcal{F}_v}(K_v,T) = H^1_{\mathrm{f}}(K_v,T)$ and $H^1_{\mathcal{F}^v}(K_v,T)/H^1_{\mathcal{F}}(K_v,T) = H^1_{\mathrm{s}}(K_v,T) \cong H^1_{L-\mathrm{tr}}(K_v,T)$ by Proposition 3.1.10, so that (3.2) becomes

$$0 \longrightarrow H^1_{\mathcal{F}_v}(K,T) \hookrightarrow H^1_{\mathcal{F}}(K,T) \xrightarrow{\mathrm{loc}_v} H^1_{\mathrm{f}}(K_v,T),$$

$$0 \longrightarrow H^1_{\mathcal{F}}(K,T) \hookrightarrow H^1_{\mathcal{F}^v}(K,T) \xrightarrow{\mathrm{loc}_v} H^1_{L-\mathrm{tr}}(K_v,T).$$

Denote the images on the right by A_{f} and A_{tr}, respectively. Then Theorem 3.2.4 states that A_{f} and A_{tr} are orthogonal complements under the local Tate pairing restricted to $H^1_{\mathrm{f}}(K_v,T) \times H^1_{L-\mathrm{tr}}(K_v,T)$. Keeping in mind the splitting from Proposition 3.1.10 and Remark 3.1.11, it follows that the orthogonal complement of A_{f} under the usual local Tate pairing (on the entire space $H^1(K_v,T) \times H^1(K_v,T)$) is $H^1_{\mathrm{f}}(K_v,T) \oplus A_{\mathrm{tr}}$, and likewise the complement of A_{tr} is $A_{\mathrm{f}} \oplus H^1_{L-\mathrm{tr}}(K_v,T)$.

4 Kolyvagin systems

4.1 Kolyvagin numbers

From this section onward, K is an imaginary quadratic field whose discriminant is different from -3 and -4, so that $\mathcal{O}_K^\times = \{\pm 1\}$. We furthermore assume that R is a local ring with maximal ideal $\mathfrak{m}$, and as before, that T is an $R[G_K]$-module that is finitely generated over R and unramified at all but finitely many places.

Definition 4.1.1. Denote by $\mathcal{L}_0 = \mathcal{L}_0(T)$ the set of rational primes $\ell \neq p$ inert in K at which T is unramified. We will often confuse $\ell \in \mathcal{L}_0$ with the prime $\lambda = \ell\mathcal{O}_K$ above it, and write $K_\ell = K_\lambda$ for the completion of K at λ.

i) For each $\lambda \mid \ell \in \mathcal{L}_0$, define I_ℓ to be the smallest ideal of R such that $\ell + 1 \in I_\ell$ and the Frobenius element $\mathrm{Fr}_\lambda \in \mathrm{Gal}(K_\lambda^{\mathrm{unr}}, K_\lambda)$ acts trivially on $T/I_\ell T$.

ii) For each $k \in \mathbb{Z}_{>0}$, define $\mathcal{L}_k = \mathcal{L}_k(T) := \{\ell \in \mathcal{L}_0 : I_\ell \subset \mathfrak{m}^k\}$.

iii) For each $\lambda \mid \ell \in \mathcal{L}_0$, let $G_\ell := k_\lambda^\times / k_\ell^\times$, where $k_\ell \cong \mathbb{F}_\ell$ and $k_\lambda \cong \mathbb{F}_{\ell^2}$ are the residue fields of $\mathbb{Q}$ and K at ℓ and λ, respectively.

iv) Let $\mathcal{N}_k$ be the set of squarefree products of the primes in $\mathcal{L}_k$. For $n \in \mathcal{N}_0$, define

$$I_n := \sum_{\ell \mid n} I_\ell, \quad G_n := \bigotimes_{\ell \mid n} G_\ell.$$

By convention, $1 \in \mathcal{N}_k$ for every k, and $I_1 = 0$ and $G_1 = \mathbb{Z}$.

Definition 4.1.2. A Selmer triple $(T, \mathcal{F}, \mathcal{L})$ (over K) is a choice of module T and Selmer structure $\mathcal{F}$ on T (over K), together with a subset $\mathcal{L} \subset \mathcal{L}_0$ disjoint from $\Sigma(\mathcal{F})$. Denote by $\mathcal{N} = \mathcal{N}(\mathcal{L})$ the set of squarefree products of primes in $\mathcal{L}$, with the usual convention that $1 \in \mathcal{N}$.

4.2 A choice of transverse condition

In this subsection we establish a canonical choice of maximal totally tamely ramified p-extension L/K_ℓ for every $\ell \in \mathcal{L}_0$. This in turn gives us a canonical choice of L-transverse condition as defined in Example 3.1.2, which we may unambiguously refer to as $H^1_{\mathrm{tr}}(K_\ell, T)$.

The reader is assumed to be familiar with the basic notions and results from class field theory as described in e.g. [Cox89, Chapter Two] and [Neu99, IV–VI]. The most important facts may be summarized as follows.

Theorem-Definition 4.2.1 (Ring class fields)**.** *Let $n \in \mathbb{Z}_{>0}$, and denote by $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ the order of conductor n. The ring class field $K[n]/K$ of conductor n has the following properties:*

i) *The extension $K[n]/K$ is abelian and unramified outside (the primes dividing) n;*

ii) *There is a canonical isomorphism $\mathrm{Gal}(K[n]/K) \cong \mathrm{Pic}(\mathcal{O}_n)$, called the Artin map, under which the primes of $\mathcal{O}_n$ correspond to their respective Frobenius elements in $\mathrm{Gal}(K[n]/K)$. The Artin map is functorial in the sense that if $m \mid n$, then*

$$\begin{array}{ccc} \mathrm{Gal}(K[n]/K) & \xrightarrow{\sim} & \mathrm{Pic}(\mathcal{O}_n) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K[m]/K) & \xrightarrow{\sim} & \mathrm{Pic}(\mathcal{O}_m) \end{array}$$

commutes.

In particular, the Hilbert class field $K[1]$ with $\mathrm{Gal}(K[1]/K) \cong \mathrm{Pic}(\mathcal{O}_K)$ is the maximal unramified abelian extension of K.

Lemma 4.2.2. *Let L/K be a finite Galois extension, λ a prime of K, and Λ one of its extensions in L. Then λ is totally split in L if and only if $L_\Lambda = K_\lambda$. In particular, $K[1]_\Lambda = K_\lambda$ if and only if λ is principal.*

Proof. Clearly $L_\Lambda = K_\lambda$ if and only if $\mathrm{Gal}_\Lambda(L/K) = \mathrm{Gal}(L_\Lambda/K_\lambda) = 1$. Now the discussion after [Neu99, I.9.2] tells us that $\mathrm{Gal}_\Lambda(L/K) = 1$ if and only if λ is totally split in L. The corollary follows from [Cox89, 5.25]: a prime is totally split in the Hilbert class field if and only if it is principal. □

In particular, if $\lambda \mid \ell \in \mathcal{L}_0$, we may unambiguously write $K[1]_\lambda = K[1]_\Lambda$ for any prime $\Lambda \mid \lambda$ of $K[1]$. Furthermore, since $K[1]$ is the maximal unramified abelian extension of K and $K[\ell]/K$ is unramified outside λ, $K[\ell]/K[1]$ is totally ramified at any such Λ; we continue our abuse of notation by writing $K[\ell]_\lambda$ for the completion of $K[\ell]$ at the unique place dividing any prime $\Lambda \mid \lambda$ of $K[1]$.

Proposition 4.2.3. *Let $\lambda \mid \ell \in \mathcal{L}_0$. The maximal p-subextension of $K[\ell]_\lambda/K_\lambda$, denoted by L, is a maximal totally tamely ramified abelian p-subextension of $K[\ell]_\lambda/K_\lambda$. Here, L/K_λ being totally ramified means that for each prime Λ of L extending λ, we have that L_Λ/K_λ is totally ramified.*

Proof. Since $K[\ell]/K$ is abelian, it is clear that L/K_λ is also abelian. From our earlier observation that $K[\ell]/K[1]$ is totally ramified at any prime dividing λ, it follows that $K[\ell]_\lambda/K[1]_\lambda$ is totally ramified, so $K[\ell]_\lambda/K_\lambda$ is totally ramified. From this it is apparent that L is totally ramified, and since $[L : K_\lambda]$ is a power of $p \neq \ell$, this ramification is tame. □

Proposition 4.2.3 gives us, for each $\ell \in \mathcal{L}_0$, a choice of L/K_ℓ which we use to define the transverse local condition $H^1_{\mathrm{tr}}(K_\ell, T) := H^1_{L-\mathrm{tr}}(K_\ell, T)$. Next we investigate the Galois group $\mathrm{Gal}(L/K_\ell)$, starting with the Galois group of $K[\ell]/K[1]$.

Proposition 4.2.4. *For any $\lambda \mid \ell \in \mathcal{L}_0$ we have isomorphisms*

$$\mathrm{Gal}(K[\ell]/K[1]) \cong \frac{(\mathcal{O}_K/\lambda)^\times}{(\mathbb{Z}/\ell\mathbb{Z})^\times} \cong G_\ell.$$

Proof. From [Neu99, I.12.12] and preceding results, we have an exact sequence

$$1 \longrightarrow \frac{\mathcal{O}_K^\times}{\mathcal{O}_\ell^\times} \longrightarrow \frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^\times}{(\mathcal{O}_\ell/\ell\mathcal{O}_\ell)^\times} \longrightarrow \mathrm{Pic}(\mathcal{O}_\ell) \longrightarrow \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 1.$$

From our assumption that $\mathcal{O}_K^\times = \{\pm 1\}$ it follows that $\mathcal{O}_K^\times/\mathcal{O}_\ell^\times = 1$, reducing the above exact sequence to the top row of

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \dfrac{(\mathcal{O}_K/\ell\mathcal{O}_K)^\times}{(\mathcal{O}_\ell/\ell\mathcal{O}_\ell)^\times} & \longrightarrow & \mathrm{Pic}(\mathcal{O}_\ell) & \longrightarrow & \mathrm{Pic}(\mathcal{O}_K) & \longrightarrow & 1 \\ & & & & \downarrow \wr & & \downarrow \wr & & \\ 1 & \longrightarrow & \mathrm{Gal}(K[\ell]/K[1]) & \longrightarrow & \mathrm{Gal}(K[\ell]/K) & \longrightarrow & \mathrm{Gal}(K[1]/K) & \longrightarrow & 1, \end{array}$$

where the vertical isomorphisms are the isomorphisms from Theorem-Definition 4.2.1(ii). By the functoriality of the Artin map, the above square commutes, and hence

$$\mathrm{Gal}(K[\ell]/K[1]) \cong \frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^\times}{(\mathcal{O}_\ell/\ell\mathcal{O}_\ell)^\times}.$$

Now, $\lambda = \ell\mathcal{O}_K$ and $\mathcal{O}_\ell = \mathbb{Z} + \ell\mathcal{O}_K$, which modulo ℓ reduces to $\mathbb{Z}/\ell\mathbb{Z}$. This yields the first isomorphism we were after. The second isomorphism is almost by definition, cf. [AM69, 10.15(ii)]. □

Lemma 4.2.5. *Let L/K be any Galois extension of number fields and let λ be a prime of K. If λ does not split in L, then the inclusion $\mathrm{Gal}(L_\lambda/K_\lambda) \to \mathrm{Gal}(L/K)$, where L_λ denotes the completion with respect to the unique place above λ, is an isomorphism.*

Proof. Since λ has a unique extension to L, [Neu99, II.8.4] tells us that

$$|\,\mathrm{Gal}(L/K)| = [L : K] = [L_\lambda : K_\lambda] = |\,\mathrm{Gal}(L_\lambda/K_\lambda)|,$$

and hence our injection must be a bijection. □

Proposition 4.2.6. *Let $\lambda \mid \ell \in \mathcal{L}_0$ and L as described in Proposition 4.2.3. Then $\mathrm{Gal}(L/K_\lambda)$ is isomorphic to the p-Sylow subgroup of G_ℓ.*

Proof. Since L is the p-maximal subextension of $K[\ell]_\lambda/K[1]_\lambda$,

$$\mathrm{Gal}(L/K_\lambda) \cong \frac{\mathrm{Gal}(K[\ell]_\lambda/K_\lambda)}{\mathrm{Gal}(K[\ell]_\lambda/L)}$$

is by the fundamental theorem of finite abelian groups isomorphic to a subgroup of $\mathrm{Gal}(K[\ell]_\lambda/K_\lambda)$, and its order is the largest power of p dividing $|\mathrm{Gal}(K[\ell]_\lambda/K_\lambda)|$; that just means that $\mathrm{Gal}(L/K_\lambda)$ is isomorphic to a p-Sylow subgroup of $\mathrm{Gal}(K[\ell]_\lambda/K_\lambda)$.

By Lemma 4.2.2, $\mathrm{Gal}(K[\ell]_\lambda/K_\lambda) = \mathrm{Gal}(K[\ell]_\lambda/K[1]_\lambda)$; since $K[\ell]/K[1]$ is totally ramified at any prime above λ, Lemma 4.2.5 shows that $\mathrm{Gal}(L/K_\lambda)$ is isomorphic to a p-Sylow subgroup of $\mathrm{Gal}(K[\ell]/K[1])$. Proposition 4.2.4 gives us the final isomorphism. □

4.3 Kolyvagin systems

Fix a Selmer triple $(T, \mathcal{F}, \mathcal{L})$ and let $\mathcal{N} = \mathcal{N}(\mathcal{L})$. From this Selmer triple we can construct a new Selmer triple as follows.

Definition 4.3.1. For any $abc \in \mathcal{N}$, define the Selmer structure $\mathcal{F}_b^a(c)$ by

$$H^1_{\mathcal{F}_b^a(c)}(K_v, T) := \begin{cases} H^1_{\mathcal{F}}(K_v, T) & \text{if } v \nmid abc; \\ H^1_{\mathrm{rel}}(K_v, T) = H^1(K_v, T) & \text{if } v \mid a; \\ H^1_{\mathrm{str}}(K_v, T) = 0 & \text{if } v \mid b; \\ H^1_{\mathrm{tr}}(K_v, T) & \text{if } v \mid c, \end{cases}$$

where the final condition is the transverse condition described in Section 4.2. Naturally, $\Sigma(\mathcal{F}_b^a(c))$ is $\Sigma(\mathcal{F})$ together with all prime divisors of abc, and we set $\mathcal{L}(abc)$ to be $\mathcal{L}$ with all prime divisors of abc removed. This gives a Selmer triple $(T, \mathcal{F}_b^a(c), \mathcal{L}(abc))$. If any one of a, b, or c is 1, we omit it from the notation.

Lemma 4.3.2. *The dual Selmer structure of $\mathcal{F}_b^a(c)$ is $(\mathcal{F}_b^a(c))^* = (\mathcal{F}^*)_a^b(c)$.*

Proof. This is immediate from Definition 4.3.1 and Proposition 3.1.10, which states that $H^1_{\mathrm{tr}}(K_v, T)$ and $H^1_{\mathrm{tr}}(K_v, T^*)$ are orthogonal complements. □

Using Definition 4.1.1 and Proposition 4.2.6 together with Proposition 3.1.7, we find for any $n\ell \in \mathcal{N}_0$ the finite-singular isomorphism

$$\phi_\ell^{\mathrm{fs}} \colon H^1_{\mathrm{f}}(K_\ell, T/I_{n\ell}T) \xrightarrow{\sim} H^1_{\mathrm{s}}(K_\ell, T/I_{n\ell}T) \otimes G_\ell.$$

This gives rise to the following diagram, which we use to define one of the fundamental objects of this thesis.

$$\begin{array}{ccccc} & & & & H^1_{\mathcal{F}(n)}(K, T/I_nT) \otimes G_n \\ & & & & \downarrow{\scriptstyle \mathrm{loc}_\ell \otimes 1} \\ & & & & H^1_{\mathrm{f}}(K_\ell, T/I_nT) \otimes G_n \\ & & & & \downarrow \\ & & & & H^1_{\mathrm{f}}(K_\ell, T/I_{n\ell}T) \otimes G_n \\ & & & & \downarrow{\scriptstyle \phi_\ell^{\mathrm{fs}} \otimes 1} \\ H^1_{\mathcal{F}(n\ell)}(K, T/I_n\ell T) \otimes G_{n\ell} & \xrightarrow{\mathrm{loc}_\ell \otimes 1} & H^1_{\mathrm{tr}}(K_\ell, T/I_{n\ell}T) \otimes G_{n\ell} & \xrightarrow{\sim} & H^1_{\mathrm{s}}(K_\ell, T/I_{n\ell}T) \otimes G_{n\ell} \end{array} \tag{4.1}$$

Definition 4.3.3 (Kolyvagin systems)**.** A Kolyvagin system $\kappa = (\kappa_n : n \in \mathcal{N})$ for $(T, \mathcal{F}, \mathcal{L})$ is a collection of cohomology classes

$$\kappa_n \in H^1_{\mathcal{F}(n)}(K, T/I_nT) \otimes G_n$$

such that, for any $n\ell \in \mathcal{N}$, the images of κ_n and $\kappa_{n\ell}$ along the maps in (4.1) agree. Here, the second vertical map is induced by the projection $T/I_nT \to T/I_{n\ell}T$ and the second horizontal map is the isomorphic projection from Proposition 3.1.10. We denote the set of all Kolyvagin systems for $(T, \mathcal{F}, \mathcal{L})$ by $\mathbf{KS}(T, \mathcal{F}, \mathcal{L})$.

Remark 4.3.4. As discussed in Remark 3.1.8, the tensor products with G_n (and $G_{n\ell}$) in (4.1) are there only to ensure that the maps, in particular ϕ^{fs}_ℓ, are canonical. By choosing a generator of G_ℓ for every $\ell \mid n$, we may and often will identify κ_n with an element of $H^1_{\mathcal{F}(n)}(K, T/I_nT)$.

5 Notation and hypotheses

We fix the following notation throughout the remainder of this thesis.

K	an imaginary quadratic field of discriminant $\neq -3, -4$.
τ	a complex conjugation in $G_{\mathbb{Q}}$.
R	a complete, Noetherian local ring with finite residue field.
$\mathfrak{m}$	the maximal ideal of $\mathfrak{m}$.
$v_{\mathfrak{m}}$	the $\mathfrak{m}$-adic valuation on R; $v_{\mathfrak{m}}(x)$ is the maximal integer t for which $x \in \mathfrak{m}^t$.
p	the characteristic of $R/\mathfrak{m}$.
T	an $R[G_K]$-module that is finitely generated as R-module.
$\mathcal{F}$	a Selmer structure on T over K.
$\mathcal{L}$	a subset of $\mathcal{L}_0(T)$, disjoint from $\Sigma(\mathcal{F})$; cf. Definition 4.1.1.
$\mathcal{N}$	$= \mathcal{N}(\mathcal{L})$, the set of squarefree products of primes in $\mathcal{L}$, including 1.

In particular, $(T, \mathcal{F}, \mathcal{L})$ is a Selmer triple as defined in Definition 4.1.2. As we saw in Section 4, the requirement that the discriminant of K is different from -3 and -4 simply means that $\mathcal{O}_K^\times = \{\pm 1\}$, which was used to choose a canonical transverse condition as described in Proposition 4.2.3. We will frequently write

$$\bar{T} := T/2\mathfrak{m}T = T/\mathfrak{m}^{1+v_{\mathfrak{m}}(2)}T,$$

which may be viewed as the smallest quotient of T on which $+1$ and -1 do not act identically; we will often choose T to be large enough for that interpretation to make sense. If $p > 2$, then $\bar{T} = T/\mathfrak{m}T$ is an $R/\mathfrak{m}$-vector space, but if $p = 2$ then $\bar{T}$ is only an $R/2\mathfrak{m}$-module. In either case, $2\bar{T} \cong T/\mathfrak{m}T$ is an $R/\mathfrak{m}$-vector space.

5.1 Hypotheses on T

The motivating example to keep in mind during our discussions comes from the p-torsion of some elliptic curve E: in Section 6, T may be taken as the module of p^k-torsion points over $\mathbb{Z}/p^k\mathbb{Z}$, and in Section 7 as the p-adic Tate module over $\mathbb{Z}_p$. This motivates the first and most common of our assumptions.

$$T \text{ is a free } R\text{-module of rank 2.} \tag{free}$$

In Section 8, we will assume that the representation $G_K \to T$ is surjective, but most of our results hold under a weaker assumption:

$$\text{The action of } G_K \text{ on } 2\bar{T} \text{ defines an irreducible representation of } G_K \to \mathrm{Aut}(2\bar{T}). \tag{irred}$$

This means that the only $R/\mathfrak{m}$-subspaces of $2\bar{T}$ that are stable under the action of G_K are 0 and $2\bar{T}$: if S is a subspace of $2\bar{T}$ such that $\sigma(S) \subset S$ for all $\sigma \in G_K$, then S is either 0 or $2\bar{T}$. It should be noted that in his original text, Howard makes the stronger assumption that the representation is *absolutely* irreducible, but this is not necessary for our purposes.

The next hypothesis is harder to motivate, and will only be used in the proof of Proposition 7.1.6.

$$\text{There is a Galois extension } F/\mathbb{Q} \text{ such that } K \subset F,\ T^{G_F} = T, \text{ and } 2H^1(F(\mu_{p^\infty})/K, \bar{T}) = 0. \tag{Gal}$$

In Section 8, we will show that $F = K(E[p^\infty])$ has the desired properties.

5.2 Hypotheses on $\mathcal{F}$

Recall the notions of functorial and cartesian local conditions from Definition 3.1.3. It is convenient to assume that the local conditions of $\mathcal{F}$ have these properties on the category from Definition 3.1.6:

$$\text{At every place of } K, \text{ the local condition } \mathcal{F} \text{ is cartesian on } \mathrm{Quot}(T). \tag{cart}$$

By Lemma 3.1.5, the finite condition is always cartesian on $\mathrm{Quot}(T)$, so in order to verify (cart) it suffices to check that $\mathcal{F}$ is cartesian at all places in $\Sigma(\mathcal{F})$.

The next assumption is motivated by Example 3.2.6:

$$\begin{gathered}\text{There is a perfect, symmetric, } R\text{-bilinear pairing } (\cdot,\cdot)\colon T\times T\to R(1).\\ \text{For all } \sigma\in G_K \text{ and } s,t\in T, \text{ we have } (\sigma s,(\tau\sigma\tau)t)=\sigma(s,t).\\ \text{At any place of } K,\ (\cdot,\cdot) \text{ induces the local Tate pairing; } T\cong T^* \text{ and } \mathcal{F}=\mathcal{F}^*.\end{gathered}\tag{dual}$$

Hypothesis (dual) may seem rather contrived, but the only part that is of significance to us is the self-duality of $\mathcal{F}$, cf. Definition 3.1.9. The pairing $(\cdot,\cdot)$ is only needed for a structure result that we will not discuss in detail, and the only time we need to verify its existence is in the example below.

Example 5.2.1. Let E be an elliptic curve defined over $\mathbb{Q}$, denote its p-adic Tate module by $T=T_p(E)$, and recall (from e.g. [Sil08, III.8]) that we have a $\mathbb{Z}_p$-bilinear, alternating, nondegenerate, Galois-invariant Weil pairing $e\colon T\times T\to\mathbb{Z}_p(1)$. Define a new pairing $(\cdot,\cdot)\colon T\times T\to\mathbb{Z}_p(1)$ by $(s,t):=e(s,\tau t)$. This pairing is clearly $\mathbb{Z}_p$-bilinear, and, using that the p-adic cyclotomic character of τ is $\chi_p(\tau)=-1$, we have

$$(s,t)=e(s,\tau t)=\chi_p(\tau)e(\tau s,t)=-\chi_p(\tau)e(t,\tau s)=e(t,\tau s)=(t,s)$$

as well as

$$(\sigma s,(\tau\sigma\tau)t)=e(\sigma s,(\sigma\tau)t)=\chi_p(\sigma)e(s,\tau t)=\chi_p(\sigma)(s,t)$$

for all $s,t\in T$ and $\sigma\in G_K$. It is immediate that $(\cdot,\cdot)$ is perfect because the Weil pairing is perfect: the Weil pairing on $E[p^k]$ is non-degenerate and hence perfect because $\mathrm{Hom}(E[p^k],\mathbb{Z}/p^k\mathbb{Z})\cong E[p^k]$ is finite; passing to the inverse limit shows that e itself is also perfect.

The local pairing $H^1(K_v,T)\times H^1(K_v,T)\to\mathbb{Z}_p$ induced by $(\cdot,\cdot)$ is precisely one of the ways to define the local Tate pairing, as done in [Sil08, Exercise 10.24].

5.3 Hypotheses on eigenspaces

Lastly, we encounter our first discrepancy between $p>2$ and $p=2$, given by the following basic result from linear algebra.

Lemma 5.3.1. *Let A be a vector space over a field of characteristic different from 2, let ι be a linear involution on A, and denote the ±1-eigenspaces of ι by $A^\pm$. Then there is a direct sum decomposition*

$$A=A^+\oplus A^-.$$

Proof. Since $\iota^2=1$, it is clear that the only possible eigenvalues of ι are ±1. Any $a\in A$ can be written as $a=a^++a^-$ with $a^\pm:=\frac{1}{2}(a\pm\iota a)\in A^\pm$, and the decomposition follows. □

The involution that we are interested in is the action of $\tau\in G_{\mathbb{Q}}$, which restricts to the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$: we assume that it acts on $\bar{T}$ by postulating that the action of G_K extends to an action of $G_{\mathbb{Q}}$ on $\bar{T}$, and if $p>2$, we want that both eigenspaces $\bar{T}^\pm$ have dimension 1. This precludes the uninteresting possibility that the action of τ is simply given by multiplication by either ±1.

If $p=2$, however, Lemma 5.3.1 fails for the obvious reason that we cannot divide by 2, and because ±1 would act identically on the vector space. This latter point is why we defined $\bar{T}$ to be an $R/2\mathfrak{m}$-module rather than an $R/\mathfrak{m}$-vector space, so that ±1 typically do act differently and we may still obtain useful information about τ from its eigenspaces.

As in Lemma 5.3.1, we will generally refer to the submodules of an $(R/2\mathfrak{m})[G_{\mathbb{Q}}]$-module A on which τ acts by ±1 as the ±1-eigenspaces, and denote them by $A^\pm$. A similar argument to our proof of Lemma 5.3.1 then yields an inclusion

$$2A\subset A^++A^-,\tag{5.1}$$

even when $p=2$.

Example 5.3.2. In order to illustrate that there is no nicer relation between a $G_{\mathbb{Q}}$-module and its eigenspaces under τ than (5.1), let A_1, A_2 and A_3 denote the same underlying $\mathbb{Z}/4\mathbb{Z}$-module given by $(\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$, and let τ act on A_1 by $\tau(x,y,z) = (x+2y+2z, x+y, x+z)$, on A_2 by $\tau(x,y,z) = (x, x+y, x+z)$ and on A_3 by $\tau(x,y,z) = (x,z,y)$. Then

$$A_1^+ = A_1^- = \langle (2,0,0), (0,1,1) \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}),$$

$$A_2^+ = A_2^- = \langle (2,0,0), (0,1,0), (0,0,1) \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}),$$

$$A_3^+ = \langle (1,0,0), (0,1,1) \rangle \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}),$$

$$A_3^- = \langle (2,0,0), (0,1,1) \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$$

as $\mathbb{Z}/4\mathbb{Z}$-modules. In contrast to the scenario in Lemma 5.3.1, we have $A_i^+ \cap A_i^- \neq 0$ for all i, and for no i do the lengths of the eigenspaces add up to the length of A_i. We will see that it may be useful to instead consider the $\mathbb{F}_2$-vector spaces $2A_i^{\pm} = 2(A_i^{\pm})$ as subspaces of $2A_i$, but in that case there does not seem to be a meaningful pattern either: $2A_i \cong \mathbb{F}_2$, but $2A_1^+ = 2A_1^- = 2A_2^+ = 2A_2^- = 2A_3^- = 0$ and $2A_3^+ \cong \mathbb{F}_2$.

Through trial and error, we have found that the following assumptions on the actions of τ are sufficient for our purposes:

The action of G_K on $\bar{T}$ extends to an action of $G_{\mathbb{Q}}$, and $\bar{T}^{\pm}$ are free $R/2\mathfrak{m}$-modules of rank 1.
$H^1_{\mathcal{F}}(K, \bar{T})$ is stable under the action of $G_{\mathbb{Q}}$. (eigen)

The final assumption in (eigen) means that the G_K-action on $H^1_{\mathcal{F}}(K, \bar{T})$ extends to an action of $G_{\mathbb{Q}}$, so that we may consider the eigenspaces $H^1_{\mathcal{F}}(K, \bar{T})^{\pm}$ under τ.

Remark 5.3.3. Hypothesis (eigen) generalizes hypotheses H.5(a) and H.5(b) from [How04, 1.3], but does not cover H.5(c). The latter plays no role in obtaining our results, but should be taken into account if one were to investigate how [How04, Section 2] generalizes for $p = 2$.

6 Modules over special principal rings

In addition to our usual assumptions on R listed in Section 5, we will often impose the following condition throughout this section.

$$\begin{gathered} R \text{ is a special principal ring: it is commutative, principal, local and Artinian of length } k. \\ \text{We fix a generator } \pi \text{ of } \mathfrak{m} \text{ and assume that } 2 \neq 0 \text{ in } R \text{ and } \mathcal{L} \subset \mathcal{L}_k(T). \end{gathered} \tag{SPR}$$

The assumption that $2 \neq 0$ ensures that ± 1 are distinct and that $\bar{T}$ is a proper quotient even if $p = 2$. Note also that together with the finiteness of $R/\mathfrak{m}$, (SPR) implies that $R = R/\mathfrak{m}^k$ is itself finite. If (free) is also assumed, then it immediately follows that T is finite as well.

The additional constraint on $\mathcal{L}$ will be motivated later.

Before we study Selmer structures on modules over rings satisfying (SPR), we first state a number of general results for finitely generated modules over special principal rings. These do not require our usual assumptions about the completeness of R and the finiteness of $R/\mathfrak{m}$.

6.1 The structure of finitely generated modules over a special principal ring

The following result generalizes the more famous structure theorem for finitely generated modules over a principal ideal *domain* (e.g. [Lan02, 7.3 and 7.7]) to finitely generated modules over any commutative ring whose ideals are principal, and will be used without proof.

Theorem 6.1.1 (Structure theorem for finitely generated modules over a principal ideal ring, [Bro93, 15.33])**.** *Let A be a finitely generated module over a principal ideal ring R. Then there is a unique $n \in \mathbb{Z}_{\geq 0}$ and an isomorphism*

$$A \cong \bigoplus_{i=1}^{n} (R/d_i R)\,,$$

where each $d_i \in R \setminus R^\times$ such that $d_1 R \subset d_2 R \subset \cdots \subset d_n R$. This decomposition is unique, up to the choice of generators of the ideals $d_i R$.

Corollary 6.1.2 (Structure theorem for finitely generated modules over a special principal ring)**.** *Let R be a special principal ring of length k and A a finitely generated module over R. Then there is a unique $n \in \mathbb{Z}_{\geq 0}$ and an isomorphism*

$$A \cong \bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^{t_i}\right),$$

where $k \geq t_1 \geq t_2 \geq \ldots \geq t_n \geq 1$ are unique.

Proof. This is immediate from Theorem 6.1.1: using that R is also local, we see that each ideal $d_i R = \mathfrak{m}^{t_i}$ for some (necessarily unique) t_i; the fact that R is Artinian gives us the desired bounds on these exponents. □

Corollary 6.1.3. *Let M be a finitely generated module over a special principal ring R; by Corollary 6.1.2, we may write M as a direct sum of m (nonzero) cyclic R-modules. Any submodule A of M is then isomorphic to a direct sum of at most m nonzero cyclic R-modules. In particular, a submodule of a rank-m free R-module is isomorphic to a direct sum of m cyclic R-modules.*

Proof. As in Corollary 6.1.2, denote by k the length of R, and by $\mathfrak{m} = \pi R$ its maximal ideal. We write

$$M \cong \bigoplus_{i=1}^{m} (R/\mathfrak{m}^{s_i})\,.$$

Note that since R is Noetherian and M is finitely generated, A is also finitely generated (cf. [AM69, 6.2 and

6.5], and hence Corollary 6.1.2 gives us an isomorphism

$$A \cong \bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^{t_i}\right).$$

This yields an injection $\bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^{t_i}\right) \to \bigoplus_{i=1}^{m} \left(R/\mathfrak{m}^{s_i}\right)$, and reduces the problem to showing that $n \leq m$. In fact, multiplication by π^{t_i-1} induces an injection $R/\mathfrak{m} \to R/\mathfrak{m}^{t_i}$ and therefore an injection $(R/\mathfrak{m})^n \to \bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^{t_i}\right)$; likewise, we obtain an injection $\bigoplus_{i=1}^{m} \left(R/\mathfrak{m}^{s_i}\right) \to R^m$ and hence an injection $\phi\colon (R/\mathfrak{m})^n \to R^m$.

Notice that for any $x \in (R/\mathfrak{m})^n$, we have $\pi\phi(x) = 0$, which implies that the image of ϕ is contained in $\mathfrak{m}^{k-1}R^m$. Multiplication by π^{k-1} gives an R-module isomorphism $R/\mathfrak{m} \cong \mathfrak{m}^{k-1}$, so the image of ϕ injects into $(R/\mathfrak{m})^m$. This gives us yet another R-linear (and hence $R/\mathfrak{m}$-linear) injection $(R/\mathfrak{m})^n \to (R/\mathfrak{m})^m$; since $R/\mathfrak{m}$ is a field, we know from linear algebra that $n \leq m$. □

Lemma 6.1.4. *Let A be a finitely generated module over a special principal ring R. Then $\mathrm{Hom}_R(A, R) \cong A$.*

Proof. With the notation as in Corollary 6.1.2, we have a chain of isomorphisms

$$\mathrm{Hom}_R(A, R) \cong \mathrm{Hom}_R\left(\bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^{t_i}\right), R\right) \cong \bigoplus_{i=1}^{n} \mathrm{Hom}_R\left(R/\mathfrak{m}^{t_i}, R\right) \cong \bigoplus_{i=1}^{n} \left(R/\mathfrak{m}^{t_i}\right) \cong A,$$

where we used the universal property of the direct sum for the second isomorphism, and

$$\mathrm{Hom}_R\left(R/\mathfrak{m}^{t_i}, R\right) \cong \mathfrak{m}^{k-t_i} \cong R/\mathfrak{m}^{t_i}$$

for the third. □

Proposition 6.1.5. *Let R be a commutative ring, M an R-module equipped with a regular bilinear form $\langle \cdot, \cdot \rangle$, and A a submodule of M. Denoting by $A^\perp$ the orthogonal complement of A under $\langle \cdot, \cdot \rangle$, we have*

$$M/A^\perp \cong \mathrm{Hom}_R(A, R).$$

In particular, if R is a special principal ring and M is finitely generated over R, then $M/A^\perp \cong A$.

Proof. Consider the exact sequence

$$0 \longrightarrow A^\perp \hookrightarrow M \xrightarrow{|_A} \mathrm{Hom}_R(A, R) \longrightarrow 0, \tag{6.1}$$

where $|_A$ denotes the isomorphism $M \cong \mathrm{Hom}_R(M, R)$ induced by $\langle \cdot, \cdot \rangle$, followed by restriction to A. This restriction map $\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(A, R)$ is simply the pullback of the injection $A \hookrightarrow M$ and is therefore surjective; the kernel of $|_A$ is

$$\{m \in M : \langle m, a \rangle = 0 \text{ for all } a \in A\} = A^\perp,$$

so (6.1) is indeed exact. The proposition follows immediately, and the particular case follows from Lemma 6.1.4. Note that A is indeed finitely generated by the same reasoning as in Corollary 6.1.3. □

Proposition 6.1.6. *Let R be a special principal ring and M a finitely generated R-module equipped with a regular alternating bilinear form $\langle \cdot, \cdot \rangle$. Then there exists an R-module A such that $M \cong A \oplus A$.*

Proof. By Theorem 6.1.1 we may assume that M is a direct sum of n nonzero cyclic R-modules. We proceed by induction on n; the claim clearly holds if $n = 0$, so assume that the claim holds for all finitely generated R-modules N that admit a non-degenerate alternating pairing and which are isomorphic to the direct sum of at most $n - 1$ nonzero cyclic R-modules.

Let e be a generator of one of the summands of M, so that $M \cong eR \oplus M/eR$; in particular, we have a projection $\pi\colon M \to eR$ that is left-inverse to the inclusion $eR \hookrightarrow M$. Denoting by $eR^\perp$ the orthogonal

complement of eR under $\langle\cdot,\cdot\rangle$, we also have an exact sequence

$$0 \longrightarrow eR^\perp/eR \hookrightarrow M/eR \xrightarrow{\phi} \mathrm{Hom}_R(eR,R) \longrightarrow 0 \tag{6.2}$$

with $\phi\colon x+eR \mapsto \langle x,\cdot\rangle$; this is well-defined since our pairing is alternating, and has a right inverse defined by sending $f \in \mathrm{Hom}_R(eR,R)$ to the image of $x \in M$ corresponding to $f\pi = \langle x,\cdot\rangle \in \mathrm{Hom}_R(M,R)$. By the splitting lemma, this implies that

$$M/eR \cong \mathrm{Hom}_R(eR,R) \oplus \left(eR^\perp/eR\right)$$

and therefore that

$$M \cong eR \oplus eR \oplus \left(eR^\perp/eR\right) \tag{6.3}$$

by our earier observation and Lemma 6.1.4. By Corollary 6.1.3, $eR^\perp/eR \subset M/eR$ is the direct sum of at most $n-1$ cyclic R-modules; we will show that $\langle\cdot,\cdot\rangle$ induces a regular bilinear form on $eR^\perp/eR$, so that we may invoke our induction hypothesis.

To that end, first notice that since $\langle\cdot,\cdot\rangle$ is alternating, it indeed defines a bilinear form on $eR^\perp/eR$. As for surjectivity of the induced map $eR^\perp/eR \to \mathrm{Hom}_R(eR^\perp/eR,R)$, note that any $f \in \mathrm{Hom}_R(eR^\perp/eR,R)$ lifts to a map $\tilde{f} \in \mathrm{Hom}_R(eR^\perp,R)$ with the property that $\tilde{f}(e)=0$. We already saw that the restriction map $\mathrm{Hom}_R(M,R) \to \mathrm{Hom}_R(eR^\perp,R)$ is surjective, so there exists an $x \in M$ such that $\tilde{f} = \langle x,\cdot\rangle|_{eR^\perp}$. Since $\tilde{f}(e)=0$, it must be that $x \in eR^\perp$, so we indeed have an $x+eR \in eR^\perp/eR$ for which $f = \langle x+eR,\cdot\rangle$.

As for non-degeneracy, $\langle x,\cdot\rangle = 0 \in \mathrm{Hom}(eR^\perp,R)$ if and only if $x \in eR^{\perp\perp}$. We claim that $eR^{\perp\perp} = eR$; by the same reasoning as for (6.2), the exact sequence

$$0 \longrightarrow eR^\perp \hookrightarrow M \xrightarrow{\phi} \mathrm{Hom}_R(eR,R) \longrightarrow 0$$

splits, so $M \cong eR^\perp \oplus \mathrm{Hom}_R(eR,R)$. The universal property of the direct sum asserts that

$$\mathrm{Hom}_R(M,R) \cong \mathrm{Hom}_R(eR^\perp,R) \oplus eR,$$

so $M/eR \cong \mathrm{Hom}_R(M,R)/eR \cong \mathrm{Hom}_R(eR^\perp,R)$. On the other hand, substituting $A = eR^\perp$ into (6.1) gives $M/eR^{\perp\perp} \cong \mathrm{Hom}_R(eR^\perp,R)$, from which we infer that

$$M/eR \cong M/eR^{\perp\perp}.$$

Combined with the general fact that $A \subset A^{\perp\perp}$, it follows that $eR^{\perp\perp} = eR$, finishing the proof that $\langle\cdot,\cdot\rangle$ is non-degenerate and hence regular on $eR^\perp/eR$.

Our induction hypothesis now tells us that there is an R-module A such that $eR^\perp/eR \cong A \oplus A$. Combining this with (6.3) yields

$$M \cong (A \oplus eR) \oplus (A \oplus eR)\,. \qquad \square$$

6.2 The structure of Selmer modules

We will now investigate the consequences of hypothesis (SPR) on the structure of Selmer modules. Firstly, we have an interesting result about the G_K-invariants of T that holds more generally. This corresponds to [MR04, 2.1.4], but Mazur–Rubin's original statement incorrectly claims that $H^0(K,S) = 0$ for any subquotient S of T. The correct statement, which we prove here, is given in the erratum of [MR16].

Lemma 6.2.1. *Suppose that $(T,\mathcal{F},\mathcal{L})$ satisfies (free, irred). Then $H^0(K,T/\mathfrak{m}^iT) = 0$ for any positive integer i. In particular, if furthermore (SPR) is assumed, then $H^0(K,T) = 0$.*

Proof. We will show this by induction. For $i=1$, (irred) tells us that $G_K \to \mathrm{Aut}_{R/\mathfrak{m}}(2\bar{T}) \cong \mathrm{Aut}_{R/\mathfrak{m}}(T/\mathfrak{m}T)$ is an irreducible representation; combined with (free), this implies that the 2-dimensional $R/\mathfrak{m}$-vector space $T/\mathfrak{m}T$ has no 1-dimensional subspace stable under the action of G_K. In particular, there is no nonzero element of $T/\mathfrak{m}T$ that is fixed under the action of G_K, so $H^0(K,T/\mathfrak{m}T) = (T/\mathfrak{m}T)^{G_K} = 0$.

Now suppose that $H^0(K, T/\mathfrak{m}^i T) = 0$ for some i. If $t + \mathfrak{m}^{i+1}T \in H^0(K, T/\mathfrak{m}^{i+1}T)$, then $t + \mathfrak{m}^i T \in H^0(K, T/\mathfrak{m}^i T)$ and hence $t \in \mathfrak{m}^i T$. It therefore suffices to show that $(\mathfrak{m}^i T/\mathfrak{m}^{i+1}T)^{G_K} = 0$.

To that end, T is free by (free), so in particular flat; an elementary exercise in commutative algebra (e.g. [Liu06, 1.2.4], which also discusses the converse) then yields a canonical isomorphism $\mathfrak{m}^i T \cong \mathfrak{m}^i \otimes T$ and hence an isomorphism

$$\frac{\mathfrak{m}^i T}{\mathfrak{m}^{i+1}T} \cong \frac{\mathfrak{m}^i \otimes T}{\mathfrak{m}^{i+1} \otimes T} \cong \left(\mathfrak{m}^i/\mathfrak{m}^{i+1}\right) \otimes T.$$

These isomorphisms respect the G_K-action, so $(\mathfrak{m}^i T/\mathfrak{m}^{i+1}T)^{G_K} \cong ((\mathfrak{m}^i/\mathfrak{m}^{i+1}) \otimes T)^{G_K}$. Using the universal property of the tensor product, one can also show that $(T/\mathfrak{m}T)^d$, with $d = \dim_{R/\mathfrak{m}} \mathfrak{m}^i/\mathfrak{m}^{i+1}$, is isomorphic to $(\mathfrak{m}^i/\mathfrak{m}^{i+1}) \otimes T$, again via a map that preserves the action of G_K. It follows that

$$(\mathfrak{m}^i T/\mathfrak{m}^{i+1}T)^{G_K} \cong \left((\mathfrak{m}^i/\mathfrak{m}^{i+1}) \otimes T\right)^{G_K} \cong \left((T/\mathfrak{m}T)^d\right)^{G_K} = 0,$$

and therefore that $H^0(K, T/\mathfrak{m}^i T) = 0$. The corollary under (SPR) follows from taking $i = k$. □

Lemma 6.2.2 ([MR04, 3.5.4])**.** *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satsfies (SPR, free, irred, cart) and let $i \leq k$ be a non-negative integer. Then multiplication by π^{k-i}, viewed as a homomorphism $T/\mathfrak{m}^i T \to T$, induces an isomorphism*

$$\pi^{k-i} \colon H^1(K, T/\mathfrak{m}^i T) \longrightarrow H^1(K, T)[\mathfrak{m}^i]$$

which restricts to an isomorphism

$$\pi^{k-i} \colon H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T) \longrightarrow H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^i].$$

Proof. The first isomorphism is a consequence of Lemma 6.2.1; the second follows from (cart). As for the first, we have exact sequences

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

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

Using Lemma 6.2.1 for the zeros on the left, Galois cohomology on the above sequences yields

$$0 \longrightarrow H^1(K, T/\mathfrak{m}^i T) \xrightarrow{\pi^{k-i}} H^1(K, T) \longrightarrow H^1(K, T/\mathfrak{m}^{k-i}T)$$

$$0 \longrightarrow H^1(K, T/\mathfrak{m}^{k-i}T) \xrightarrow{\pi^i} H^1(K, T).$$

Now a simple diagram chase shows that $H^1(K, T)[\mathfrak{m}^i] \subset \pi^{k-i}H^1(K, T/\mathfrak{m}^i T)$, yielding our first isomorphism. In order to show that this restricts to an isomorphism on the respective Selmer modules, it now suffices to argue that $\pi^{k-i}H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T) \subset H^1_{\mathcal{F}}(K, T)$ and $(\pi^{k-i})^{-1}H^1_{\mathcal{F}}(K, T) \subset H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T)$.

The first inclusion follows by definition: a class $[\xi] \in H^1(K, T/\mathfrak{m}^i T)$ lives in $H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T)$ if and only if for each place v of K, $\mathrm{loc}_v[\xi] = [\xi|_{G_{K_v}}] \in H^1_{\mathcal{F}}(K_v, T/\mathfrak{m}^i T)$, where the local condition $\mathcal{F}$ on $T/\mathfrak{m}^i T$ is the local condition $\mathcal{F}$ on T propagated through the projection $\pi_i \colon T \to T/\mathfrak{m}^i T$. In other words, $[\xi] \in H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T)$ precisely when, for each place v, we have $[\xi|_{G_{K_v}}] = [\pi_i \chi_v]$ for some $[\chi_v] \in H^1_{\mathcal{F}}(K_v, T)$.

Hence, for any $[\xi_v] \in H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T)$, we have for any v that

$$\mathrm{loc}_v[\pi^{k-i}\xi] = [\pi^{k-i}\xi|_{G_{K_v}}] = [\pi^{k-i}\pi_i\chi_v] = [\pi^{k-i}\chi_v] = \pi^{k-i}[\chi_v]$$

for some $\chi_v \in H^1_{\mathcal{F}}(K_v, T)$. Since $H^1_{\mathcal{F}}(K_v, T)$ is an R-submodule of $H^1(K_v, T)$, it follows that $[\pi^{k-i}\xi] \in H^1_{\mathcal{F}}(K, T)$, proving the first inclusion we were after.

As for the second inclusion, by the definition of Quot(T) (Definition 3.1.6), $\pi^{k-i} \colon T/\mathfrak{m}^i T \to T$ is an (injec-

tive) morphism in $\mathrm{Quot}(T)$. Thefore, since (cart) assumes that $\mathcal{F}$ is Cartesian on $\mathrm{Quot}(T)$ at each place v of K, the local condition $\mathcal{F}$ at any such v on $T/\mathfrak{m}^iT$ (propagated through π_i as described earlier) is the same as the local condition propagated through π^{k-i}. More concretely,

$$H^1_{\mathcal{F}}(K_v, T/\mathfrak{m}^iT) = (\pi^{k-i})^{-1}H^1_{\mathcal{F}}(K_v, T)$$

at every place v. The global inclusion now follows directly from spelling out the definitions of $H^1_{\mathcal{F}}(K,T)$ and $H^1_{\mathcal{F}}(K, T/\mathfrak{m}^iT)$. □

Although we have not made use of it thus far, hypothesis (SPR) also assumes that $\mathcal{L} \subset \mathcal{L}_k(T)$. This allows us to use the following result.

Lemma 6.2.3. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR). Then $H^1_{\mathrm{f}}(K_\ell, T) \cong H^1_{\mathrm{tr}}(K_\ell, T) \cong T$ for all $\ell \in \mathcal{L}$. If moreover (free) is assumed, then $H^1_{\mathrm{f}}(K_\ell, T)$ and $H^1_{\mathrm{tr}}(K_\ell, T)$ are both free R-modules of rank 2; it follows that $H^1_{\mathrm{f}}(K_\ell, T/\mathfrak{m}^iT)$ and $H^1_{\mathrm{tr}}(K_\ell, T/\mathfrak{m}^iT)$ with $0 < i \leq k$ are free $R/\mathfrak{m}^i$-modules of rank 2, and if furthermore (eigen) is assumed, that $H^1_{\mathrm{f}}(K_\ell, \bar{T})^{\pm}$ and $H^1_{\mathrm{tr}}(K_\ell, \bar{T})^{\pm}$ have length $1 + v_{\mathfrak{m}}(2)$.*

Proof. All of this is a direct consequence of the finite-singular isomorphism from Proposition 3.1.7 and Remark 3.1.8, together with the isomorphism $H^1_{\mathrm{tr}}(K_\ell, T) \cong H^1_{\mathrm{s}}(K_\ell, T)$ from Proposition 3.1.10. We simply need to verify the conditions that are necessary to reply those results.

Let $\lambda \mid \ell \in \mathcal{L}$. Since $\mathcal{L}$ is disjoint from $\Sigma(\mathcal{F})$, it is immediate that $\lambda \nmid p$ and that T is unramified at λ. The assumption that $\mathcal{L} \subset \mathcal{L}_k(T)$ implies that $I_\ell \subset \pi^k R = 0$, so I_ℓ is trivial. Now, since λ is a prime of degree 2 above ℓ, we have

$$|k_\lambda^\times| = \ell^2 - 1 = (\ell+1)(\ell-1) \in I_\ell$$

by the definition of I_ℓ, so $|k_\lambda^\times| = 0$ in R and hence annihilates T. Lastly, again by definition, Fr_λ acts trivially on $T/I_\ell T = T$, giving rise to the finite-singular isomorphism.

Exploiting that R is principal and Artinian, it can be shown that an R-basis of $H^1_{\mathrm{f}}(K_\ell, T)$ gives an $R/\mathfrak{m}^i$-basis of $H^1_{\mathrm{f}}(K_\ell, T/\mathfrak{m}^iT)$ via the projection $T \to T/\mathfrak{m}^iT$, and likewise for the transverse condition. □

Lemma 6.2.4 ([How04, 1.5.1])**.** *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, irred, Gal, cart, dual, eigen). Then for any $n \in \mathcal{N}$, $(T, \mathcal{F}(n), \mathcal{L}(n))$ satisfies the same hypotheses.*

Proof. Hypotheses (SPR, free, irred, Gal, eigen) directly carry over from $(T, \mathcal{F}, \mathcal{L})$ to $(T, \mathcal{F}(n), \mathcal{L}(n))$. Hypothesis (dual) is immediate from Proposition 3.1.10, so the only nontrivial claim is (cart): proving this amounts to showing that the transverse condition is cartesian on $\mathrm{Quot}(T)$.

To that end, we follow the proof of [MR04, 3.7.4]. We first show that, for any $0 < i \leq k$, propagating the transverse condition on T through the injection $\pi^{k-i}\colon T/\mathfrak{m}^iT \to T$ yields the usual transverse condition on $T/\mathfrak{m}^iT$. We have a commutative diagram

$$\begin{array}{ccc} H^1(K_\ell, T/\mathfrak{m}^iT) & \longrightarrow & H^1_{\mathrm{f}}(K_\ell, T/\mathfrak{m}^iT) \\ \downarrow{\scriptstyle \pi^{k-i}} & & \downarrow{\scriptstyle \pi^{k-i}} \\ H^1(K_\ell, T) & \longrightarrow & H^1_{\mathrm{f}}(K_\ell, T), \end{array} \tag{6.4}$$

where the horizontal maps are projections with respect to the direct sum decomposition from Proposition 3.1.10; the kernels of those maps are precisely the respective transverse conditions. From Lemma 6.2.3 we know that $H^1_{\mathrm{f}}(K_\ell, T/\mathfrak{m}^iT)$ and $H^1_{\mathrm{f}}(K_\ell, T)$ are free $R/\mathfrak{m}^i$- respectively R-modules of rank 2, so the right vertical map in (6.4) is injective.

Suppose that $c \in H^1(K_\ell, T/\mathfrak{m}^iT)$ such that $\pi^{k-i}c \in H^1_{\mathrm{tr}}(K_\ell, T)$. Then $\pi^{k-i}c$ is in the kernel of the bottom map in (6.4), so by the injectivity of the right vertical map, c is in the kernel of the top map. This means that $c \in H^1_{\mathrm{tr}}(K_\ell, T/\mathfrak{m}^iT)$, from which it follows that $(\pi^{k-i})^{-1}H^1_{\mathrm{tr}}(K_\ell, T) \subset H^1_{\mathrm{tr}}(K_\ell, T/\mathfrak{m}^iT)$. The reverse inclusion is clear, so propagating the transverse condition through π^{k-i} indeed yields the transverse condition on $T/\mathfrak{m}^iT$.

The proof is finished once we've argued that $\pi^{k-i}\colon T/\mathfrak{m}^i T \to T$ is essentially the only kind of injection in $\mathrm{Quot}(T)$. Since R is local and principal, its ideals are powers of $\mathfrak{m}$. In particular, any $r \in R$ can be written as $r = u\pi^t$ for some $u \in R^\times$ and some integer $0 \le t \le k$; since $u\colon T/\mathfrak{m}^i T \to T/\mathfrak{m}^i T$ is an isomorphism, we may assume that $u = 1$. For $\pi^t\colon T/\mathfrak{m}^i T \to T/\mathfrak{m}^j T$ to define a map in $\mathrm{Quot}(T)$, we require that $\pi^t \mathfrak{m}^i \subset \mathfrak{m}^j$, so $t + i \ge j$. In fact, for this π^t to be injective, we need that $\pi^t x \in \mathfrak{m}^j T$ only if $x \in \mathfrak{m}^i T$. Clearly, the first condition is equivalent to $x \in \mathfrak{m}^{j-t}$, and it follows that $j - t \ge i$, and hence that $t = j - i$.

Thus the only maps of interest are $\pi^{j-i}\colon T/\mathfrak{m}^i T \to T/\mathfrak{m}^j T$. We already saw that the transverse condition propagated through $\pi^{k-j}\colon T/\mathfrak{m}^j \to T$ is the transverse condition, so propagating the transverse condition through π^{j-i} is the same as propagating through $\pi^{k-j} \circ \pi^{j-i} = \pi^{k-i}$, which we also saw yields the transverse condition on $T/\mathfrak{m}^i T$. □

The following theorem will play an important role in the remainder, but we will refrain from giving a detailed proof due to its technical but uninformative nature.

Theorem 6.2.5. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, irred, cart, dual). Then for any $n \in \mathcal{N}$, there is an $\epsilon(n) \in \{0, 1\}$ and an R-module $M(n)$ such that*

$$H^1_{\mathcal{F}(n)}(K, T) \cong R^{\epsilon(n)} \oplus M(n) \oplus M(n).$$

Proof. Note that by Lemma 6.2.4 it suffices to show this for $H^1_{\mathcal{F}}(K, T)$. Howard does so in [How04, 1.4], by first constructing, for every $s, t \in \mathbb{Z}_{>0}$ with $s + t \le k$, a pairing

$$H^1_{\mathcal{F}}(K, T/\mathfrak{m}^s T) \times H^1_{\mathcal{F}}(K, T/\mathfrak{m}^{k-t} T) \longrightarrow R$$

whose kernel on the left is the image of $H^1_{\mathcal{F}}(K, T/\mathfrak{m}^{s+t} T) \to H^1_{\mathcal{F}}(K, T/\mathfrak{m}^s T)$ and whose kernel on the right is the image of the map $H^1_{\mathcal{F}}(K, T/\mathfrak{m}^{k-s-t} T) \to H^1_{\mathcal{F}}(K, T/\mathfrak{m}^{k-t})$ induced by multiplication by π^s. From this he derives, for each $1 \le s < k$, a regular alternating bilinear form on the $R/\mathfrak{m}$-vector space

$$\frac{H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^s]/\mathfrak{m} H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^{s+1}]}{H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^{s-1}]/\mathfrak{m} H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^s]}.$$

It then follows from Proposition 6.1.6 that this vector space is even-dimensional for each s, from which it can be deduced that $H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^{k-1}]/\mathfrak{m} H^1_{\mathcal{F}}(K, T)$ is a square and hence that

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

for some R-module M and integer ϵ. Without loss of generality, we can assume that $\epsilon \in \{0, 1\}$. □

Note that, although Howard's original result assumes that $p > 2$, the proof of Theorem 6.2.5 is also valid for $p = 2$. However, his method is nonconstructive and tells us nothing about the relations between $\epsilon(n)$ and $\epsilon(n')$ for different $n, n' \in \mathcal{N}$. In the next section we will find that this relation is surprisingly simple when $p > 2$, but we will also encounter the first obstacles that cause Howard's proofs to fail for $p = 2$.

6.3 Eigenspaces

Throughout the remainder of this section, abbreviate the notation from Definition 4.3.1 by

$$\mathcal{H}^a_b(c) := H^1_{\mathcal{F}^a_b(c)}(K, T) \quad \text{and} \quad \bar{\mathcal{H}}^a_b(c) := H^1_{\mathcal{F}^a_b(c)}(K, \bar{T})$$

for any $abc \in \mathcal{N}$; as usual, we omit an index if it is 1. Under the assumptions of (eigen), there is an action of the complex conjugation $\tau \in G_{\mathbb{Q}}$ on $\bar{T}$, which induces an action on $\bar{\mathcal{H}}^a_b(c)$ given by $(\tau\xi)(\sigma) = \tau(\xi(\tau\sigma\tau))$ on cocycles.

Our interest in studying the ± 1-eigenspaces $\bar{\mathcal{H}}^a_b(c)^\pm$ is the main reason we chose to define $\bar{T}$ as $T/2\mathfrak{m}T$: if we simply defined $\bar{T} = T/\mathfrak{m}T$ for $p = 2$, then multiplication by $+1$ and -1 would be identical in $\bar{T}$, and we would have no hope of distinguishing the two eigenspaces $\bar{\mathcal{H}}^a_b(c)^\pm$. By ensuring that $+1$ and -1 are distinct on $\bar{T}$, we may expect more useful information about the action of τ, although we will soon see that this is still not enough to deduce a satisfactory generalization of Howard's original results.

We define $\rho_0^\pm(n) := \operatorname{len} \bar{\mathcal{H}}(n)^\pm$ to be the length of $\bar{\mathcal{H}}(n)^\pm$ as $R/2\mathfrak{m}$-module. As discussed in Section 5.3, for $p > 2$ this is just the $R/\mathfrak{m}$-dimension of the vector space $\bar{\mathcal{H}}(n)^\pm$, and we have that

$$\dim \bar{\mathcal{H}}(n) = \rho_0^+(n) + \rho_0^-(n). \tag{6.5}$$

Proposition 6.3.1. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, dual, eigen) and let $n\ell \in \mathcal{N}$.*

i) *If $\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ then $\rho_0^\pm(n\ell) = \rho_0^\pm(n) - (1 + v_{\mathfrak{m}}(2))$ and $\operatorname{loc}_\ell \bar{\mathcal{H}}(n\ell)^\pm = 0$;*

ii) *If $\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = 0$ then $\rho_0^\pm(n\ell) = \rho_0^\pm(n) + (1 + v_{\mathfrak{m}}(2))$.*

Assuming $p > 2$ in Proposition 6.3.1 recovers [How04, 1.5.3]: by Lemma 6.2.3, $H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ is a one-dimensional $R/\mathfrak{m}$-vector space, so that $\operatorname{loc}_\ell \colon \bar{\mathcal{H}}(n)^\pm \to H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ is surjective precisely when $\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm$ is nontrivial. This reduces the above to

Corollary 6.3.2. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, dual, eigen) and that $p > 2$; let $n\ell \in \mathcal{N}$.*

i) *If $\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm \neq 0$ then $\rho_0^\pm(n\ell) = \rho_0^\pm(n) - 1$ and $\operatorname{loc}_\ell \bar{\mathcal{H}}(n\ell)^\pm = 0$;*

ii) *If $\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = 0$ then $\rho_0^\pm(n\ell) = \rho_0^\pm(n) + 1$.*

Proof of Proposition 6.3.1. We follow the proof of [How04, 1.5.3] very closely; the only difference we need to take into account for our more general setting is that under hypothesis (eigen), the eigenspaces $\bar{T}^\pm$ are not necessarily 1-dimensional $R/\mathfrak{m}$-vector spaces, but free $R/2\mathfrak{m}$-modules of rank 1. As in Example 3.2.6, Hypothesis (dual) gives rise to exact sequences

$$\begin{aligned} 0 \longrightarrow \bar{\mathcal{H}}_\ell(n) \hookrightarrow \bar{\mathcal{H}}(n) \xrightarrow{\operatorname{loc}_\ell} H^1_{\mathrm{f}}(K_\ell, \bar{T}), \\ 0 \longrightarrow \bar{\mathcal{H}}(n) \hookrightarrow \bar{\mathcal{H}}^\ell(n) \xrightarrow{\operatorname{loc}_\ell} H^1_{\mathrm{tr}}(K_\ell, \bar{T}), \end{aligned} \tag{6.6}$$

and the images of the rightmost maps are each other's orthogonal complement under the restriction of the local Tate pairing at ℓ to $H^1_{\mathrm{f}}(K_\ell, \bar{T}) \times H^1_{\mathrm{tr}}(K_\ell, \bar{T})$. By Lemma 6.2.3, the eigenspaces $H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ and $H^1_{\mathrm{tr}}(K_\ell, \bar{T})^\pm$ have length $1 + v_{\mathfrak{m}}(2)$.

i) Suppose that the restriction $\operatorname{loc}_\ell \colon \bar{\mathcal{H}}(n)^\pm \to H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ is surjective. Then the orthogonal complement of its image under the local Tate pairing, restricted to $H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm \times H^1_{\mathrm{tr}}(K_\ell, \bar{T})^\pm$, is 0; by Theorem 3.2.4, this means that $\operatorname{loc}_\ell \colon \bar{\mathcal{H}}^\ell(n)^\pm \to H^1_{\mathrm{tr}}(K_\ell, \bar{T})$ is zero, so $\bar{\mathcal{H}}(n)^\pm = \bar{\mathcal{H}}^\ell(n)^\pm$.

Consider an analogous pair of exact sequences

$$\begin{aligned} 0 \longrightarrow \bar{\mathcal{H}}_\ell(n) \hookrightarrow \bar{\mathcal{H}}(n\ell) \xrightarrow{\operatorname{loc}_\ell} H^1_{\mathrm{tr}}(K_\ell, \bar{T}), \\ 0 \longrightarrow \bar{\mathcal{H}}(n\ell) \hookrightarrow \bar{\mathcal{H}}^\ell(n) \xrightarrow{\operatorname{loc}_\ell} H^1_{\mathrm{f}}(K_\ell, \bar{T}). \end{aligned} \tag{6.7}$$

Since $\operatorname{loc}_\ell \bar{\mathcal{H}}^\ell(n)^\pm = \operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$, it follows from another application of Theorem 3.2.4 that $\operatorname{loc}_\ell \colon \bar{\mathcal{H}}(n\ell)^\pm \to H^1_{\mathrm{tr}}(K_\ell, \bar{T})^\pm$ is zero, proving the second part of **(i)** and implying that $\bar{\mathcal{H}}(n\ell)^\pm = \bar{\mathcal{H}}_\ell(n)^\pm$. Now, the top sequence of (6.6) restricts to a short exact sequence

$$0 \longrightarrow \bar{\mathcal{H}}_\ell(n)^\pm \hookrightarrow \bar{\mathcal{H}}(n)^\pm \xrightarrow{\operatorname{loc}_\ell} H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm \longrightarrow 0$$

which tells us that

$$\operatorname{len} \bar{\mathcal{H}}(n)^\pm = \operatorname{len} \bar{\mathcal{H}}_\ell(n)^\pm + \operatorname{len} H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm.$$

Plugging in $\rho_0^\pm(n) = \operatorname{len} \bar{\mathcal{H}}(n)^\pm$, $\rho_0^\pm(n\ell) = \operatorname{len} \bar{\mathcal{H}}(n\ell)^\pm = \operatorname{len} \bar{\mathcal{H}}_\ell(n)^\pm$ and $\operatorname{len} H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm = 1 + v_{\mathfrak{m}}(2)$ yields the relation in **(i)**.

ii) Now suppose that $\operatorname{loc}_\ell \colon \bar{\mathcal{H}}(n)^\pm \to H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ is zero. Then, again by Theorem 3.2.4, the restriction

$\operatorname{loc}_\ell\colon \bar{\mathcal{H}}^\ell(n)^\pm \to H^1_{\mathrm{tr}}(K_\ell,\bar{T})^\pm$ is surjective, from which it follows that

$$\operatorname{len}\bar{\mathcal{H}}^\ell(n)^\pm = \rho_0^\pm(n) + (1+v_{\mathfrak{m}}(2)).$$

It thus suffices to show that $\bar{\mathcal{H}}^\ell(n)^\pm = \bar{\mathcal{H}}(n\ell)^\pm$. To that end, let $c \in \bar{\mathcal{H}}^\ell(n)^\pm$, and note that $\langle c_v, c_v\rangle_v = 0$ for all $v \neq \ell$ by (dual). Then Lemma 2.3.8 tells us that

$$\langle c_\ell, c_\ell\rangle_\ell = \sum_v \langle c_v, c_v\rangle_v = 0.$$

From the surjectivity of $\operatorname{loc}_\ell\colon \bar{\mathcal{H}}^\ell(n)^\pm \to H^1_{\mathrm{tr}}(K_\ell,\bar{T})^\pm$ we know that the transverse condition is contained in the localization of $H^1_{\mathrm{tr}}(K_\ell,\bar{T})^\pm$ which together with the above and the self-duality of the transverse condition implies that $\bar{\mathcal{H}}^\ell(n)^\pm$ localizes to $H^1_{\mathrm{tr}}(K_\ell,\bar{T})^\pm$, i.e. that $\bar{\mathcal{H}}^\ell(n)^\pm = \bar{\mathcal{H}}(n\ell)^\pm$. This shows **(ii)**. □

6.3.1 The case $v_{\mathfrak{m}}(2) = 1$

Although Proposition 6.3.1 provides some information about the relation between the eigenspaces of $\bar{\mathcal{H}}(n)$ and $\bar{\mathcal{H}}(n\ell)$, it does not cover all possible cases when $p = 2$. In particular, since $H^1_{\mathrm{f}}(K_\ell,\bar{T})^\pm \cong \bar{T}^\pm$ is assumed to have length $1 + v_{\mathfrak{m}}(2) > 1$ under (eigen), it is possible that $\operatorname{loc}_\ell : \bar{\mathcal{H}}(n)^\pm \to H^1_{\mathrm{f}}(K_\ell,\bar{T})^\pm$ is neither zero nor surjective, in which case Proposition 6.3.1 does not give a formula for $\rho_0^\pm(n\ell)$. We can however still obtain a complete description for $\rho_0^\pm(n\ell)$, specifically if we restrict ourselves to the simplest case $v_{\mathfrak{m}}(2) = 1$, that is, where $\pi = 2$.

Proposition 6.3.3. *Suppose that $(T,\mathcal{F},\mathcal{L})$ satisfies (SPR, free, dual, eigen) and that $\pi = 2$; let $n\ell \in \mathcal{N}$.*

- ***i)*** *If $\operatorname{len}\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = 2$, then $\rho_0^\pm(n\ell) = \rho_0^\pm(n) - 2$ and $\operatorname{len}\operatorname{loc}_\ell \bar{\mathcal{H}}(n\ell)^\pm = 0$;*
- ***ii)*** *If $\operatorname{len}\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = 1$, then $\rho_0^\pm(n\ell) = \rho_0^\pm(n)$ and $\operatorname{len}\operatorname{loc}_\ell \bar{\mathcal{H}}(n\ell)^\pm = 1$;*
- ***iii)*** *If $\operatorname{len}\operatorname{loc}_\ell \bar{\mathcal{H}}(n)^\pm = 0$, then $\rho_0^\pm(n\ell) = \rho_0^\pm(n) + 2$.*

Proof. Parts **(i)** and **(iii)** are just the statements of Proposition 6.3.1. In order to show **(ii)**, we fix the following notation. Let $A^\pm \subset H^1(K_\ell,\bar{T})^\pm$ be the localization of $\bar{\mathcal{H}}^\ell(n)^\pm$ at ℓ, and write

$$A^\pm_{\mathrm{f}} := A^\pm \cap H^1_{\mathrm{f}}(K_\ell,\bar{T}), \quad A^\pm_{\mathrm{tr}} := A^\pm \cap H^1_{\mathrm{tr}}(K_\ell,\bar{T}).$$

With the decomposition from Proposition 3.1.10 in mind, let

$$\pi_{\mathrm{f}}\colon H^1(K_\ell,\bar{T}) \to H^1_{\mathrm{f}}(K_\ell,\bar{T}), \quad \pi_{\mathrm{tr}}\colon H^1(K_\ell,\bar{T}) \to H^1_{\mathrm{tr}}(K_\ell,\bar{T})$$

denote the projections onto the finite respectively transverse parts of the cohomology module. It is readily seen that $A^\pm_{\mathrm{f}} = \operatorname{loc}\bar{\mathcal{H}}(n)^\pm$ and $A^\pm_{\mathrm{tr}} = \operatorname{loc}\bar{\mathcal{H}}(n\ell)^\pm$, and that we have exact sequences

$$\begin{aligned} 0 \longrightarrow \bar{\mathcal{H}}(n)^\pm \hookrightarrow \bar{\mathcal{H}}^\ell(n)^\pm \xrightarrow{\operatorname{loc}_\ell} \pi_{\mathrm{tr}}A^\pm \longrightarrow 0, \\ 0 \longrightarrow \bar{\mathcal{H}}(n\ell)^\pm \hookrightarrow \bar{\mathcal{H}}^\ell(n)^\pm \xrightarrow{\operatorname{loc}_\ell} \pi_{\mathrm{f}}A^\pm \longrightarrow 0. \end{aligned} \tag{6.8}$$

Now suppose that $\operatorname{loc}\bar{\mathcal{H}}(n)^\pm$ has length 1. By (eigen) and the above observations, this means that $A^\pm_{\mathrm{f}} = 2H^1_{\mathrm{f}}(K_\ell,\bar{T})$, and it follows from Theorem 3.2.4 on (6.6) that $\pi_{\mathrm{tr}}A^\pm = 2H^1_{\mathrm{tr}}(K_\ell,\bar{T})$. By Proposition 3.1.10 and Corollary 6.1.3, $A^\pm$ is generated by at most two elements. Assuming that $A^\pm$ is cyclic would contradict Theorem 3.2.4 on (6.7), so it must be that $A^\pm = 2H^1(K_\ell,\bar{T}^\pm$ is generated by two elements of order 2. It now follows that $\pi_{\mathrm{f}}A^\pm = 2H^1_{\mathrm{f}}(K_\ell,\bar{T})^\pm$. Plugging this into the sequences in (6.8) yields

$$\operatorname{len}\bar{\mathcal{H}}(n)^\pm = \operatorname{len}\bar{\mathcal{H}}^\ell(n)^\pm - 1 = \operatorname{len}\bar{\mathcal{H}}(n\ell)^\pm,$$

proving **(ii)**. □

6.3.2 The case $v_{\mathfrak{m}}(2) > 1$

One could try to deduce analogous results to Proposition 6.3.3 for $v_{\mathfrak{m}}(2) > 1$, but those would be stated as a list of $(1 + v_{\mathfrak{m}}(2))$-many different cases which may not be particularly enlightening. Instead, we could limit our view to not the entire eigenspace $\bar{\mathcal{H}}(n)^{\pm}$, but its submodule $2\bar{\mathcal{H}}(n)^{\pm} = 2(\bar{\mathcal{H}}(n)^{\pm})$. This is an $R/\mathfrak{m}$-vector space, so allows use to exploit the usual results from linear algebra: $2H^1_{\mathrm{f}}(K_\ell, \bar{T})^{\pm} \cong 2\bar{T}^{\pm}$ is one-dimensional, so the map $\mathrm{loc}_\ell \colon 2\bar{\mathcal{H}}(n)^{\pm} \to 2H^1_{\mathrm{f}}(K_\ell, \bar{T})^{\pm}$ is either zero or surjective.

Although ± 1 are indistinguishable over $R/\mathfrak{m}$, these vector spaces come from the $R/2\mathfrak{m}$-module $\bar{\mathcal{H}}(n)$ in which ± 1 are distinct; therefore, $2\bar{\mathcal{H}}(n)^{+}$ and $2\bar{\mathcal{H}}(n)^{-}$ will generally not be identical and still carry meaningful information about the action of τ on $\bar{\mathcal{H}}(n)$. In particular, we define $\rho_1^{\pm}(n) := \dim 2\bar{\mathcal{H}}(n)^{\pm}$. If $p > 2$, we simply refer to $\rho_0^{\pm} = \rho_1^{\pm}$ as $\rho^{\pm}$.

Now we could seek to prove a generalization of Corollary 6.3.2 that gives a formula of $\rho_1^{\pm}(n\ell)$ in terms of $\rho_1^{\pm}(n)$, depending on whether or not $\mathrm{loc}_\ell 2\bar{\mathcal{H}}(n)^{\pm}$ is zero. However, our proof of Proposition 6.3.1 heavily relied on exact sequences of the form

$$0 \longrightarrow \bar{\mathcal{H}}_\ell(n) \hookrightarrow \bar{\mathcal{H}}(n) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{f}}(K_\ell, \bar{T}),$$

which we used to apply the global duality principle from Theorem 3.2.4. If we were to prove results for $\rho_1^{\pm}$ by adjusting the proof of Proposition 6.3.1 to consider the image of $\mathrm{loc}_\ell \colon 2\bar{\mathcal{H}}(n)^{\pm} \to 2H^1_{\mathrm{f}}(K_\ell, \bar{T})^{\pm}$, we would instead have to work with exact sequences of the form

$$0 \longrightarrow \bar{\mathcal{H}}_\ell(n) \cap 2\bar{\mathcal{H}}(n) \hookrightarrow 2\bar{\mathcal{H}}(n) \xrightarrow{\mathrm{loc}_\ell} 2H^1_{\mathrm{f}}(K_\ell, \bar{T}). \tag{6.9}$$

It should not be understated that in general, $\bar{\mathcal{H}}_\ell(n) \cap 2\bar{\mathcal{H}}(n)$ is different from $2\bar{\mathcal{H}}_\ell(n)$. Clearly, this makes it much harder to use the kernel of $\mathrm{loc}_\ell \colon 2\bar{\mathcal{H}}(n)^{\pm} \to 2H^1_{\mathrm{f}}(K_\ell, \bar{T})^{\pm}$ in any other exact sequence; for instance, whereas the kernel of $\mathrm{loc}_\ell \colon \bar{\mathcal{H}}(n\ell)^{\pm} \to H^1_{\mathrm{tr}}(K_\ell, \bar{T})^{\pm}$ is $\bar{\mathcal{H}}_\ell(n)$, the kernel of the restriction $\mathrm{loc}_\ell \colon 2\bar{\mathcal{H}}(n\ell)^{\pm} \to 2H^1_{\mathrm{tr}}(K_\ell, \bar{T})^{\pm}$ is $\bar{\mathcal{H}}_\ell(n) \cap 2\bar{\mathcal{H}}(n\ell)$, which, again, is not the same as $2\bar{\mathcal{H}}_\ell(n)$.

Moreover, Theorem 3.2.4 only gives us a relation between $\mathrm{loc}_\ell \bar{\mathcal{H}}(n)$ and $\mathrm{loc}_\ell \bar{\mathcal{H}}^\ell(n)$, not between $\mathrm{loc}_\ell 2\bar{\mathcal{H}}(n)$ and $\mathrm{loc}_\ell 2\bar{\mathcal{H}}^\ell(n)$. To make any use of sequences of the form in (6.9), we would need a stronger version of 3.2.4 or apply it in a significantly more careful way than Howard originally did.

6.3.3 Independence of ϵ

Before calling upon more advanced methods, however, one might ask if the information that is encoded in $\rho_0^{\pm}$ and $\rho_1^{\pm}$ is actually useful for our purposes. Unfortunately, the answer is only partly positive: we will encounter these functions again in Section 7, but the main result for which Howard needed his $\rho^{\pm}$ is one that relies on another property that does not hold for $p = 2$.

Conjecture 6.3.4. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, irred, cart, dual, eigen). With the notation from Theorem 6.2.5, $\epsilon(n) = \epsilon$ is independent of $n \in \mathcal{N}$.*

Proof of Conjecture 6.3.4 for $p > 2$. This is [How04, 1.5.5], which states more concretely that $\epsilon(n) \equiv \rho^{+}(n) + \rho^{-}(n) \bmod 2$; the claim then follows from Corollary 6.3.2. By Lemma 6.2.2, we have an isomorphism between the vector spaces $\mathcal{H}(n)[\mathfrak{m}]$ and $\bar{\mathcal{H}}(n)$. Due to Theorem 6.2.5, the dimension of the first is given by

$$\dim \mathcal{H}(n)[\mathfrak{m}] = \dim R^{\epsilon(n)}[\mathfrak{m}] + 2 \dim M(n)[\mathfrak{m}] \equiv \epsilon(n) \bmod 2.$$

As for the latter, we already deduced in (6.5) that $\dim \bar{\mathcal{H}}(n) = \rho^{+}(n) + \rho^{-}(n)$, and the result follows. □

There are several points at which this proof breaks down when $p = 2$. Although we do still have that

$$\operatorname{len} \mathcal{H}(n)[2\mathfrak{m}] = \operatorname{len} R^{\epsilon(n)}[2\mathfrak{m}] + 2 \operatorname{len} M(n)[2\mathfrak{m}] \equiv (1 + v_{\mathfrak{m}}(2))\epsilon(n) \bmod 2,$$

this vanishes if $v_{\mathfrak{m}}(2)$ is odd, giving us no information about $\epsilon(n)$. This could still be remedied by instead considering

$$\dim 2\mathcal{H}(n)[2\mathfrak{m}] = \dim 2R^{\epsilon(n)}[2\mathfrak{m}] + 2\dim M(n)[2\mathfrak{m}] \equiv \epsilon(n) \bmod 2,$$

potentially motivating further investigation into $\rho_1^{\pm}$. However, another key argument in Howard's proof is the equality (6.5), which comes from the splitting $\bar{\mathcal{H}}(n) = \bar{\mathcal{H}}(n)^+ \oplus \bar{\mathcal{H}}(n)^-$ from Lemma 5.3.1. As we already saw in Section 5.3, this splitting is no longer valid when $p = 2$, and we have been unsuccessful in finding a similar relation between $\operatorname{len} \bar{\mathcal{H}}(n)$ and $\rho_0^{\pm}(n)$ or between $\dim 2\bar{\mathcal{H}}(n)$ and $\rho_1^{\pm}(n)$.

We are therefore resigned to leave Conjecture 6.3.4 as a conjecture, and assume it to be true even for $p = 2$ throughout the sequel.

6.4 The stub Selmer module

Recall that, by Theorem 6.2.5, we have under the assumptions of (SPR, free, irred, cart, dual, eigen) and Conjecture 6.3.4 that

$$\mathcal{H}(n) \cong R^{\epsilon} \oplus M(n) \oplus M(n).$$

We write $\lambda_0(n) := \operatorname{len} M(n)$, and define the stub Selmer module as

$$\mathcal{S}_0(n) := \mathfrak{m}^{\lambda_0(n)}\mathcal{H}(n) \cong \mathfrak{m}^{\lambda_0(n)}R^{\epsilon}.$$

This can be thought of as eliminating the square part of $\mathcal{H}(n)$, preserving only a "stub" of the original Selmer module, which is a submodule of R^{ϵ}. Naturally, $\mathcal{S}_0(n) = 0$ if $\epsilon = 0$ or if $\lambda_0(n) \geq k$.

In the spirit of our discussion of $\rho_0^{\pm}$ in the previous section, we aim to find a relationship between $\mathcal{S}_0(n)$ and $\mathcal{S}_0(n\ell)$ for $n\ell \in \mathcal{N}$. As the subscript 0 already indicates, however, we may want to consider alternative generalizations of Howard's stub Selmer module to obtain a stronger result than we managed for $\mathcal{S}_0(n)$. As with $\rho_1^{\pm}$, though, these alternative definitions do not allow us to employ the methods with which Howard proved his findings.

Lemma 6.4.1. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, dual). For any $mn \in \mathcal{N}$, the image of $\mathcal{H}^m(n)$ inside $\bigoplus_{\ell|m} H^1(K_\ell, T)$ is its own orthogonal complement under the sum $\sum_{\ell|m}\langle\cdot,\cdot\rangle_\ell$ of local Tate pairings.*

Proof. This is [How04, 1.5.6]; the proof for Howard's original result is also valid for $p = 2$. Denote by A the image of $\mathcal{H}^m(n)$ in $\oplus_{\ell|m}H^1(K_\ell, T)$, and by $A^\perp$ its orthogonal complement under $\sum_{\ell|m}\langle\cdot,\cdot\rangle_\ell$. Our goal is to prove that $A = A^\perp$; we will do so by first showing that $A \subset A^\perp$ and then that $\operatorname{len} A = \operatorname{len} A^\perp$.

For places $v \nmid m$, we have by Theorem 3.2.4 and (dual) that $H^1_{\mathcal{F}^m(n)}(K_v, T) = H^1_{\mathcal{F}(n)}(K_v, T)$ is its own orthogonal complement under the local Tate pairing. Therefore, for any $c, d \in \mathcal{H}^m(n)$ we have that

$$\sum_{\ell|m}\langle c_\ell, d_\ell\rangle_\ell = \sum_v \langle c_v, d_v\rangle_v = 0$$

by Lemma 2.3.8. This means that $A \subset A^\perp$.

Using the universal property of the direct sum and the fact that the local Tate pairing is perfect, it is easily verified that $\sum_{\ell|m}\langle\cdot,\cdot\rangle_\ell$ is regular on $\oplus_{\ell|m}H^1(K_\ell, T)$; by Proposition 3.1.10 and Lemma 6.2.3, this module is free of rank $4\omega(m)$. We may thus invoke Proposition 6.1.5:

$$\operatorname{len}\left(\bigoplus_{\ell|m} H^1(K_\ell, T)\right) = \operatorname{len} A + \operatorname{len} A^\perp. \tag{6.10}$$

Since R has length k, the left hand side of (6.10) evaluates to $4k\omega(m)$. As for the right hand side, consider

the exact sequences

$$0 \longrightarrow \mathcal{H}(n) \hookrightarrow \mathcal{H}^m(n) \xrightarrow{\oplus_{\ell|m} \mathrm{loc}_\ell} \bigoplus_{\ell|m} H^1_{\mathrm{tr}}(K_\ell, T),$$
$$0 \longrightarrow \mathcal{H}_m(n) \hookrightarrow \mathcal{H}(n) \xrightarrow{\oplus_{\ell|m} \mathrm{loc}_\ell} \bigoplus_{\ell|m} H^1_{\mathrm{f}}(K_\ell, T). \tag{6.11}$$

These are just a generalization of the sequences we saw in Example 3.2.6, and applying Theorem 3.2.4 tells us that the images of the rightmost maps are each other's orthogonal complements under the restriction of $\sum_{\ell|m}\langle\cdot,\cdot\rangle_\ell$ to the product of the top and bottom right modules. More concretely, it follows from the same reasoning as in Example 3.2.6 that

$$\left(\oplus_{\ell|m} \mathrm{loc}_\ell \mathcal{H}^m(n)\right)^\perp = \left(\oplus_{\ell|m} \mathrm{loc}_\ell \mathcal{H}(n)\right) \bigoplus \left(\oplus_{\ell|m} H^1_{\mathrm{tr}}(K_\ell, T)\right) \tag{6.12}$$

Similar to our observations in the proof of Proposition 6.3.3, the top right image in (6.11) is the image of A under the projection $\pi_{\mathrm{tr}}\colon \oplus_{\ell|m} H^1(K_\ell, T) \to \oplus_{\ell|m} H^1_{\mathrm{tr}}(K_\ell, T)$, and the image of the bottom right map is the intersection $A_{\mathrm{f}} := A \cap \oplus_{\ell|m} H^1_{\mathrm{f}}(K_\ell, T)$, that is, the kernel of $\pi_{\mathrm{tr}}|_A$. Hence π_{tr} induces an isomorphism $A/A_{\mathrm{f}} \cong \pi_{\mathrm{tr}} A$, which gives us

$$\mathrm{len}(A) = \mathrm{len}(A_{\mathrm{f}}) + \mathrm{len}(\pi_{\mathrm{tr}} A).$$

Now, combining Proposition 6.1.5 with $\pi_{\mathrm{tr}} A = \oplus_{\ell|m} \mathrm{loc}_\ell \mathcal{H}^m(n)$ and (6.12) yields

$$\begin{aligned} 4k\omega(m) = \mathrm{len}\left(\bigoplus_{\ell|m} H^1(K_\ell, T)\right) &= \mathrm{len}(\pi_{\mathrm{tr}} A) + \mathrm{len}(\pi_{\mathrm{tr}} A)^\perp \\ &= \mathrm{len}(\pi_{\mathrm{tr}} A) + \mathrm{len}(A_{\mathrm{f}}) + \mathrm{len}\left(\oplus_{\ell|m} H^1_{\mathrm{tr}}(K_\ell, T)\right) = \mathrm{len}(A) + 2k\omega(m), \end{aligned}$$

from which we obtain $\mathrm{len}(A) = 2k\omega(m)$. It follows from (6.10) that $\mathrm{len}\, A = \mathrm{len}\, A^\perp$, which finishes the proof that $A = A^\perp$. □

The following three results generalize [How04, 1.5.7–9]. Although our strategy of proof is similar to Howard's, small modifications had to be made for his arguments to apply to the case $p = 2$, causing our results to be generally weaker.

Lemma 6.4.2. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (SPR, free, dual). For any $n\ell \in \mathcal{N}$, there exist $\delta_1, \delta_2 \in \mathbb{Z}_{\geq 0}$ such that*

$$\frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n) + \mathcal{H}(n\ell)} \cong (R/\mathfrak{m}^{\delta_1}) \oplus (R/\mathfrak{m}^{\delta_2}).$$

If either $\delta_i > v_{\mathfrak{m}}(2)$, then $\delta_1 = \delta_2$.

Proof. Localization induces an injection $\mathcal{H}^\ell(n)/\mathcal{H}(n) \to H^1_{\mathrm{tr}}(K_\ell, T)$, whose codomain is free of rank 2 by Lemma 6.2.3. Corollary 6.1.3 then tells us that $\mathcal{H}^\ell(n)/\mathcal{H}(n)$ and hence its quotient $\mathcal{H}^\ell(n)/(\mathcal{H}(n)+\mathcal{H}(n\ell))$ is generated by 2 elements; by Corollary 6.1.2, this means that $\mathcal{H}^\ell(n)/(\mathcal{H}(n) + \mathcal{H}(n\ell)) \cong (R/\mathfrak{m}^{\delta_1}) \oplus (R/\mathfrak{m}^{\delta_2})$.

We will now show that there is an $R/R[2]$-module D such that

$$\frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n) + \mathcal{H}(n\ell)} \Big/ \frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n) + \mathcal{H}(n\ell)}[2] \cong D \oplus D. \tag{6.13}$$

We will do so by constructing a regular, alternating, $R/R[2]$-bilinear form on the left hand module. Since T is finite, $\mathcal{H}^\ell(n)$ and the above quotient is finite by Lemma 3.2.3, so any non-degenerate bilinear form on this quotient is automatically regular.

To that end, let A denote the image of $\mathcal{H}^\ell(n)$ in $H^1(K_\ell, T)$; by Lemma 6.4.1, A is its own orthogonal complement under the local Tate pairing. Denote $A_{\mathrm{f}} := A \cap H^1_{\mathrm{f}}(K_\ell, T)$, $A_{\mathrm{tr}} := A \cap H^1_{\mathrm{tr}}(K_\ell, T)$ and $\bar{A} :=$

$A/(A_{\mathrm{f}}+A_{\mathrm{tr}})$. Then loc_ℓ gives a surjection $\mathcal{H}^\ell(n)\to\bar{A}$ with kernel $\mathcal{H}(n)+\mathcal{H}(n\ell)$, yielding an isomorphism $\mathcal{H}^\ell(n)/(\mathcal{H}(n)+\mathcal{H}(n\ell))\cong\bar{A}$. Under this identification, we may define our pairing on $\bar{A}/\bar{A}[2]$.

Recall the direct sum decomposition from Proposition 3.1.10 and denote for any $x\in A$ the component in (i.e. projection onto) $H^1_{\mathrm{f}}(K_\ell,T)$ by x_{f}, and the component in $H^1_{\mathrm{tr}}(K_\ell,T)$ by x_{tr}. For $x,y\in A$, define $[x,y]:=\langle x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell\in R$, where $\langle\cdot,\cdot\rangle_\ell$ denotes the usual local Tate pairing. The R-bilinearity of this pairing immediately follows from the R-bilinearity of $\langle\cdot,\cdot\rangle_\ell$, but it is worth verifying that it is well-defined on $\bar{A}/\bar{A}[2]$.

As such, suppose that $x\in A_{\mathrm{f}}+A_{\mathrm{tr}}$. Then $x_{\mathrm{f}}\in A$, so for any $y\in A$ we have

$$[x,y]=\langle x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell=\langle x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell+\langle x_{\mathrm{f}},y_{\mathrm{f}}\rangle_\ell=\langle x_{\mathrm{f}},y\rangle_\ell=0$$

by the self-duality of $H^1_{\mathrm{f}}(K_\ell,T)$ and A. The self-duality of $H^1_{\mathrm{tr}}(K_\ell,T)$ allows for an identical argument for the well-definedness in the second component. Now suppose that x represents an element in $\bar{A}[2]$, that is, $2x\in A_{\mathrm{f}}+A_{\mathrm{tr}}$. Then

$$2[x,y]=[2x,y]=0,$$

implying that $[x,y]\in R[2]$ and hence reduces to 0 in $R/R[2]$. An identical argument for the second component shows that $[\cdot,\cdot]$ is well-defined.

As for the alternating property, we again exploit the self-duality of A, $H^1_{\mathrm{f}}(K_\ell,T)$ and $H^1_{\mathrm{tr}}(K_\ell,T)$ to deduce

$$\begin{aligned}0=\langle x,y\rangle_\ell=\langle x_{\mathrm{f}}+x_{\mathrm{tr}},y_{\mathrm{f}}+y_{\mathrm{tr}}\rangle_\ell&=\langle x_{\mathrm{f}},y_{\mathrm{f}}\rangle_\ell+\langle x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell+\langle x_{\mathrm{tr}},y_{\mathrm{f}}\rangle_\ell+\langle x_{\mathrm{tr}},y_{\mathrm{tr}}\rangle_\ell\\&=\langle x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell+\langle y_{\mathrm{f}},x_{\mathrm{tr}}\rangle_\ell=[x,y]+[y,x],\end{aligned}$$

which implies that $2[x,x]=0$, i.e. $[x,x]\in R[2]$.

Lastly, suppose that $x\in A$ such that $[x,y]\in R[2]$ for all $y\in A$. Then

$$0=2[x,y]=[2x,y]=\langle 2x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell=\langle 2x_{\mathrm{f}},y_{\mathrm{tr}}\rangle_\ell+\langle 2x_{\mathrm{f}},y_{\mathrm{f}}\rangle_\ell=\langle 2x_{\mathrm{f}},y\rangle_\ell,$$

which by the self-duality of A implies that $2x_{\mathrm{f}}\in A$. Hence also $2x_{\mathrm{tr}}\in A$, so $2x\in A_{\mathrm{f}}+A_{\mathrm{tr}}$. This means that x is trivial in $\bar{A}/\bar{A}[2]$, and therefore that $[\cdot,\cdot]$ is non-degenerate.

We may now invoke Proposition 6.1.6 to obtain (6.13). Since $\mathcal{H}^\ell(n)/(\mathcal{H}(n)+\mathcal{H}(n\ell))\cong(R/\mathfrak{m}^{\delta_1})\oplus(R/\mathfrak{m}^{\delta_2})$, it follows that D is generated by one element and we may write $D\cong R/\mathfrak{m}^\delta$. If any $\delta_i>v_{\mathfrak{m}}(2)$, then

$$\frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n)+\mathcal{H}(n\ell)}\Big/\frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n)+\mathcal{H}(n\ell)}[2]\neq 0,$$

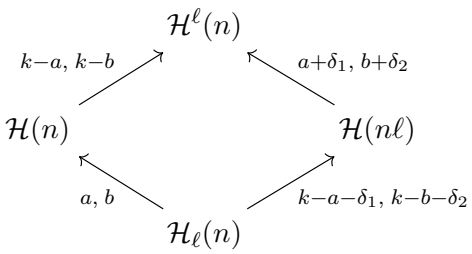
so $\delta>0$. It follows that

$$\frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n)+\mathcal{H}(n\ell)}\cong R/\mathfrak{m}^{\delta+v_{\mathfrak{m}}(2)}\oplus R/\mathfrak{m}^{\delta+v_{\mathfrak{m}}(2)},$$

showing that $\delta_1=\delta_2$. □

Remark 6.4.3. Clearly, if $p\neq 2$ then the quotienting by 2-torsions in the proof of Lemma 6.4.2 is wholly redundant. The statement of the lemma would be simpler, too, as we would always have $\delta_1=\delta_2$.

Proposition 6.4.4. *Suppose that $(T,\mathcal{F},\mathcal{L})$ satisfies (SPR, free, dual). For any $n\ell\in\mathcal{N}$, there exist $a,b,\delta_1,\delta_2\in\mathbb{Z}_{\geq 0}$ such that the cokernel of each inclusion in (6.14) is a direct sum of two cyclic R-modules of the indicated lengths. If either $\delta_i>v_{\mathfrak{m}}(2)$, then $\delta_1=\delta_2$.*



(6.14)

For instance, the bottom left arrow indicates that $\mathcal{H}(n)/\mathcal{H}_\ell(n) \cong (R/\mathfrak{m}^a) \oplus (R/\mathfrak{m}^b)$.

Proof. Consider the exact sequences below, which are just a special case of (6.11):

$$\begin{aligned} 0 \longrightarrow \mathcal{H}(n) \hookrightarrow \mathcal{H}^\ell(n) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{tr}}(K_\ell, T), \\ 0 \longrightarrow \mathcal{H}_\ell(n) \hookrightarrow \mathcal{H}(n) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{f}}(K_\ell, T). \end{aligned} \tag{6.15}$$

Exactness gives us injections $\mathcal{H}^\ell(n)/\mathcal{H}(n) \to H^1_{\mathrm{tr}}(K_\ell, T)$ and $\mathcal{H}(n)/\mathcal{H}_\ell(n) \to H^1_{\mathrm{f}}(K_\ell, T)$, both of whose codomains are free of rank 2 over R by Lemma 6.2.3; Corollary 6.1.3 now assures that both quotients are indeed direct sums of two cyclic R-modules.

By the same reasoning as in Example 3.2.6, we can apply Theorem 3.2.4: the images of the rightmost maps are each other's orthogonal complements with respect to the local Tate pairing at ℓ, restricted to $H^1_{\mathrm{tr}}(K_\ell, T) \times H^1_{\mathrm{f}}(K_\ell, T)$. Now the same argument we used at the end of the proof of Lemma 6.4.1, slightly refined to take the individual direct summands into account, yields the relation between the bottom and top left arrows in (6.14). The relation between the bottom and top right arrows in (6.14), as well as the claim that those quotients are direct sums of two cyclic modules, follows from the very same reasoning.

As for the relation between the bottom left and top right, consider the exact sequence

$$0 \longrightarrow \frac{\mathcal{H}(n) + \mathcal{H}(n\ell)}{\mathcal{H}(n\ell)} \longrightarrow \frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n\ell)} \longrightarrow \frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n) + \mathcal{H}(n\ell)} \longrightarrow 0. \tag{6.16}$$

Since $H^1_{\mathrm{f}}(K_\ell, T) \cap H^1_{\mathrm{tr}}(K_\ell, T) = 0$, we have that $\mathcal{H}(n) \cap \mathcal{H}(n\ell) = \mathcal{H}_\ell(n)$ and hence that

$$\frac{\mathcal{H}(n) + \mathcal{H}(n\ell)}{\mathcal{H}(n\ell)} \cong \frac{\mathcal{H}(n)}{\mathcal{H}_\ell(n)} \cong (R/\mathfrak{m}^a) \oplus (R/\mathfrak{m}^b)$$

by assumption. Furthermore, Lemma 6.4.2 tells us that $\mathcal{H}^\ell(n)/(\mathcal{H}(n) + \mathcal{H}(n\ell)) \cong (R/\mathfrak{m}^{\delta_1}) \oplus (R/\mathfrak{m}^{\delta_2})$ for some δ_1 and δ_2. By considering the first and second summands of the terms in (6.16), we now see that $\mathcal{H}^\ell(n)/\mathcal{H}(n\ell)$ has summands of lengths $a + \delta_1$ and $b + \delta_2$. The fact that $\delta_1 = \delta_2$ if $\delta_i > v_{\mathfrak{m}}(2)$ directly carries over from Lemma 6.4.2.

The relation between the bottom right and top left quotients in (6.14) follows from the exact same reasoning, or as an immediate consequence of the relations we already deduced. □

Proposition 6.4.5. *Suppose that Conjecture 6.3.4 holds and that* $(T, \mathcal{F}, \mathcal{L})$ *satisfies (SPR, free, irred, cart, dual, eigen). If* $\mathrm{loc}_\ell \mathcal{S}_0(n) = 0$ *for some* $n\ell \in \mathcal{N}$*, then* $\mathrm{loc}_\ell \mathcal{S}_0(n\ell)$ *is 2-torsion.*

Proof. If $\mathrm{loc}_\ell \mathcal{S}_0(n) = 0$, then $\mathrm{loc}_\ell\left(\mathfrak{m}^{\lambda_0(n)}\mathcal{H}(n)/\mathcal{H}_\ell(n)\right) = 0$; since $\mathrm{loc}_\ell \colon \mathcal{H}(n)/\mathcal{H}_\ell(n) \to H^1_{\mathrm{f}}(K_\ell, T)$ defines an injection, this implies that $\mathfrak{m}^{\lambda_0(n)}\mathcal{H}(n)/\mathcal{H}_\ell(n) = 0$. We also have $\mathcal{H}(n)/\mathcal{H}_\ell(n) \cong (R/\mathfrak{m}^a) \oplus (R/\mathfrak{m}^b)$ by Proposition 6.4.4, and for this to be annihilated by $\mathfrak{m}^{\lambda_0(n)}$ it must be that $\lambda_0(n) \geq a, b$.

From Theorem 6.2.5 and Conjecture 6.3.4, we see that $\operatorname{len} \mathcal{H}(n) = \epsilon k + 2\lambda_0(n)$, which together with $\operatorname{len} \mathcal{H}(n)/\mathcal{H}_\ell(n) = a + b$ implies that $\operatorname{len} \mathcal{H}_\ell(n) = \epsilon k + 2\lambda_0(n) - a - b$. Similarly, we have $\operatorname{len} \mathcal{H}(n\ell) = \epsilon k + 2\lambda_0(n\ell)$ and $\operatorname{len} \mathcal{H}(n\ell)/\mathcal{H}_\ell(n) = 2k - a - b - \delta_1 - \delta_2$ by Proposition 6.4.4, which combined with $\operatorname{len} \mathcal{H}_\ell(n) = \epsilon k + 2\lambda_0(n) - a - b$ yield the equality

$$\epsilon k + 2\lambda_0(n\ell) = \epsilon k + 2\lambda_0(n) + 2k - 2a - 2b - \delta_1 - \delta_2. \tag{6.17}$$

Now suppose that $\delta_1 = \delta_2$, so that (6.17) reduces to

$$\lambda_0(n\ell) = \lambda_0(n) + k - a - b - \delta_1.$$

Using that $\lambda_0(n) \geq a, b$, this implies that $\lambda_0(n\ell) \geq k - a - \delta_1, k - b - \delta_2$. The bottom right arrow in

Proposition 6.4.4 now tells us that $\mathfrak{m}^{\lambda_0(n\ell)}$ annihilates $\mathcal{H}(n\ell)/\mathcal{H}_\ell(n)$, from which it follows that

$$\operatorname{loc}_\ell \mathcal{S}_0(n\ell) = \operatorname{loc}_\ell \left(\mathfrak{m}^{\lambda_0(n\ell)}\mathcal{H}(n\ell)/\mathcal{H}_\ell(n)\right) = 0.$$

If $\delta_1 \neq \delta_2$, then Proposition 6.4.4 tells us that $\delta_1, \delta_2 \leq v_\mathfrak{m}(2)$. This reduces (6.17) to the inequality

$$\lambda_0(n\ell) + v_\mathfrak{m}(2) \geq \lambda_0(n) + k - a - b,$$

which combined with $\lambda_0(n) \geq a, b$ gives $\lambda_0(n\ell) + v_\mathfrak{m}(2) \geq k - a, k - b$. This means, again by the bottom right arrow in Proposition 6.4.4, that $2\mathfrak{m}^{\lambda_0(n\ell)} = \mathfrak{m}^{\lambda_0(n\ell)+v_\mathfrak{m}(2)}$ annihilates $\mathcal{H}(n\ell)/\mathcal{H}_\ell(n)$, so

$$2\operatorname{loc}_\ell \mathcal{S}_0(n\ell) = 2\operatorname{loc}_\ell \left(\mathfrak{m}^{\lambda_0(n\ell)}\mathcal{H}(n\ell)/\mathcal{H}_\ell(n)\right) = 0. \qquad \square$$

6.4.1 Alternative definitions

The proof of Proposition 6.4.5 illustrates the utility of Conjecture 6.3.4: it allows us to cancel the ϵ-terms in (6.17), and a weaker relation between $\epsilon(n)$ and $\epsilon(n\ell)$ may not have been sufficient to obtain the lower bound on $\lambda_0(n\ell)$.

Still, even with the assumption of Conjecture 6.3.4, Proposition 6.4.5 is weaker than Howard's original [How04, 1.5.9] that it generalizes. For $p > 2$ we do have that $\operatorname{loc}_\ell \mathcal{S}_0(n) = 0$ implies $\operatorname{loc}_\ell \mathcal{S}_0(n\ell) = 0$, but for $p = 2$ we can only draw the weaker conclusion that $\operatorname{loc}_\ell \mathcal{S}_0(n\ell)$ is annihilated by 2. Looking at our proof, we may still conclude that $\operatorname{loc}_\ell \mathcal{S}_0(n\ell) = 0$, provided that $\delta_1 = \delta_2$, so in particular if either $\delta_i > v_\mathfrak{m}(2)$.

This motivates us to retrace our steps and consider where we first encountered these δ_i's. In particular, we saw in the proof of Lemma 6.4.2 that $\delta_i > v_\mathfrak{m}(2)$ if and only if

$$2\frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n)+\mathcal{H}(n\ell)} \cong \frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n)+\mathcal{H}(n\ell)} \Big/ \frac{\mathcal{H}^\ell(n)}{\mathcal{H}(n)+\mathcal{H}(n\ell)}[2] \neq 0,$$

so we may conclude that $\operatorname{loc}_\ell \mathcal{S}_0(n\ell) = 0$ if we can show that $2\mathcal{H}^\ell(n) \not\subset \mathcal{H}(n) + \mathcal{H}(n\ell)$, i.e. that there is a $c \in \mathcal{H}^\ell(n)$ that does not satisfy $2c_\ell = c_\ell^{\mathrm{f}} + c_\ell^{\mathrm{tr}}$ for any $c^{\mathrm{f}} \in \mathcal{H}(n)$ and $c^{\mathrm{tr}} \in \mathcal{H}(n\ell)$. However, verifying this condition requires detailed information about the localizations of $\mathcal{H}(n)$ and $\mathcal{H}(n\ell)$ at ℓ, which is generally no easier to obtain than information about $\operatorname{loc}_\ell \mathcal{S}(n\ell)$ itself.

In an effort to find a stronger generalization of [How04, 1.5.9], we may instead want to define the stub Selmer module as

$$\lambda_1(n) := \operatorname{len} 2M(n) \quad \text{and} \quad \mathcal{S}_1(n) := 2\mathfrak{m}^{\lambda_1(n)}\mathcal{H}(n) \cong 2\mathfrak{m}^{\lambda_1(n)}R^\epsilon,$$

or more generally

$$\lambda_t(n) := \operatorname{len} 2^t M(n) \quad \text{and} \quad \mathcal{S}_t(n) := 2^t\mathfrak{m}^{\lambda_1(n)}\mathcal{H}(n) \cong 2^t\mathfrak{m}^{\lambda_t(n)}R^\epsilon$$

for any non-negative integer t. The assumption $\operatorname{loc}_\ell \mathcal{S}_t(n) = 0$ then implies that $2^t\mathfrak{m}^{\lambda_t(n)}$ annihilates $\mathcal{H}(n)/\mathcal{H}_\ell(n)$, so $\lambda_t(n)+tv_\mathfrak{m}(2) \geq a, b$. We also have for small enough t that $\operatorname{len} 2^t\mathcal{H}(n) = \epsilon(k-tv_\mathfrak{m}(2))+2\lambda_t(n)$ and $\operatorname{len} 2^t\mathcal{H}(n\ell) = \epsilon(k - tv_\mathfrak{m}(2)) + 2\lambda_t(n\ell)$, but in order to relate this to $\operatorname{len} 2^t\mathcal{H}_\ell(n)$ in the way we related $\operatorname{len}\mathcal{H}_\ell(n)$ to $\operatorname{len}\mathcal{H}(n)$ and $\operatorname{len}\mathcal{H}(n\ell)$ in the proof of Proposition 6.4.5, we would need an analogy to Proposition 6.4.4 with respect to the cokernels in

$$\begin{array}{ccccc} & & 2^t\mathcal{H}^\ell(n) & & \\ & \nearrow & & \nwarrow & \\ 2^t\mathcal{H}(n) & & & & 2^t\mathcal{H}(n\ell) \\ & \nwarrow & & \nearrow & \\ & & 2^t\mathcal{H}_\ell(n). & & \end{array}$$

However, our proof of Proposition 6.4.4 heavily relies on exact sequences and diagrams of the form (6.15),

and in adjusting this proof to the above diagram, we run into the same issue as when we tried to prove results about $\rho_1^{\pm}$ in the previous section: multiplication by (powers of) 2 does not preserve exactness and global duality.

Instead of considering the length of $2^t M(n)$, we could define the stub Selmer module using the smallest annihilator of $M(n)$, that is,

$$\lambda_*(n) := \min\{t \in \mathbb{Z}_{\geq 0} : \mathfrak{m}^t M(n) = 0\} \quad \text{and} \quad \mathcal{S}_*(n) := \mathfrak{m}^{\lambda_*(n)}\mathcal{H}(n) \cong \mathfrak{m}^{\lambda_*(n)}R^{\epsilon}.$$

It should however be evident that working with $\mathcal{S}_*(n)$ is no easier than with $\mathcal{S}_t(n)$ for $t > 0$, and we are forced to conclude that, without digressing too far from Howard's strategy, Proposition 6.4.5 is the strongest generalization of his [How04, 1.5.9] that we can achieve.

7 Modules over discrete valuation rings

Now that we understand the situation when R is a special principal ring, we turn to the non-Artinian case where R is a discrete valuation ring:

$$R \text{ is a discrete valuation ring with uniformizer } \pi. \tag{DVR}$$

As before, we fix a Selmer triple $(T, \mathcal{F}, \mathcal{L})$, and for any integer $k > v_{\mathfrak{m}}(2)$ we write

$$R^{(k)} := R/\mathfrak{m}^k, \quad T^{(k)} := T/\mathfrak{m}^k T, \quad \mathcal{L}^{(k)} := \mathcal{L} \cap \mathcal{L}_k(T).$$

By propagating through the surjection $T \to T^{(k)}$ we obtain a Selmer triple $(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$; if $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR), then $(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$ satisfies (SPR). Furthermore, it is readily checked that if $(T, \mathcal{F}, \mathcal{L})$ satisfies any of the hypotheses from Section 5, then $(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$ satisfies that hypothesis as well.

Given the necessary assumptions on $(T, \mathcal{F}, \mathcal{L})$, we may thus invoke the results and definitions from Section 6 with respect to $(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$. In particular, if $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, cart, dual), then Theorem 6.2.5 gives a decomposition

$$H^1_{\mathcal{F}(n)}(K, T^{(k)}) \cong R^{(k),\epsilon} \oplus M^{(k)}(n) \oplus M^{(k)}(n) \tag{7.1}$$

for each $n \in \mathcal{N}^{(k)} := \mathcal{N}(\mathcal{L}^{(k)})$. If we furthermore assume (eigen), then Conjecture 6.3.4 claims that this ϵ is independent of n. Because of this convenience, we will assume throughout this section that Conjecture 6.3.4 holds.

For any non-negative integer $i \leq k$, Lemma 6.2.2 gives an isomorphism $H^1_{\mathcal{F}(n)}(K, T^{(i)}) \cong H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}^i]$, implying that ϵ is also independent of k.

With the above hypotheses and notation in mind and given any integers $k > v_{\mathfrak{m}}(2)$, $t \geq 0$ and $n \in \mathcal{N}^{(k)}$, we write $\lambda_t^{(k)}(n) := \operatorname{len} 2^t M^{(k)}(n)$ and define the stub Selmer module

$$\mathcal{S}_t^{(k)}(n) := 2^t \mathfrak{m}^{\lambda_t^{(k)}(n)} H^1_{\mathcal{F}(n)}(K, T^{(k)}) \cong 2^t \mathfrak{m}^{\lambda_t^{(k)}(n)} R^{\epsilon}.$$

Any Kolyvagin system $\kappa \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L})$ induces a Kolyvagin system $\kappa^{(k)} \in \mathbf{KS}(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$ via the maps $H^1_{\mathcal{F}(n)}(K, T/I_n) \to H^1_{\mathcal{F}(n)}(K, T^{(k)})$ induced by $T \to T^{(k)}$.

7.1 First results

By our general assumption, R is complete with respect to its $\mathfrak{m}$-adic topology, so $R \cong \varprojlim_k R^{(k)}$, with the inverse limit taken over the projections $R^{(k+1)} \to R^{(k)}$. It follows that

$$T \cong T \otimes_R R \cong T \otimes_R (\varprojlim_k R^{(k)}) \cong \varprojlim_k (T \otimes_R R^{(k)}) \cong \varprojlim_k T^{(k)},$$

with the inverse limit over the projections $T^{(k+1)} \to T^{(k)}$. We have a similar result for the cohomology modules and Selmer module of T:

Lemma 7.1.1. *Assume (DVR, free). The projections $T \to T^{(k)}$ induce isomorphisms*

$$H^1(K, T) \cong \varprojlim_k H^1(K, T^{(k)}) \quad \text{and} \quad H^1_{\mathcal{F}}(K, T) \cong \varprojlim_k H^1_{\mathcal{F}}(K, T^{(k)}),$$

where the inverse limit is taken over the maps induced by $T^{(k+1)} \to T^{(k)}$.

Proof. Since every $T^{(k)}$ is finite, [Rub00, B.2.3] gives us the first isomorphism. Since $\mathcal{F}$ is propagated through the projections $T \to T^{(k)}$, it is readily verified that the image of $H^1_{\mathcal{F}}(K, T)$ lies in $\varprojlim_k H^1_{\mathcal{F}}(K, T^{(k)})$ and the preimage of $\varprojlim_k H^1_{\mathcal{F}}(K, T^{(k)})$ lies in $H^1_{\mathcal{F}}(K, T)$, yielding the second isomorphism. □

Remark 7.1.2. Lemma 7.1.1 is one of the results we alluded to in Remark 2.3.6: [Rub00, B.2.3] requires that we consider *continuous* cohomology, where both G_K and T are equipped with the profinite topology.

We have already found that the exponent ϵ in (7.1) is independent of k, so it is worth also investigating the behaviour of the squared term $M^{(k)}(n)$ as k increases. It turns out that, if the stub Selmer module is nontrivial, this term eventually stabilizes:

Lemma 7.1.3. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, cart, dual, eigen) and that $\mathcal{S}_t^{(k_*)}(n) \neq 0$ for some $k_* > v_{\mathfrak{m}}(2)$, $t \geq 0$ and $n \in \mathcal{N}^{(k_*)}$. Then $M^{(k)}(n) \cong M^{(k_*)}(n)$ for all $k \geq k_*$ for which $n \in \mathcal{N}^{(k)}$.*

Proof. For $\mathcal{S}_t^{(k_*)}(n) \cong 2^t \mathfrak{m}^{\lambda_t^{(k_*)}(n)} R^{(k_*),\epsilon}$ to be nonzero, we need that $\epsilon \neq 0$ and $\lambda_t^{(k_*)}(n) + tv_{\mathfrak{m}}(2) < k_*$. Furthermore, since $R^{(k)}[\mathfrak{m}^{k_*}] \cong R^{(k_*)}$ for any $k \geq k_*$, Lemma 6.2.2 gives us an isomorphism

$$\begin{aligned} R^{(k_*)} \oplus M^{(k_*)}(n) \oplus M^{(k_*)}(n) &\cong H^1_{\mathcal{F}(n)}(K, T^{(k_*)}) \cong H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}^{k_*}] \\ &\cong \left(R^{(k)} \oplus M^{(k)}(n) \oplus M^{(k)}(n)\right)[\mathfrak{m}^{k_*}] \cong R^{(k_*)} \oplus \left(M^{(k)}(n)\right)[\mathfrak{m}^{k_*}] \oplus \left(M^{(k)}(n)\right)[\mathfrak{m}^{k_*}], \end{aligned}$$

from which it follows that $M^{(k_*)}(n) \cong (M^{(k)}(n))[\mathfrak{m}^{k_*}]$. It now suffices to show that $\mathfrak{m}^{k_*} M^{(k)}(n) = 0$: if this were not the case, then the decomposition of $M^{(k)}(n)$ in Corollary 6.1.2 would have a direct summand $R/\mathfrak{m}^s$ with $s > k_*$. However, then $(M^{(k)}(n))[\mathfrak{m}^{k_*}]$ would have a direct summand $(R/\mathfrak{m}^s)[\mathfrak{m}^{k_*}] \cong R^{(k_*)}$, implying that

$$\lambda_t^{(k_*)}(n) = \operatorname{len}\left(2^t M^{(k_*)}(n)\right) = \operatorname{len}\left(2^t \left(M^{(k)}(n)\right)[\mathfrak{m}^{k_*}]\right) \geq k_* - tv_{\mathfrak{m}}(2)$$

which contradicts our earlier finding. Hence it must be that $M^{(k)}(n) \cong M^{(k_*)}(n)$. □

Proposition 7.1.4. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, cart, dual, eigen) and that $\mathcal{S}_t^{(k)}(n) \neq 0$ for some $k > v_{\mathfrak{m}}(2)$, $t \geq 0$ and $n \in \mathcal{N}^{(2k-1)}$. Then the image of the map*

$$H^1_{\mathcal{F}(n)}(K, T^{(2k-1)}) \longrightarrow H^1_{\mathcal{F}(n)}(K, T^{(k)}) \tag{7.2}$$

induced by $T^{(2k-1)} \to T^{(k)}$ is a free $R^{(k)}$-submodule of rank 1.

Proof. This is [How04, 1.6.3]. By Lemma 6.2.2 we may identify $H^1_{\mathcal{F}(n)}(K, T^{(k)})$ with $H^1_{\mathcal{F}(n)}(K, T^{(2k-1)})[\mathfrak{m}^k]$ and (7.2) with the map

$$H^1_{\mathcal{F}(n)}(K, T^{(2k-1)}) \longrightarrow H^1_{\mathcal{F}(n)}(K, T^{(2k-1)})[\mathfrak{m}^k]$$

given by multiplication by π^{k-1}. From Lemma 7.1.3 it follows that $\operatorname{len} M^{(2k-1)}(n) = \operatorname{len} M^{(k)}(n) < k$, so the image of this map is

$$\mathfrak{m}^{k-1} H^1_{\mathcal{F}(n)}(K, T^{(2k-1)}) \cong \mathfrak{m}^{k-1}\left(R^{(2k-1)} \oplus M^{(2k-1)}(n) \oplus M^{(2k-1)}(n)\right) \cong \mathfrak{m}^{k-1} R^{(2k-1)} \cong R^{(k)}. \qquad \square$$

For the next result we need a famous theorem from class field theory. A proof and some of its consequences can be found in [Neu99, VII.13]; for our purposes, a weak corollary will suffice.

Theorem 7.1.5 (Chebotarev's density theorem, [Neu99, VII.13.4])**.** *Let L/K be a (finite) Galois extension of number fields and $\mathcal{C}$ a conjugacy class of $\operatorname{Gal}(L/K)$. Then the set of primes of K that are unramified in L and whose Frobenius elements belong to $\mathcal{C}$ has density $|\mathcal{C}|/|\operatorname{Gal}(L/K)|$.*

Here, for a set S of primes in K, "density" refers to the natural density

$$d_{\mathrm{nat}}(S) = \lim_{x \to \infty} \frac{|\{\mathfrak{p} \in S : |\mathcal{O}_K/\mathfrak{p}| \leq x\}|}{|\{\mathfrak{p} \text{ prime of } K : |\mathcal{O}_K/\mathfrak{p}| \leq x\}|}$$

or the analytic density

$$d_{\mathrm{an}}(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} |\mathcal{O}_K/\mathfrak{p}|^{-s}}{\sum_{\mathfrak{p} \text{ prime}} |\mathcal{O}_K/\mathfrak{p}|^{-s}}$$

interchangably. In particular, Theorem 7.1.5 tells us that there are infinitely many primes in K that are unramified in L with Frobenius in the class $\mathcal{C}$. That is all we need to prove the following generalization of [How04, 1.6.2].

Proposition 7.1.6. *Assume that $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, Gal, cart, dual, eigen) and that $\mathcal{L}_k(T) \subset \mathcal{L}$ for sufficiently large k. If $c^{\pm} \in H^1_{\mathcal{F}(n)}(K, \bar{T})^{\pm}$ such that $2c^{\pm} \neq 0$, then for sufficiently large k there are infinitely many $\ell \in \mathcal{L}^{(2k-1)}$ such that $c^{\pm}_{\ell} \neq 0$. Moreover, if we have both $2c^+, 2c^- \neq 0$, then there are infinitely many $\ell \in \mathcal{L}^{(2k-1)}$ such that both $c^+_{\ell}, c^-_{\ell} \neq 0$.*

Proof. We assume that $2c^+, 2c^- \neq 0$; the case for a single sign follows from a simplification of our proof.

Let $F/\mathbb{Q}$ be the Galois extension from (Gal): $K \subset F$, $T^{G_F} = T$, and $2H^1(F(\mu_{p^\infty})/K, \bar{T}) = 0$. Furthermore, let $L/\mathbb{Q}$ be the Galois closure of (i.e. the intersection of all Galois extensions of $\mathbb{Q}$ containing) $K(T^{(2k-1)}, \mu_{p^{2k-1}})$. From this construction is is clear that $L \subset F(\mu_{p^\infty})$.

It now follows that $2H^1(L/K, \bar{T}) = 0$: any cocycle $\mathrm{Gal}(L/K) \to \bar{T}$ induces a cocycle $\mathrm{Gal}(F(\mu_{p^\infty})/K) \to \bar{T}$ via the restriction $\mathrm{Gal}(F(\mu_{p^\infty})/K) \to \mathrm{Gal}(L/K)$. Since $2H^1(F(\mu_{p^\infty})/K, \bar{T}) = 0$, any such cocycle is a coboundary when multiplied by 2.

Together with the facts that $\bar{T}^{G_L} = \bar{T}$ and $H^1(L, \bar{T}) \cong \mathrm{Hom}(G_L, \bar{T})$ by Corollary 2.3.3, the inflation-restriction sequence from Proposition 2.3.4,

$$0 \longrightarrow H^1(L/K, \bar{T}^{G_L}) \longrightarrow H^1(K, \bar{T}) \longrightarrow H^1(L, \bar{T})^{\mathrm{Gal}(L/K)},$$

yields a map $H^1(K, \bar{T}) \to \mathrm{Hom}(G_L, \bar{T})^{\mathrm{Gal}(L/K)}$ whose kernel is 2-torsion. Since $2c^{\pm} \neq 0$, we may identify $c^{\pm}$ with its nonzero image under this map.

With this identification in mind, let E be the fixed field of $\ker c^+ \cap \ker c^-$, and put

$$G := \mathrm{Gal}(E/L) \cong G_L/G_E = G_L/(\ker c^+ \cap \ker c^-),$$

which injects into $\bar{T} \oplus \bar{T}$ via $\sigma \mapsto (c^+(\sigma), c^-(\sigma))$. This implies that G is an $R/2\mathfrak{m}$-module and, because of (free), finite. We equip G with a $\mathrm{Gal}(L/\mathbb{Q})$-action via conjugation and write, as usual, $G^{\pm}$ for its ± 1-eigenspace under τ.

By passing through the isomorphism $G \cong G_L/G_E$, we have maps $c^{\pm} \colon G \to \bar{T}$; we claim that both $c^+(G^+), c^-(G^+) \neq 0$. Indeed, since $2G \subset G^+ + G^-$ by (5.1), the assumption that $c^+(G^+) = 0$ would imply that $2c^+(G) \subset c^+(G^-)$. Since $c^+ \in H^1_{\mathcal{F}(n)}(K, \bar{T})^+$, we have for any $\sigma \in G^-$ that $\tau c^+(\sigma) = -\tau c^+(\tau\sigma\tau) = -c^+(\sigma)$, meaning that $2c^+(G) \subset \bar{T}^-$ and hence $2c^+(G) \subset 2\bar{T} \cap \bar{T}^-$. Moreover, $2c^+(G)$ is stable under the action of G_K: since $c^+ \in \mathrm{Hom}(G_L, \bar{T})^{\mathrm{Gal}(L/K)}$, we have for any $\eta \in G_K$ and $\sigma \in G$ that

$$\eta 2c^+(\sigma) = 2c^+(\eta^{-1}\sigma\eta) \in 2c^+(G).$$

Hypothesis (irred) now tells us that $2c^+(G)$ is either 0 or $2\bar{T}$. However, (eigen) states that $\bar{T}^-$ is a free $R/2\mathfrak{m}$-module of rank 1, so $2c^+(G) \subset 2\bar{T} \cap \bar{T}^-$ is generated by at most one element by Corollary 6.1.3. Subsequently, (irred) forces $2c^+(G) = 0$, contradicting the assumption that we began with. It must therefore be that $c^+(G^+) \neq 0$, and an analogous approach shows that $c^-(G^+) \neq 0$.

Since neither c^+ nor c^- is trivial on G^+, we may choose an $\eta \in G^+$ such that $c^+(\eta), c^-(\eta) \neq 0$. We wish to apply Theorem 7.1.5 to the conjugacy class of η, but we first need to confirm that $E/\mathbb{Q}$ is a finite Galois extension. As for finiteness, we already saw that $G = \mathrm{Gal}(E/L)$ and therefore E/L is finite. Likewise, since the absolute Galois group of $K(T^{(2k-1)})$ is the kernel of the representation $G_K \to \mathrm{Aut}_R(T^{(2k-1)})$ induced by the group action of G_K, $\mathrm{Gal}(K(T^{(2k-1)})/K)$ injects into $\mathrm{Aut}_R(T^{(2k-1)})$ which, under (free), is finite. Subsequently, $K(T^{(2k-1)}, \mu_{p^{2k-1}})/\mathbb{Q}$ is finite and it follows that its Galois closure $L/\mathbb{Q}$ is finite as well.

In order to show that $E/\mathbb{Q}$ is Galois, we follow the approach outlined in [DL20, p.41]. The pairing

$$[\cdot, \cdot] \colon \mathrm{Hom}(G_L, \bar{T})^{\mathrm{Gal}(L/K)} \times G_L \to \bar{T}, \quad [\phi, \rho] := \phi(\rho)$$

is injective on the left, and the orthogonal complement of $Rc^+ + Rc^-$ is $\ker c^+ \cap \ker c^- = G_E$. Using that

$$\sigma[\phi, \rho] = \sigma\phi(\rho) = \sigma\sigma^{-1}\phi(\sigma\rho\sigma^{-1}) = \phi(\sigma\rho\sigma^{-1}) = [\phi, \sigma\rho\sigma^{-1}]$$

for any $\sigma \in \mathrm{Gal}(L/K)$, $\phi \in \mathrm{Hom}(G_L, \bar{T})^{\mathrm{Gal}(L/K)}$ and $\rho \in G_L$, we see that $\sigma G_E \sigma^{-1} = G_E$, implying that

E/K is Galois. A similar argument with the identity $\tau[\phi,\rho] = [\tau\phi, \tau\rho\tau]$ shows that $E/\mathbb{Q}$ is Galois.

We may now invoke Theorem 7.1.5 and deduce that there are infinitely many primes ℓ in $\mathbb{Q}$ that are unramified in E and whose Frobenius element is (conjugate to) our earlier choice of η. Since η fixes L, it follows that all of these Fr_ℓ act trivially on $T^{(2k-1)}$ and hence that each such ℓ belongs to $\mathcal{L}_{2k-1}(T) = \mathcal{L}^{(2k-1)}$.

For these ℓ, evaluation at Fr_ℓ defines an isomorphism $H^1_{\mathrm{f}}(K_\ell, \bar{T}) \to \bar{T}$ by the proof of Proposition 3.1.7. For both signs we have

$$c^{\pm}_\ell(\mathrm{Fr}_\ell) = c^{\pm}(\mathrm{Fr}_\ell) = c^{\pm}(\eta) \neq 0,$$

so both $c^+_\ell, c^-_\ell \neq 0$. □

7.2 Stub Selmer modules

We have now arrived at what could be considered the motivation of the theory we developed in the previous sections. We will make use of the Kolyvagin system structure from Section 4.3, the $\rho^{\pm}$-functions studied in Section 6.3, and the stub Selmer modules from Section 6.4. From this, our main Theorem 7.3.3 will follow without much more work.

Unfortunately, while our results thus far allow us to prove this section's conjecture when $p > 2$, they are not sufficient to deduce an analogous result when $p = 2$, even if we adjust our goal to be significantly weaker than Howard's theorem. Fortunately, one of the lemmas that our proof relies on *does* hold for all p.

Lemma 7.2.1. *Suppose that $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, Gal, cart, dual, eigen) and admits a Kolyvagin system $\kappa \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L})$, and fix integers $s \geq 1$, $t \geq 0$. If there exists a $k > v_{\mathfrak{m}}(2)$ and $n \in \mathcal{N}^{(2k-1)}$ such that $2^s\kappa_n^{(k)} \notin \mathcal{S}_t^{(k)}(n) \otimes G_n$, then $\mathcal{S}_t^{(k)}(n) = 0$.*

Proof. Note that by Remark 4.3.4, we may identify $H^1_{\mathcal{F}(n)}(K, T^{(k)}) \otimes G_n$ with $H^1_{\mathcal{F}(n)}(K, T^{(k)})$ and view the entries of a Kolyvagin system to be elements of the latter.

We argue by contradiction: suppose that $\mathcal{S}_t^{(k)}(n) \neq 0$, and let $k > v_{\mathfrak{m}}(2)$ be the smallest integer for which $2^s\kappa_n^{(k)} \notin \mathcal{S}_t^{(k)}(n)$, for some $n \in \mathcal{N}^{(2k-1)}$. It follows that $\epsilon = 1$ and $i := \lambda_t^{(k)}(n) + tv_{\mathfrak{m}}(2) < k$; if $i \leq v_{\mathfrak{m}}(2)$, then $2H^1_{\mathcal{F}(n)}(K, T^{(k)}) \subset \mathcal{S}_t^{(k)}(n)$, contradicting our choice for k. Hence $i > v_{\mathfrak{m}}(2)$, so we have a stub Selmer module $\mathcal{S}_t^{(i)}(n)$ and by the minimality of k that $2^s\kappa_n^{(i)} \in \mathcal{S}_t^{(i)}(n)$.

By the same reasoning as in the proof of Lemma 7.1.3, we have an isomorphism $M^{(i)}(n) \cong M^{(k)}(n)[\mathfrak{m}^i] = M^{(k)}(n)$, from which it follows that $\lambda_t^{(i)}(n) = \lambda_t^{(k)}(n)$ and therefore that $\mathcal{S}_t^{(i)}(n) = 0$. Combined with the above, this implies that $2^s\kappa_n^{(i)} = 0$.

From Lemma 6.2.2 it follows that $\pi^{k-i}\kappa_n^{(k)} = \pi^{k-i}\kappa_n^{(i)}$, so $2^s\pi^{k-i}\kappa_n^{(k)} = 0$. Moreover, from the way $\kappa^{(k)}$ is derived from κ we see that $\kappa_n^{(k)}$ lies in the image of (7.2), which by Proposition 7.1.4 is a free $R^{(k)}$-module of rank 1. The equality $2^s\pi^{k-i}\kappa_n^{(k)} = 0$ thus implies that $2^s\kappa_n^{(k)}$ is a multiple of π^i in that image, which means that $2^s\kappa_n^{(k)} \in \mathfrak{m}^i H^1_{\mathcal{F}(n)}(K, T^{(k)}) = \mathcal{S}_t^{(k)}(n)$, contradicting our choice of k.

It must therefore be that $\mathcal{S}_t^{(k)}(n) = 0$. □

Conjecture 7.2.2. *Assume that $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, Gal, cart, dual, eigen) and $\mathcal{L}_k(T) \subset \mathcal{L}$ for sufficiently large k, and let $\kappa \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L})$. There exist integers $s \geq 1$ and $t \geq 0$, independent of $(T, \mathcal{F}, \mathcal{L})$ and κ, such that*

$$2^s\kappa_n^{(k)} \in \mathcal{S}_t^{(k)}(n) \otimes G_n$$

for sufficiently large $k > v_{\mathfrak{m}}(2)$ and $n \in \mathcal{N}^{(2k-1)}$.

If $p > 2$, then Conjecture 7.2.2 reduces to [How04, 1.6.1]: since 2 is a unit in R and $\mathcal{S}^{(k)}(n) = \mathcal{S}_t^{(k)}(n)$ is independent of t, the claim simply says that $\kappa_n^{(k)} \in \mathcal{S}^{(k)}(n) \otimes G_n$. This is what we now prove.

Proof for $p > 2$. As before, we may identify $H^1_{\mathcal{F}(n)}(K, T^{(k)}) \otimes G_n \cong H^1_{\mathcal{F}(n)}(K, T^{(k)})$. Suppose, for contradiction, that $k > 0$ is the smallest integer such that there exists an $n \in \mathcal{N}^{(2k-1)}$ for which $\kappa_n^{(k)} \notin \mathcal{S}^{(k)}(n)$. By Lemma 7.2.1, this forces $\mathcal{S}^{(k)}(n) = 0$.

For k as above, let n be such that $D := \dim H^1_{\mathcal{F}(n)}(K, \bar{T})$ is minimal. Note that if $D = 0$, then Lemma 6.2.2 gives $H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}] = 0$, from which it follows that $H^1_{\mathcal{F}(n)}(K, T^{(k)}) = 0 = \mathcal{S}^{(k)}(n)$, contradicting our assumption on k. Likewise, $D = 1$ implies $H^1_{\mathcal{F}(n)}(K, T^{(k)}) \cong R/\mathfrak{m}$, so $\lambda^{(k)}(n) = 0$ and hence $H^1_{\mathcal{F}(n)}(K, T^{(k)}) = \mathcal{S}^{(k)}(n)$. We therefore must have $D > 1$.

From (6.5) we know that $D = \rho^+(n) + \rho^-(n)$. Suppose that both $\rho^\pm(n) \neq 0$. Since $\kappa_n^{(k)} \neq 0$, multiplying it by a sufficiently high power of π gives a nonzero class in $H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}]$, which we identify with a nonzero class $c \in H^1_{\mathcal{F}(n)}(K, \bar{T})$ via Lemma 6.2.2. Lemma 5.3.1 now gives a decomposition $c = c^+ + c^-$ with $c^\pm \in H^1_{\mathcal{F}(n)}(K, \bar{T})^\pm$; without loss of generality, we may assume that $c^+ \neq 0$.

Since $\rho^-(n) \neq 0$, we may also pick a nonzero $d^- \in H^1_{\mathcal{F}(n)}(K, \bar{T})^-$. Proposition 7.1.6 now gives us an $\ell \in \mathcal{L}^{(2k-1)}$ such that $\ell \nmid n$ and for which both $c_\ell^+, d_\ell^- \neq 0$. This means that $\mathrm{loc}_\ell H^1_{\mathcal{F}(n)}(K, \bar{T}) \neq 0$ for both signs, so Corollary 6.3.2 tells us that $\rho^\pm(n\ell) = \rho^\pm(n) - 1$. In particular, $\dim H^1_{\mathcal{F}(n\ell)}(K, \bar{T}) < D$, which by the minimality of D implies that $\kappa_{n\ell}^{(k)} \in \mathcal{S}^{(k)}(n\ell)$.

From Proposition 6.4.5 we see that $\mathrm{loc}_\ell \kappa_{n\ell}^{(k)} = 0$, which by the Kolyvagin system relations from Definition 4.3.3 implies that $\mathrm{loc}_\ell \kappa_n^{(k)} = 0$. However, this also means that $c_\ell^+ = 0$, contradicting our choice of ℓ.

It therefore must be that either $\rho^\pm(n) = 0$; assume without loss of generality that $\rho^-(n) = 0$, so that $\rho^+(n) > 1$. Similarly to the previous case, we can identify a nonzero multiple of $\kappa_n^{(k)}$ with a nonzero $c^+ \in H^1_{\mathcal{F}(n)}(K, \bar{T}) = H^1_{\mathcal{F}(n)}(K, \bar{T})^+$ and use Proposition 7.1.6 to obtain an $\ell \in \mathcal{L}^{(2k-1)}(n)$ for which $c_\ell^+ \neq 0$. Corollary 6.3.2 now states that $\rho^+(n\ell) = \rho^+(n) - 1$ and $\rho^-(n\ell) = \rho^-(n) + 1$, so $\dim H^1_{\mathcal{F}(n\ell)}(K, \bar{T}) = D$ and $\rho^\pm(n\ell) > 0$ for both signs.

As we saw in the previous case, this is only possible if $\kappa_{n\ell}^{(k)} \in \mathcal{S}^{(k)}(n\ell)$, so $\mathrm{loc}_\ell \kappa_{n\ell}^{(k)} = 0$. The Kolyvagin system relations now force $\mathrm{loc}_\ell \kappa_n^{(k)} = 0$, and we arrive at the same contradiction that $c_\ell^+ = 0$.

Having exhausted all possibilities, we conclude that there is no k and $n \in \mathcal{N}^{(2k-1)}$ for which Conjecture 7.2.2 does not hold. □

7.2.1 The case $p = 2$

Since the s- and t-exponents in the statement of Conjecture 7.2.2 have no significance when $p > 2$, the fact that the conjecture is true for $p > 2$ does not give us any indication as to what values we ought to assign to s and t. We may however try emulating the above proof in the more general scenario and see what exponents could be appropriate, as well as where Howard's proof breaks down when $p = 2$.

Non-proof of Conjecture 7.2.2. With the usual identification in mind, we argue by contradiction: let $k > v_{\mathfrak{m}}(2)$ be the smallest integer for which there exists an $n \in \mathcal{N}^{(2k-1)}$ such that $2^s \kappa_n^{(k)} \notin \mathcal{S}_t^{(k)}(n)$. By Lemma 7.2.1, this forces $\mathcal{S}_t^{(k)}(n) = 0$.

For k as above, let n be such that $D_0 := \mathrm{len}\, H^1_{\mathcal{F}(n)}(K, \bar{T})$ is minimal. If $D_0 = 0$, then it follows from Lemma 6.2.2 that $H^1_{\mathcal{F}(n)}(K, T^{(k)}) = 0 = \mathcal{S}_t^{(k)}(n)$; if instead $D_0 = 1$, then $\lambda_0^{(k)}(n) = 0$ and hence $H^1_{\mathcal{F}(n)}(K, T^{(k)}) = \mathcal{S}_t^{(k)}(n)$. Therefore we must have $D_0 > 1$.

In line with our discussion in Section 6.3, we may instead want $D_1 := \dim 2H^1_{\mathcal{F}(n)}(K, \bar{T})$ to be minimal. If $t \geq 1$, then $D_1 = 0$ implies $H^1_{\mathcal{F}(n)}(K, T^{(k)}) = 0 = \mathcal{S}_t^{(k)}(n)$, and $D_1 = 1$ implies $2^t H^1_{\mathcal{F}(n)}(K, T^{(k)}) = \mathcal{S}_t^{(k)}(n)$; although the latter is not necessarily in contradiction with our assumptions, it would be if we set $s \geq t$.

This is as far as we can go before Howard's method begins to break down: we no longer have the equality $D_i = \rho_i^+(n) + \rho_i^-(n)$ for either $i \in \{0,1\}$ when $p = 2$, so our observation that $D_i > 1$ gives us no useful information about $H^1_{\mathcal{F}(n)}(K,\bar{T})^\pm$ or $2H^1_{\mathcal{F}(n)}(K,\bar{T})^\pm$. We may however investigate what happens if we assume that $\rho_i^\pm(n) \neq 0$ for both signs and both $i \in \{0,1\}$, and continue with the argument we used for $p > 2$.

Since $2^s\kappa_n^{(k)} \neq 0$, we have $2\kappa_n^{(k)} \neq 0$ which after multiplying with some power of π can be identified with a nonzero $2c \in 2H^1_{\mathcal{F}(n)}(K,\bar{T})$. Again, we can no longer decompose c into eigenvectors the way we did for $p > 2$, but we do have the inclusion $2H^1_{\mathcal{F}(n)}(K,\bar{T}) \subset H^1_{\mathcal{F}(n)}(K,\bar{T})^+ + H^1_{\mathcal{F}(n)}(K,\bar{T})^-$, so we may write $2c = c^+ + c^-$ for some, not necessarily unique, $c^\pm \in H^1_{\mathcal{F}(n)}(K,\bar{T})^\pm$.

Without loss of generality we may assume that $c^+ \neq 0$, but this is not enough to invoke Proposition 7.1.6: for that, we need $2c^+ \neq 0$. Suppose that that is indeed the case, and use $\rho_1^-(n) > 0$ to choose a $d^- \in H^1_{\mathcal{F}(n)}(K,\bar{T})^-$ such that $2d^- \neq 0$. Then Proposition 7.1.6 gives us an $\ell \in \mathcal{L}^{(2k-1)}(n)$ such that $c_\ell^+, d_\ell^- \neq 0$.

At this point in the proof we would like to deduce that $\operatorname{len} H^1_{\mathcal{F}(n\ell)}(K,\bar{T}) < D_0$ or $\dim 2H^1_{\mathcal{F}(n\ell)}(K,\bar{T}) < D_1$, so that by the minimality of such D_i we may conclude $2^s\kappa_{n\ell}^{(k)} \in \mathcal{S}_t^{(k)}(n\ell)$. Although we do have relations between $\rho_0^\pm(n)$ and $\rho_0^\pm(n\ell)$ from Proposition 6.3.1 and Proposition 6.3.3, we again run into the problem that (6.5) does not hold for $p = 2$, so we do not have enough information to draw the desired conclusion.

Suppose that $2^s\kappa_{n\ell}^{(k)} \in \mathcal{S}_t^{(k)}(n\ell)$ does hold. From Proposition 6.4.5 it follows that $2^{s+1}\operatorname{loc}_\ell \kappa_{n\ell}^{(k)} = 0$, and hence from the Kolyvagin system relations that $2^{s+1}\operatorname{loc}_\ell \kappa_n^{(k)} = 0$, so $2^{s+1}c_\ell = 0$. This, despite all of the reckless assumptions that we've made up until this point, is still not enough to reach a contradiction like we did for $p > 2$: from $2c = c^+ + c^-$ it follows that $2^s(c_\ell^+ + c_\ell^-) = 0$. Assuming the simplest case $s = 1$, this means that $2c_\ell^+ = -2c_\ell^-$, so $4c_\ell^+ = 0$. When $p = 2$, this is vacuously true for all elements of $H^1_{\mathcal{F}(n)}(K,\bar{T})$! □

The main obstacle we encountered while trying to prove Conjecture 7.2.2 is that, while $p > 2$ permits a splitting

$$H^1_{\mathcal{F}(n)}(K,\bar{T}) = H^1_{\mathcal{F}(n)}(K,\bar{T})^+ \oplus H^1_{\mathcal{F}(n)}(K,\bar{T})^- \tag{7.3}$$

from Lemma 5.3.1, this is no longer true when $p = 2$. In that case, the closest analogy is an inclusion into the non-direct sum of eigenspaces (5.1):

$$2H^1_{\mathcal{F}(n)}(K,\bar{T}) \subset H^1_{\mathcal{F}(n)}(K,\bar{T})^+ + H^1_{\mathcal{F}(n)}(K,\bar{T})^-. \tag{7.4}$$

Howard's methods heavily rely on (7.3), and (7.4) is often too weak to be an adequate replacement. This is apparent from the above attempt at a proof, in that we were unsuccessful in relating $D_i = \operatorname{len} 2^i H^1_{\mathcal{F}(n)}(K,\bar{T})$ to the $\rho_i^\pm(n)$-functions from Section 6.3, and unable to write $c \in H^1_{\mathcal{F}(n)}(K,\bar{T})$ as the sum of elements in $H^1_{\mathcal{F}(n)}(K,\bar{T})$.

The requirement that $2c^+ \neq 0$ in Proposition 7.1.6 comes from a similar discrepancy: although the $(R/2\mathfrak{m})[\operatorname{Gal}(L/\mathbb{Q})]$-module $G = \operatorname{Gal}(E/L)$ admits a splitting $G^+ \oplus G^-$ when $p > 2$, when $p = 2$ we can only assume that $2G \subset G^+ + G^-$.

A first step in repairing our non-proof for Conjecture 7.2.2 is to investigate whether (7.3) admits a stronger generalization than (7.4). More generally, we ought to find meaningful relationships between D_1, D_2, $\rho_0^\pm(n)$ and $\rho_1^\pm(n)$, as well as between $\rho_1^\pm(n)$ and $\rho_1^\pm(n\ell)$ like we discussed in Section 6.3. This should allows us to overcome some of the major issues we encountered above, and possibly also strengthen some of our intermediary results.

Lastly, notice that the only additional assumptions we imposed on the exponents s and t is that $s \geq t \geq 1$, and aside from that we only ever used the fact that $s \geq 1$. This gives us reason to believe that Conjecture 7.2.2 can be shown for $s = t = 1$.

7.3 Bounding the Selmer module

Although we failed to prove Conjecture 7.2.2 in full generality, it is still worth considering the implications of our conjecture. For $p > 2$ (for which we managed to prove Conjecture 7.2.2), this yields [How04, 1.6.1], which describes the structure of $H^1_{\mathcal{F}}(K,T)$ and of an associated module $H^1_{\mathcal{F}}(K,A)$; most importantly, it gives a bound on the non-free part of the latter. The full generality of Conjecture 7.2.2 allows us to generalize [How04, 1.6.1] to obtain similar structure results but a weaker bound when $p = 2$.

Denote by Φ the field of fractions of R, and put $\mathcal{D} := \Phi/R$ and $A := T \otimes_R \mathcal{D}$. We write $\mathcal{F}$ for the Selmer structure on A given by propagating $\mathcal{F} \otimes_R \Phi$ through the natural map $T \otimes_R \Phi \to A$, where $\mathcal{F} \otimes_R \Phi$ is the image of

$$\begin{aligned} H^1_{\mathcal{F}}(K_\ell, T) \otimes_R \Phi &\longrightarrow H^1(K_\ell, T \otimes_R \Phi) \\ [\xi] \otimes x &\longmapsto [\sigma \mapsto \xi(\sigma) \otimes x]. \end{aligned}$$

Lemma 7.3.1. *Assume (DVR). We have $\varinjlim_k R^{(k)} \cong \mathcal{D}$, where the direct limit is taken over the maps $R^{(k)} \to R^{(k+1)}$ defined by multiplication by π.*

Proof. Define a map $\varinjlim_k R^{(k)} \to \mathcal{D}$ by sending the class of $(k, x + \mathfrak{m}^k)$ to $\pi^{-k}x + R$. It is easily checked that this is a well-defined, R-linear bijection. □

Lemma 7.3.2. *Assume (DVR, free). The inclusions $A[\mathfrak{m}^k] \hookrightarrow A$ induce isomorphisms*

$$H^1(K,A) \cong \varinjlim_k H^1(K, A[\mathfrak{m}^k]) \quad \text{and} \quad H^1_{\mathcal{F}}(K,A) \cong \varinjlim_k H^1_{\mathcal{F}}(K, A[\mathfrak{m}^k]),$$

where the direct limit is taken over the maps induced by $A[\mathfrak{m}^k] \hookrightarrow A[\mathfrak{m}^\infty]$.

Proof. Notice the similarity with Lemma 7.1.1. Since $A = A[\mathfrak{m}^\infty] \cong \varinjlim_k A[\mathfrak{m}^k]$, [NSW20, 1.5.1] gives us the first isomorphism. Since $\mathcal{F}$ is propagated through the inclusions $A[\mathfrak{m}^k] \hookrightarrow A$, it follows that the first isomorphism restricts to the second. □

We are now ready to generalize [How04, 1.6.1] to obtain what may be considered the main theorem of this thesis. Note however that this heavily relies on Conjecture 7.2.2, which we only proved for $p > 2$, that is, for the cases that are already covered by Howard's original theorem.

Theorem 7.3.3. *Assume that Conjecture 7.2.2 holds, that $(T, \mathcal{F}, \mathcal{L})$ satisfies (DVR, free, irred, Gal, cart, dual, eigen) with $\mathcal{L}_k(T) \subset \mathcal{L}$ for sufficiently large k, and let $\kappa \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L})$. There exist integers $s \geq 1$ and $t \geq 0$, independent of $(T, \mathcal{F}, \mathcal{L})$ and κ, such that if $2^s \kappa_1 \neq 0$, then*

- ***i)*** *$H^1_{\mathcal{F}}(K,T)$ is a free R-module of rank 1;*
- ***ii)*** *$H^1_{\mathcal{F}}(K,A) \cong \mathcal{D} \oplus M \oplus M$ for some finite R-module M;*
- ***iii)*** *$\operatorname{len}(2^t M) \leq \operatorname{len}(H^1_{\mathcal{F}}(K,T)/R\kappa_1) + (s-t)v_{\mathfrak{m}}(2)$.*

Proof. For any k we have

$$A[\mathfrak{m}^k] = T \otimes_R (\pi^{-k}R/R) \cong T \otimes_R R^{(k)} \cong T^{(k)},$$

yielding an isomorphism $H^1(K, T^{(k)}) \cong H^1(K, A[\mathfrak{m}^k])$. In fact, working out the propagation along the diagram

$$\begin{array}{ccccccc} & & & & & & H^1_{\mathcal{F}}(K_v,T) \otimes_R \Phi \\ & & & & & & \downarrow \\ & & & & & & H^1(K_v, T \otimes_R \Phi) \\ & & & & & & \downarrow \\ H^1_{\mathcal{F}}(K_v,T) & \longrightarrow & H^1(K_v, T^{(k)}) & \xrightarrow{\sim} & H^1(K_v, A[\mathfrak{m}^k]) & \longrightarrow & H^1(K_v, A) \end{array}$$

shows that $H^1_{\mathcal{F}}(K_v, T^{(k)})$ is mapped into $H^1_{\mathcal{F}}(K_v, A[\mathfrak{m}^k])$ and vice versa, and therefore that our isomorphism restricts to

$$H^1_{\mathcal{F}}(K, T^{(k)}) \cong H^1_{\mathcal{F}}(K, A[\mathfrak{m}^k]) \tag{7.5}$$

Let s and t be as in Conjecture 7.2.2. If $2^s\kappa_1 \neq 0$, then $2^s\kappa_1^{(k_*)} \neq 0$ for sufficiently large k_*. Fix such a k_*. Taking $n = 1$ in Conjecture 7.2.2 yields $2^s\kappa_1^{(k_*)} \in \mathcal{S}_t^{(k_*)}$ which implies that $\mathcal{S}_t^{(k_*)} \neq 0$. Lemma 7.1.3 now tells us that $M^{(k)} \cong M^{(k_*)} =: M$ for all $k \geq k_*$, which combined with (7.5) gives

$$H^1_{\mathcal{F}}(K, A[\mathfrak{m}^k]) \cong R^{(k)} \oplus M \oplus M$$

for all $k \geq k_*$. Now, take the direct limit on both sides: Lemma 7.3.2 gives $H^1_{\mathcal{F}}(K, A)$ on the left, and Lemma 7.3.1 gives $\mathcal{D} \oplus M \oplus M$ on the right. Since $T^{(k_*)}$ is finite, $H^1_{\mathcal{F}}(K, T^{(k_*)})$ and hence $M^{(k_*)} = M$ are finite by Lemma 3.2.3, showing **(ii)**.

Furthermore, applying Lemma 7.1.1 to (7.5) shows that

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

is the $\mathfrak{m}$-adic Tate module of $H^1_{\mathcal{F}}(K, A) \cong \mathcal{D} \oplus M \oplus M$, which is readily seen to be a free R-module of rank 1. This shows **(i)**.

Lastly, put $\lambda := \lambda_t^{(k_*)}(1) = \operatorname{len} 2^t M$, so that $2^s\kappa_1^{(k_*)} \in 2^t\mathfrak{m}^\lambda H^1_{\mathcal{F}}(K, T^{(k_*)})$. It is readily verified that the kernel of $H^1_{\mathcal{F}}(K, T) \to H^1_{\mathcal{F}}(K, T^{(k_*)})$ is $\mathfrak{m}^{k_*} H^1_{\mathcal{F}}(K, T)$, which gives us an injection

$$H^1_{\mathcal{F}}(K, T)/\mathfrak{m}^{k_*} H^1_{\mathcal{F}}(K, T) \longrightarrow H^1_{\mathcal{F}}(K, T^{(k_*)}).$$

Taking the preimage of $2^s\kappa_1^{(k_*)}$ under this map, we see that $2^s\kappa_1 \in 2^t\mathfrak{m}^\lambda H^1_{\mathcal{F}}(K, T)$ due to **(i)**. Finally, the exact sequence

$$0 \longrightarrow \frac{R\kappa_1}{R2^s\kappa_1} \hookrightarrow \frac{H^1_{\mathcal{F}}(K, T)}{R2^s\kappa_1} \longrightarrow \frac{H^1_{\mathcal{F}}(K, T)}{R\kappa_1} \longrightarrow 0$$

gives

$$\begin{aligned}
\operatorname{len}\left(H^1_{\mathcal{F}}(K, T)/R\kappa_1\right) &= \operatorname{len}\left(H^1_{\mathcal{F}}(K, T)/R2^s\kappa_1\right) - \operatorname{len}(R\kappa_1/R2^s\kappa_1) \\
&\geq \operatorname{len}\left(H^1_{\mathcal{F}}(K, T)/2^t\mathfrak{m}^\lambda H^1_{\mathcal{F}}(K, T)\right) - \operatorname{len}(R/2^s R) \\
&= \lambda + tv_{\mathfrak{m}}(2) - sv_{\mathfrak{m}}(2) = \operatorname{len}(2^t M) - (s-t)v_{\mathfrak{m}}(2),
\end{aligned}$$

proving **(iii)**. □

Remark 7.3.4. In line with our final comment in Section 7.2, it is likely enough to take $s = t = 1$, so that the bound in part **(iii)** of Theorem 7.3.3 is given by $\operatorname{len}(2M) \leq \operatorname{len}(H^1_{\mathcal{F}}(K, T)/R\kappa_1)$.

8 An application to elliptic curves

Throughout this section we fix the following notation, most of which coincides with the conventions established in Section 5.

K	an imaginary quadratic field of discriminant $D \neq -3, -4$.
τ	a complex conjugation in $G_{\mathbb{Q}}$.
E	an elliptic curve defined over $\mathbb{Q}$.
N	the conductor of E, cf. [Sil94, IV.10].
p	a rational prime.
T	$= T_p(E)$, the p-adic Tate module of E.

We assume that D, N and p are pairwise coprime and that K satisfies the "Heegner hypothesis" that all rational primes dividing N are split in K. As mentioned in Section 5, our assumption that $D \neq -3, -4$ is required for our construction of the canonical transverse condition in Proposition 4.2.3.

The Tate module $T = T_p(E)$ is a $\mathbb{Z}_p[G_K]$-module (cf. Example 2.2.4), and the p-subgroup $E[p^\infty] \cong \varinjlim_k E[p^k]$ is a $\mathbb{Z}(p^\infty)[G_K]$-module, where $\mathbb{Z}(p^\infty) = \varinjlim_k \mathbb{Z}/p^k\mathbb{Z} \cong \mathbb{Q}_p/\mathbb{Z}_p$ is the Prüfer p-group; notice that $E[p^\infty] \cong T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$, so that $E[p^\infty]$ assumes the role of A in Section 7.3.

We assume that the representation $G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective, and if $p = 2$, that the discriminant of E is negative; this ensures that $E[2]$ is not contained in $E(\mathbb{R})$. Throughout this section we assume that Conjectures 6.3.4 and 7.2.2 hold.

In Section 8.1 we construct a Selmer structure on T and verify that it satisfies the hypotheses required by Theorem 7.3.3; in order to apply the theorem, we construct a nontrivial Kolyvagin system in Section 8.2. Section 8.3 discusses some of the implications of our final result.

8.1 The geometric Selmer structure

Consider the p^k-torsion subgroup $E[p^k]$ of E, viewed as a $(\mathbb{Z}/p\mathbb{Z})[G_K]$-module. By applying Galois cohomology (over K_v for some place v) to the exact sequence

$$0 \longrightarrow E[p^k] \hookrightarrow E \xrightarrow{p^k} E \longrightarrow 0, \tag{8.1}$$

we obtain the so-called Kummer sequence

$$0 \longrightarrow E(K_v)/p^kE(K_v) \longrightarrow H^1(K_v, E[p^k]) \longrightarrow H^1(K_v, E)[p^k] \longrightarrow 0. \tag{8.2}$$

The injection $E(K_v)/p^kE(K_v) \to H^1(K_v, E[p^k])$ in (8.2) is called the Kummer map, and we define a local condition $\mathcal{F}$ on $E[p^k]$ at v to be its image.

By [Cas65, 4.1], this is precisely the unramified condition at the non-Archimedean places that do not divide pN, and by the criterion of Néron–Ogg-Shafarevich [Sil08, VII.7.1], $E[p^k]$ is unramified at those places. Therefore $\mathcal{F}$ is a Selmer structure, with $\Sigma(\mathcal{F})$ consisting of the places dividing $pN\infty$.

Lemma 8.1.1. *With the Selmer structure $\mathcal{F}$ on $E[p^k]$ as defined above, we have an exact sequence*

$$0 \longrightarrow E(K)/p^kE(K) \longrightarrow H^1_{\mathcal{F}}(K, E[p^k]) \longrightarrow Ш(E/K)[p^k] \longrightarrow 0, \tag{8.3}$$

with $E(K)/p^kE(K) \to H^1_{\mathcal{F}}(K, E[p^k])$ the Kummer map. That is, $H^1_{\mathcal{F}}(K, E[p^k]) = \mathrm{Sel}_{p^k}(E/K)$ is the usual p^k-Selmer group of E/K.

Proof. In the very same way by which we obtained (8.2), we obtain the top row of the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/p^kE(K) & \longrightarrow & H^1(K,E[p^k]) & \longrightarrow & H^1(K,E)[p^k] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \prod \mathrm{loc}_v} & & \downarrow{\scriptstyle \prod \mathrm{loc}_v} & & \\ 0 & \longrightarrow & \prod_v E(K_v)/p^kE(K_v) & \longrightarrow & \prod_v H^1(K_v,E[p^k]) & \longrightarrow & \prod_v H^1(K_v,E)[p^k] & \longrightarrow & 0, \end{array} \tag{8.4}$$

where the products are over all places v of K and the left vertical map is induced by $x + p^kE(K) \mapsto x + p^kE(K_v)$; the left square indeed commutes by [NSW20, 1.5.2].

Firstly, note that an element of $E(K)/p^kE(K)$ maps through $\prod_v E(K_v)/p^kE(K_v)$ into $H^1_{\mathcal{F}}(K_v, E[p^k])$ by the definition of $\mathcal{F}$. The commutativity of the left square then implies that the image of $E(K)/p^kE(K)$ is contained in $H^1_{\mathcal{F}}(K, E[p^k])$.

Secondly, if $c \in H^1_{\mathcal{F}}(K, E[p^k])$, then $\prod \mathrm{loc}_v(c) \in \prod H^1_{\mathcal{F}}(K_v, E[p^k])$ is in the image of $\prod_v E(K_v)/p^kE(K_v)$ and hence maps to 0 in $\prod H^1(K_v, E)[p^k]$. This means that, under the top right horizontal map, c is mapped into the kernel of $\prod \mathrm{loc}_v \colon H^1(K,E)[p^k] \to \prod H^1(K_v,E)[p^k]$, which is precisely the Shafarevich–Tate group $Ш(E/K)$; it is clear that c lands in the p^k-torsion of this group.

For any $d \in Ш(E/K)[p^k]$, the surjectivity of the top right horizontal map implies that there is a $c \in H^1(K, E[p^k])$ that maps to d. Using that $\prod \mathrm{loc}_v(d) = 0$, it follows from the commutativity of the right square and the definition of $\mathcal{F}$ that $H^1_{\mathcal{F}}(K, E[p^k]) \to Ш(E/K)[p^k]$ is surjective.

Lastly, (8.3) is exact in the middle because the top row of (8.4) is. □

Exploiting the functoriality of the cohomology functor, we may extend (8.2) to a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K_v)/p^{k+1}E(K_v) & \longrightarrow & H^1(K_v,E[p^{k+1}]) & \longrightarrow & H^1(K_v,E)[p^{k+1}] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \\ 0 & \longrightarrow & E(K_v)/p^kE(K_v) & \longrightarrow & H^1(K_v,E[p^k]) & \longrightarrow & H^1(K_v,E)[p^k] & \longrightarrow & 0 \end{array}$$

for any positive integer k. Since the left vertical map is the canonical surjection, it follows that multiplication by p defines a surjection $H^1_{\mathcal{F}}(K_v, E[p^{k+1}]) \to H^1_{\mathcal{F}}(K_v, E[p^k])$. It is along these maps that we take the inverse limit, and using the identification $H^1(K_v, T) \cong \varprojlim_k H^1(K_v, E[p^k])$ from Lemma 7.1.1 or [Rub00, B.2.3], we may define a local condition on T by

$$H^1_{\mathcal{F}}(K_v, T) \cong \varprojlim_k H^1_{\mathcal{F}}(K_v, E[p^k]).$$

Since each $H^1_{\mathcal{F}}(K_v, E[p^k])$ is the finite condition at almost all places, it is readily verified that $\mathcal{F}$ defines a Selmer structure on T, with the same $\Sigma(\mathcal{F})$ as before. Analogously, we can extend (8.2) to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K_v)/p^kE(K_v) & \longrightarrow & H^1(K_v,E[p^k]) & \longrightarrow & H^1(K_v,E)[p^k] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_v)/p^{k+1}E(K_v) & \longrightarrow & H^1(K_v,E[p^{k+1}]) & \longrightarrow & H^1(K_v,E)[p^{k+1}] & \longrightarrow & 0 \end{array}$$

to obtain an injection $H^1_{\mathcal{F}}(K_v, E[p^k]) \to H^1_{\mathcal{F}}(K_v, E[p^{k+1}])$. Using $E[p^\infty] \cong \varinjlim_k E[p^k]$ as well as the identification $H^1(K_v, E[p^\infty]) \cong \varinjlim_k H^1(K_v, E[p^k])$ from Lemma 7.3.1 or [NSW20, 1.5.1], we define a local condition on $E[p^\infty]$ by

$$H^1_{\mathcal{F}}(K_v, E[p^\infty]) \cong \varinjlim_k H^1_{\mathcal{F}}(K_v, E[p^k]).$$

Once again, $\mathcal{F}$ defines a Selmer structure on $E[p^\infty]$ with the same $\Sigma(\mathcal{F})$ as we had on $E[p^k]$.

Remark 8.1.2. As one might expect, if we take our local conditions $\mathcal{F}$ on T and $E[p^\infty]$ and propagate them through the canonical maps $T \to E[p^k]$ and $E[p^k] \hookrightarrow E[p^\infty]$ respectively, we obtain in both cases the local

condition $\mathcal{F}$ on $E[p^k]$ that we started with. Moreover, taking the Selmer structure $\mathcal{F} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ on $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as described in Section 7.3 and propagating it to $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \cong E[p^\infty]$ yields the local condition $\mathcal{F}$ on $E[p^\infty]$ that we constructed above.

In a sense, Howard constructs $\mathcal{F}$ precisely "the other way around", by first defining a local condition on $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and propagating it to T and $E[p^\infty]$, and later to $E[p^k]$. His local condition is given by the image of the map $E(K_v) \otimes \mathbb{Q}_p \to H^1(K_v, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, which is induced by the Kummer maps from (8.2). Of course, our definition of $\mathcal{F}$ is equivalent to Howard's.

Proposition 8.1.3. *With the Selmer structure $\mathcal{F}$ on T and $E[p^\infty]$ as above, we have exact sequences*

$$0 \longrightarrow E(K) \otimes \mathbb{Z}_p \longrightarrow H^1_{\mathcal{F}}(K, T) \longrightarrow \varprojlim_k Ш(E/K)[p^k] \longrightarrow 0 \tag{8.5}$$

and

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1_{\mathcal{F}}(K, E[p^\infty]) \longrightarrow Ш(E/K)[p^\infty] \longrightarrow 0, \tag{8.6}$$

with $E(K) \otimes \mathbb{Z}_p \to H^1_{\mathcal{F}}(K, T)$ and $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1_{\mathcal{F}}(K, E[p^\infty])$ induced by the Kummer maps. That is, $H^1_{\mathcal{F}}(K, T) = S_p(E/K)$ and $H^1_{\mathcal{F}}(K, E[p^\infty]) = \mathrm{Sel}_{p^\infty}(E/K)$ are the usual p-power Selmer groups.

Proof. Naturally, this is just a matter of taking inverse and direct limits, respectively, of (8.3). Direct limits are always exact, and since the transition maps $E(K)/p^{k+1}E(K) \to E(K)/p^kE(K)$ are surjective, our inverse limit also preserves the exactness of (8.3) by [AM69, 10.2]

As for the first terms in (8.5) and (8.6), we have $E(K)/p^kE(K) \cong E(K) \otimes \mathbb{Z}/p^k\mathbb{Z}$; by [AM69, 10.13], this has inverse limit $E(K) \otimes \mathbb{Z}_p$. Since direct limits always commute with tensor products, we have furthermore that $\varinjlim_k (E(K) \otimes \mathbb{Z}/p^k\mathbb{Z}) \cong E(K) \otimes \mathbb{Z}(p^\infty)$, where $\mathbb{Z}(p^\infty) \cong \mathbb{Q}_p/\mathbb{Z}_p$ is the Prüfer p-group. □

In this setting, we have the following theorem, which corresponds to [How04, Theorem A and 1.6.5].

Theorem 8.1.4. *There exist integers $s \geq 1$ and $t \geq 0$, independent of E, such that if there is a Kolyvagin system $\kappa \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L}_1)$ with $2^s\kappa_1 \neq 0$, then*

- ***i)*** *$S_p(E/K)$ is a free $\mathbb{Z}_p$-module of rank 1;*
- ***ii)*** *$\mathrm{Sel}_{p^\infty}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus M \oplus M$ for some finite $\mathbb{Z}_p$-module M;*
- ***iii)*** *$\mathrm{len}(2^tM) \leq \mathrm{len}_{\mathbb{Z}_p}(S_p(E/K)/\kappa_1\mathbb{Z}_p) + (s-t)v_p(2)$.*

Proof. Given Proposition 8.1.3 and the preceding remark, this is simply an application of Theorem 7.3.3. We only need to verify that hypotheses (DVR, free, irred, Gal, cart, dual, eigen) are satisfied. Hypothesis (DVR) is obvious, and (free) is a standard fact, e.g. [Sil08, III.7.1]. Hypothesis (irred) is immediate from our assumption that $G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective.

As for (Gal), we claim that $F := K(E[p^\infty])$ has the desired properties. Clearly, $K \subset F$ and, since G_F acts trivially on $E[p^\infty]$, it also acts trivially on each $E[p^k]$ and hence on T. Note also that $\mu_{p^\infty} \subset F$: if F does not contain the primitive p^kth roots of unity, then there is a $\sigma \in G_F$ that permutes these roots. Consequently, for any $x, y \in E[p^\infty]$ the Weil pairing would evaluate to

$$e(x - \sigma(x), y) = \chi_p(\sigma)e(x, y) - e(x, y)$$

with χ_p the p-adic cyclotomic character. Since $\chi_p(\sigma) \neq 1$, the above would not vanish unless $e(x, y) = 0$, so σ does not act trivially on $E[p^\infty]$.

In order to show that $H^1(F/K, \bar{T})$ is trivial, we again use that $G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ and hence the induced map $\mathrm{Gal}(F/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(\bar{T})$ is surjective. Assume first that $p > 2$. Then $\bar{T} \cong E[p] \cong \mathbb{F}_p^2$, so we may identify the $\mathrm{Gal}(F/K)$-module $\bar{T}$ with the $\mathrm{GL}_2(\mathbb{F}_p)$-module $\mathbb{F}_p^2$, yielding

$$H^1(F/K, \bar{T}) \cong H^1(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2).$$

We diagonally embed $\mathbb{F}_p^\times$ into $\mathrm{GL}_2(\mathbb{F}_p)$, so that we may consider $\mathbb{F}_p^\times$ as a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Proposition 2.3.4) then gives an exact sequence

$$0 \longrightarrow H^1\left(\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times, (\mathbb{F}_p^2)^{\mathbb{F}_p^\times}\right) \longrightarrow H^1\left(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2\right) \longrightarrow H^1\left(\mathbb{F}_p^\times, \mathbb{F}_p^2\right)^{\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times}. \tag{8.7}$$

Since $\mathbb{F}_p^\times$ acts on $\mathbb{F}_p^2$ by scalar multiplication, it is clear that $(\mathbb{F}_p^2)^{\mathbb{F}_p^\times}$ and hence the second entry in (8.7) is trivial. As for the final term, keep in mind that $\mathbb{F}_p^\times$ acts trivially on $H^1(\mathbb{F}_p^\times, \mathbb{F}_p^2)$; otherwise, of course, it would not admit a well-defined action by $\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times$). For a cocycle $\xi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^2$, this means that for any $x, y \in \mathbb{F}_p^\times$, we have $x\xi(y) - \xi(y) = yw - w$ for some fixed $w \in \mathbb{F}_p^2$. Since $p > 2$, we may pick a nontrivial $x \in \mathbb{F}_p^\times$ and find that $\xi(y) = y(x-1)^{-1}w - (x-1)^{-1}w$ is a coboundary, from which it follows that $H^1\left(\mathbb{F}_p^\times, \mathbb{F}_p^2\right) = 0$.

From the exactness of (8.7) we can now infer that $H^1(F/K, \bar{T}) = H^1(\mathrm{GL}_2(\mathbb{F}_p), \mathbb{F}_p^2) = 0$, so our choice of F indeed has the desired properties and (Gal) is verified for $p > 2$.

The argument for $p = 2$ is similar: $\bar{T} \cong E[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$, and we identify $\bar{T}$ with the $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$-module $(\mathbb{Z}/4\mathbb{Z})^2$; here, $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ consists of the 2×2 matrices over $\mathbb{Z}/4\mathbb{Z}$ whose determinants are in $(\mathbb{Z}/4\mathbb{Z})^\times$. This yields

$$H^1(F/K, \bar{T}) \cong H^1(\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), (\mathbb{Z}/4\mathbb{Z})^2).$$

We diagonally embed $(\mathbb{Z}/4\mathbb{Z})^\times$ into $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ to obtain the exact sequence

$$\begin{aligned} 0 \longrightarrow H^1\left(\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})/(\mathbb{Z}/4\mathbb{Z})^\times, ((\mathbb{Z}/4\mathbb{Z})^2)^{(\mathbb{Z}/4\mathbb{Z})^\times}\right) \longrightarrow H^1\left(\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), (\mathbb{Z}/4\mathbb{Z})^2\right) \\ \longrightarrow H^1\left((\mathbb{Z}/4\mathbb{Z})^\times, (\mathbb{Z}/4\mathbb{Z})^2\right)^{\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})/(\mathbb{Z}/4\mathbb{Z})^\times}. \end{aligned} \tag{8.8}$$

It is easily seen that $((\mathbb{Z}/4\mathbb{Z})^2)^{(\mathbb{Z}/4\mathbb{Z})^\times} = 2(\mathbb{Z}/4\mathbb{Z})^2$ is 2-torsion. As for the final term, let $\xi\colon (\mathbb{Z}/4\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^2$ be a cocycle representing a class that is fixed by $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. That means that, for any $x \in (\mathbb{Z}/4\mathbb{Z})^\times$ and $A \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, we have $A\xi(x) - \xi(x) = xw - w$ for some fixed $w \in (\mathbb{Z}/4\mathbb{Z})^2$. Taking A to be the lower triangular matrix of all ones, we see that $\xi(x) = x(A-1)^{-1}w - (A-1)^{-1}w$ defines a coboundary, meaning that the final term in (8.8) vanishes.

The exactness of (8.8) and the preceding isomorphism now imply that $2H^1(F/K, \bar{T}) = 0$, and (Gal) is verified for $p = 2$.

Hypothesis (cart) is a direct consequence of the way we constructed $\mathcal{F}$. Alternatively, one could show that $H^1(K_v, T)/H^1_{\mathcal{F}}(K_v, T)$ is torsion-free and invoke [MR04, 3.7.1(i)].

For (dual), we define $(\cdot,\cdot)\colon T \times T \to \mathbb{Z}_p(1)$ as in Example 5.2.1, in which we already verified its desired properties. From the Weil pairing we have that $T^* \cong T$ and the self-duality of $\mathcal{F}$ follows from local Tate duality, cf. [CS00, 1.6(ii)].

Lastly, we verify (eigen). Since E is defined over $\mathbb{Q}$, the action of G_K on $\bar{T}$ obviously extends to an action of $G_\mathbb{Q}$. As for the eigenspaces of τ, assume first that $p > 2$. If $s, t \in E[p]$ belong to the same eigenspace, then the Weil pairing on $E[p]$ evaluates to

$$e(s,t) = e(\tau s, \tau t) = \chi_p(\tau) e(s,t) = -e(s,t),$$

implying $e(s,t) = 0$. Therefore, $E[p] = E[p]^\pm$ would contradict the nondegeneracy of the Weil pairing. If $p = 2$, there are *a priori* six different $\mathbb{Z}/4\mathbb{Z}$-modules that either $E[4]^\pm$ may be isomorphic to:

$$(\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}), \quad (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/4\mathbb{Z}), \quad (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}), \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}, \quad 0.$$

In the first three cases, we would have $\mathbb{F}_2^2 \cong E[2] \subset E[4]^\pm$, implying that $E[2]$ is invariant under the action of τ and hence that $E[2] \subset E(\mathbb{R})$; this contradicts our assumption that the discriminant of E is negative. The inclusion $E[2] \subset E[4]^+ + E[4]^-$ from (5.1) eliminates the possibility that either $E[4]^\pm = 0$, and the case

$E[4]^{\pm} \cong \mathbb{Z}/2\mathbb{Z}$ can be excluded via a straight forward computation: there are 20 matrices in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ with characteristic polynomial $x^2 - 1$, and none of those have an eigenspace of only 2 elements. Hence it must be that both $E[4] \cong \mathbb{Z}/4\mathbb{Z}$.

Finally, $H^1_{\mathcal{F}}(K, \bar{T})$ is stable under the action of τ because the Kummer maps are $G_{\mathbb{Q}}$-homomorphism, coming from the exact sequence (8.1) of $G_{\mathbb{Q}}$-modules. □

8.2 The Heegner point Kolyvagin system

We will now construct a Kolyvagin system for the Selmer structure from Section 8.1. We closely follow the discussions in [How04, 1.7] and [Wes01a, 5.2–6.2]; since their results are valid regardless of the parity of p, we only give an overview of the construction without detailed proofs.

Keep the notation as in Section 8.1. The first ingredient in our construction are modular curves: an introduction to these objects can be found in [Wes01b], and a more thorough but for our purposes incomplete discussion in [Sil94, I]. We only need two well-known properties:

Definition 8.2.1. An N-isogeny between two elliptic curves is an isogeny (cf. [Sil08, III.4]) whose kernel is cyclic of order N.

Theorem-Definition 8.2.2 (Modular curves, [Zho23, 1.10])**.** *For every positive integer N there exists a smooth projective curve $X_0(N)$ over $\mathbb{Q}$ whose non-cuspidal (hence all but finitely many) $\mathbb{C}$-valued points correspond to N-isogenies over $\mathbb{C}$ modulo isomorphisms over $\mathbb{C}$. Therefore, we have an injection*

$$\{N\text{-isogenies over } \mathbb{C}\}/\sim \hookrightarrow X_0(N),$$

where two N-isogenies $\phi_1 \colon E_1 \to E_1'$ and $\phi_2 \colon E_2 \to E_2'$ are equivalent if and only if there are isomorphisms $\psi \colon E_1 \to E_2$ and $\psi' \colon E_1' \to E_2'$ (over $\mathbb{C}$) such that $\psi' \phi_1 = \phi_2 \psi$. For any number field K, the non-cuspidal points of $X_0(N)(K)$ correspond to N-isogenies over K, but only up to isomorphism over $\bar{K}$: this gives an injection

$$\{N\text{-isogenies over } K\}/\sim \hookrightarrow X_0(N)(K)$$

with the equivalence relation as before.

Theorem 8.2.3 (Modularity theorem (formerly Taniyama–Shimura–Weil conjecture), [Wil95, 0.4], [CDT99, p. 522], [Bre+01, Theorem A])**.** *For any elliptic curve E defined over $\mathbb{Q}$ with conductor N, there exists a rational map $X_0(N) \to E$. This map is called a modular parametrization of E.*

All primes dividing N are assumed to be split in K and coprime to the discriminant in K, hence unramified; by choosing a prime of K above every rational prime dividing N, we obtain an ideal $\mathfrak{a}$ satisfying $\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$. Recall that we take $\mathcal{L} := \mathcal{L}_1(T)$ and denote for every $n \in \mathcal{N}(\mathcal{L})$ the order of conductor n by $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$.

Since $\mathfrak{a}$ is coprime to n, the ideal $\mathfrak{a}_n := \mathfrak{a} \cap \mathcal{O}_n$ is invertible by e.g. [Con, 3.8], yielding a fractional ideal $\mathfrak{a}_n^{-1} \supset \mathcal{O}_n$. We may view these latter two sets as lattices in $\mathbb{C}$, so that the identity map induces a map

$$\mathbb{C}/\mathcal{O}_n \longrightarrow \mathbb{C}/\mathfrak{a}_n^{-1} \tag{8.9}$$

which is an isogeny of elliptic curves by [Sil08, VI.4.1]. The kernel of this map is

$$\mathfrak{a}_n^{-1}/\mathcal{O}_n \cong \mathcal{O}_n/\mathfrak{a}_n \cong \mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$$

(see again [Con, 3.8] for the second isomorphism), so (8.9) is an N-isogeny and hence corresponds to a point $h_n \in X_0(N)$. Fixing a modular parametrization $X_0(N) \to E$, each such h_n is sent to a point $P[n] \in E$, which we call the Heegner point of conductor n. Strictly speaking, we shouldn't use a definite article because our construction relies on a choice for $\mathfrak{a}$ as well as for a modular parametrization; this will however not impact our further discussion because these choices are assumed to be fixed.

Proposition 8.2.4. *With notation as above and $n\ell \in \mathcal{N}$, we have*

i) $P[n] \in E(K[n])$, *cf. Theorem-Definition 4.2.1;*

ii) $\mathrm{Tr}_\ell\, P[n\ell] = (\ell + 1 - |E(\mathbb{F}_\ell)|)P[n]$, *where* $\mathrm{Tr}_\ell \colon E(K[n\ell]) \to E(K[n]$ *is the trace map;*

iii) $P[n\ell] \equiv \mathrm{Fr}_{\lambda[n]}\, P[n] \bmod \lambda[n\ell]$, *where* $\lambda[n]$ *is a prime of* $K[n]$ *above* ℓ, $\lambda[n\ell]$ *the unique prime of* $K[n\ell]$ *above* $\lambda[n]$, *and* $\mathrm{Fr}_{\lambda[n]}$ *the Frobenius of* $\lambda[n]$ *in* $\mathrm{Gal}(K[n]/K)$.

Proof. The first claim follows from the theory of complex multiplication, cf. [Sil94, II], and [Wes01a, p.15] for a sketch of the proof. For the other two, see [Wes01a, 5.2] and the preceding discussion. □

For any $n \in \mathcal{N}$, write $\mathcal{G}(n) = \mathrm{Gal}(K[n]/K)$ and $G(n) = \prod_{\ell|n} G_\ell$; from Proposition 4.2.4 we know that $G_\ell \cong \mathrm{Gal}(K[\ell]/K[1])$ is cyclic of order $\ell + 1$, yielding

$$G(n) \cong \mathrm{Gal}(K[n]/K[1]) \quad \text{and} \quad G(n/m) \cong \mathrm{Gal}(K[n]/K[m])$$

for any $m \mid n$. For each ℓ fix a generator σ_ℓ of $G(\ell)$ and define the Kolyvagin derivative operators by

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i, \quad D_n := \prod_{\ell|n} D_\ell.$$

Now put

$$\tilde{\kappa}_n = \sum_{\eta \in \mathcal{G}(n)/G(n)} \eta D_n P[n] \in E(K[n]),$$

where the sum is taken over some choice of coset representatives of $G(n)$ in $\mathcal{G}(n)$. Again, this definition depends on our choice, and we consider this choice fixed throughout the rest of our discussion.

Lemma 8.2.5. *With notation as above and any* $n \in \mathcal{N}$, *the projection of* $\tilde{\kappa}_n$ *in* $E(K[n])/I_nE(K[n])$ *is fixed by* $\mathcal{G}(n)$.

Proof. This is [How04, 1.7.1]. Key to the argument is the observation that the right hand side of

$$(\sigma_\ell - 1)\, D_\ell = \ell + 1 - \sum_{i=0}^{\ell} \sigma_\ell^i$$

is contained in I_ℓ for every $\ell \mid n$. □

From these $\tilde{\kappa}_n$'s we wish to obtain cohomology classes that satisfy the Kolyvagin system relations as described in Definition 4.3.3. To that end, the same reasoning by which we obtained (8.2) yields

$$0 \longrightarrow E(K[n])/I_nE(K[n]) \longrightarrow H^1(K[n], E[I_n]) \longrightarrow H^1(K[n], E)[I_n] \longrightarrow 0.$$

Together with the fact that $E[I_n] \cong T/I_nT$, this gives us the injective Kummer map

$$\delta_n \colon E(K[n])/I_nE(K[n]) \longrightarrow H^1(K[n], T/I_nT).$$

Furthermore, we have

Lemma 8.2.6. *The curve* E *has no nonzero* $K[n]$*-rational* p*-torsion points.*

Proof. This is [Gro91, 4.3], but his proof assumes that $p > 2$. For our more general setting, we instead follow the proof of [DL20, 7.17].

First note that $K[n]/K$ is unramified outside (the prime divisors of) n and $K/\mathbb{Q}$ is unramified outside D, so $K[n]/\mathbb{Q}$ is unramified outside nD. Additionally, it follows from the Néron–Ogg–Shafarevich criterion that $\mathbb{Q}(E[p])/\mathbb{Q}$ is unramified outside pN. By assumption, nD and pN are coprime.

Now suppose that we have a nonzero $Q \in E(K[n])[p]$, and choose a $Q' \in E[p]$ such that $E[p]$ is generated by Q and Q'. Then $\mathrm{Gal}(K[n])$ acts trivially on $\langle Q \rangle \subset E[p]$, so is contained in the kernel of the representation

$G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]/\langle Q' \rangle)$; this implies that $K[n] \supset \mathbb{Q}(Q)$, so $\mathbb{Q}(Q)/\mathbb{Q}$ is unramified outside nD. Simultaneously, $\mathbb{Q}(E[p]) \supset \mathbb{Q}(Q)$, so $\mathbb{Q}(Q)/\mathbb{Q}$ is unramified outside pN. Since nD and pN are coprime, it follows that $\mathbb{Q}(Q)/\mathbb{Q}$ is unramified (outside 1), and thus that $\mathbb{Q}(Q) = \mathbb{Q}$, i.e. $Q \in E(\mathbb{Q})$. But this means that $G_{\mathbb{Q}}$ acts trivially on the subgroup of $E[p]$ generated by Q, hence that $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is not surjective. This contradicts our assumption that $G_K \to \mathrm{Aut}(T_p(E))$ is surjective. □

A nonzero element of $(T/I_nT)^{\mathrm{Gal}(K[n])}$ gives rise to a nonzero point of $E(K[n])[p]$, so by Lemma 8.2.6 it must be that $(T/I_nT)^{\mathrm{Gal}(K[n])} = 0$. Subsequently, the inflation-restriction sequence

$$0 \longrightarrow H^1(K[n]/K, (T/I_nT)^{\mathrm{Gal}(K[n])}) \longrightarrow H^1(K, T/I_nT) \longrightarrow H^1(K[n], T/I_nT)^{\mathcal{G}(n)} \longrightarrow H^2(K[n]/K, (T/I_nT)^{\mathrm{Gal}(K[n])})$$

reduces to an isomorphism

$$H^1(K, T/I_nT) \cong H^1(K[n], T/I_nT)^{\mathcal{G}(n)}.$$

Now, with Lemma 8.2.5 in mind, define $\kappa_n \in H^1(K, T/I_nT)$ to be the preimage of $\delta_n(\tilde{\kappa}_n)$ along the above isomorphism. This cohomology class has the following explicit description.

Proposition 8.2.7 ([McC91, 4.1])**.** *Let $I_n = p^{M_n}\mathbb{Z}_p$ and fix a point $(\tilde{\kappa}_n/p^{M_n}) \in E(\bar{K})$ such that*

$$p^{M_n}\left(\frac{\tilde{\kappa}_n}{p^{M_n}}\right) = \tilde{\kappa}_n.$$

By Lemma 8.2.5, $(\sigma - 1)\tilde{\kappa}_n \in p^{M_n}E(K[n])$ for every $\sigma \in G_K$; let $((\sigma-1)\tilde{\kappa}_n/p^{M_n}) \in E(K[n])$ be the unique point such that

$$p^{M_n}\left(\frac{(\sigma-1)\tilde{\kappa}_n}{p^{M_n}}\right) = (\sigma-1)\tilde{\kappa}_n.$$

Then κ_n has a representative

$$\sigma \longmapsto (\sigma-1)\left(\frac{\tilde{\kappa}_n}{p^{M_n}}\right) - \left(\frac{(\sigma-1)\tilde{\kappa}_n}{p^{M_n}}\right).$$

By [Gro91, 6.2] and [How04, 1.7.3], $\kappa_n \in H^1_{\mathcal{F}(n)}(K, T/I_nT)$ for the geometric Selmer structure $\mathcal{F}$ defined in Section 8.1. However, the κ_n's do not form a Kolyvagin system; they still require a small amount of modification described in [How04, 1.7.4 and 5] to finally give us

Theorem 8.2.8 ([How04, 1.7.5])**.** *With the notation as above, there is a Kolyvagin system κ' for $(T, \mathcal{F}, \mathcal{L}_1)$ with $\kappa'_1 = \kappa_1$.*

By the famous results of Gross and Zagier [GZ86], κ_1 has infinite order precisely when the L-function of E/K (cf. [Sil08, C.16]) has a zero of order 1 at 1. Combined with 8.1.4, we obtain the result that we promised in Section 1.

Theorem 8.2.9. *Suppose that $\mathrm{ord}_{z=1} L(E/K, z) = 1$. Then*

- ***i)*** *$S_p(E/K)$ is a free $\mathbb{Z}_p$-module of rank 1;*
- ***ii)*** *$\mathrm{Sel}_{p^\infty}(E/K) \cong \mathbb{Q}_p/\mathbb{Z}_p \oplus M \oplus M$ for some finite $\mathbb{Z}_p$-module M;*
- ***iii)*** *$\mathrm{len}(2^tM) \leq \mathrm{len}(S_p(E/K)/\kappa_1\mathbb{Z}_p) + (s-t)v_p(2)$.*

8.3 Consequences

Theorem 8.2.9 can now be used to show the conclusion from [Kol89] that if the analytic rank $\mathrm{ord}_{z=1} L(E/K, z)$ of E is 1, then the Shafarevich–Tate group $Ш(E/K)$ is finite and the algebraic (Mordell–Weil) rank of E is also 1. This proves a specific case of two famous conjectures:

Conjecture 8.3.1. *Let E be an elliptic curve defined over K. Then $Ш(E/K)$ is finite.*

Conjecture 8.3.2 (Birch–Swinnerton-Dyer)**.** *The analytic rank of E is equal to its algebraic rank.*

A detailed discussion of these conjectures can be found in e.g. [Sil08, X.4 and C.16]. Rather than the specific cases of these conjectures, however, the second section of Howard's paper [How04] instead focuses on applying his results in the context of Iwasawa theory, proving one divisibility of the equality conjectured by Perrin-Riou [Per87] under his usual assumption that $p > 2$. Although the conjecture itself requires too many preliminaries to state here, it is likely that Howard's proof can be generalized to all primes p using the results presented in this thesis.

9 Conclusion and further research

We began this thesis by recalling results from Galois cohomology and defining local conditions, Selmer structures, Selmer triples and finally Kolyvagin systems. The nature of the ring our modules were defined over had no significance, until we formulated hypothesis (eigen) in Section 5.3. We partially managed to remedy the discrepancy between odd and even residue characteristics p by considering modules over $R/2\mathfrak{m}$ instead of $R/\mathfrak{m}$, which ensured that multiplication by $+1$ and -1 act differently even when $p = 2$. However, without a splitting into eigenspaces like we have for $p > 2$, we were unable to prove Conjecture 6.3.4 for $p = 2$.

In Section 7.2, we also saw that our intermediate results were insufficient to prove Conjecture 7.2.2 for $p = 2$, again in large part because that scenario does not permit the same direct sum decomposition into eigenspaces that we have when p is odd.

Still, under the assumption of those conjectures, we arrived at a meaningful generalization of Howard's results, in the form of Theorem 7.3.3. This was then applied to obtain a bound on the Selmer module of an elliptic curve; with only a minor additional assumption on the discriminant, Howard's original arguments generalized almost immediately. In particular, the Heegner point Kolyvagin system constructed in [How04] is valid for all primes p, ultimately yielding Theorem 8.2.9.

Naturally, ambitious readers are encouraged to seek a proof of Conjectures 6.3.4 and 7.2.2, or of weaker results that are still sufficient to deduce our final theorem.

Additionally, it should be noted that we only discussed the first part of [How04] in detail, and only briefly touched upon the Iwasawa theory of [How04, Section 2] in Section 8.3. Given our generalization of Howard's Theorem A for some imaginary quadratic field K, it would be worth investigating how our results extend from K to its anticyclotomic $\mathbb{Z}_p$-extension in order to deduce a generalization of [How04, Theorem B], which would generalize a partial proof of the Perrin-Riou conjecture.

Furthermore, generalizations of Kolyvagin's results to different classes of (higher-dimensional) abelian varieties are presented in [KL92] and conjectured in [Log05]. It would be worth investigating how Theorem 7.3.3 can be used to prove those generalizations, in the same way we used it in Section 8 to prove Kolyvagin's original result for elliptic curves.

Bibliography

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. First edition. Addison–Wesley Series in Mathematics. Addison–Wesley, 1969.

[Bre+01] Christophe Breuil et al. "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises". In: *Journal of the Mathematical Society* 14.4 (2001).

[Bro93] William C. Brown. *Matrices over commutative rings*. First edition. Vol. 169. Pure and Applied Mathematics: A Series of Monographs and Textbooks. Marcel Dekker, 1993.

[Cas65] John W. S. Cassels. "Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer". In: *Journal für die reine und angewandte Mathematik* 217 (1965).

[CS00] John H. Coates and Ramdorai Sujatha. *Galois Cohomology of Elliptic Curves*. First edition. Narosa Publishing House, 2000.

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor. "Modularity of certain Barsotti–Tate Galois representations". In: *Journal of the Mathematical Society* 12.2 (1999).

[Con] Keith Conrad. "The conductor ideal of an order". Available at https://swc-math.github.io/aws/2001/notes.html.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. First edition. John Wiley & Sons, 1989.

[DL20] Netan Dogra and Samuel Le Fourn. "Quadratic Chabauty for modular curves and modular forms of rank one". In: *Mathematische Annalen* 380 (2020).

[Gro91] Benedict H. Gross. "Kolyvagin's work on modular elliptic curves". In: *L-functions and Arithmetic*. Proceedings of the Durham Symposium, July, 1989. Ed. by John H. Coates and Martin J. Taylor. Vol. 153. London Mathematical Society Lecture Notes Series. Cambridge University Press, 1991.

[GZ86] Benedict H. Gross and Don B. Zagier. "Heegner points and derivatives of L-series". In: *Inventiones Mathematicae* 84.2 (1986).

[How04] Benjamin Howard. "The Heegner point Kolyvagin system". In: *Compositio Mathematica* 141.6 (2004).

[Kol89] Victor A. Kolyvagin. "Finiteness of $E(\mathbb{Q})$ and Ш$(E, \mathbb{Q})$ for a subclass of Weil curves". In: *Mathematics of the USSR-Izvestiya* 32.3 (1989).

[KL92] Victor A. Kolyvagin and Dmitry Logachev. "Finiteness of Ш over totally real fields". In: *Mathematics of the USSR-Izvestiya* 39.1 (1992).

[Lan02] Serge Lang. *Algebra*. Revised third edition. Graduate Texts in Mathematics. Springer-Verlag, 2002.

[Liu06] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. First edition. Vol. 6. Oxford Graduate Texts in Mathematics. Oxford University Press, 2006.

[Log05] Dmitry Logachev. "Reduction of a problem of finiteness of Tate–Shafarevich group to a result of Zagier type". Available at https://arxiv.org/abs/math/0411346. 2005.

[MR04] Barry Mazur and Karl Rubin. "Kolyvagin Systems". In: *Memoirs of the American Mathematics Society* 168.799 (2004).

[MR16] Barry Mazur and Karl Rubin. "Controlling Selmer groups in the higher core rank case". In: *Journal de théorie des nombres de Bordeaux* 28.1 (2016).

[McC91] William G. McCallum. "Kolyvagin's work on Shararevich–Tate groups". In: *L-functions and Arithmetic*. Proceedings of the Durham Symposium, July, 1989. Ed. by John H. Coates and Martin J. Taylor. Vol. 153. London Mathematical Society Lecture Notes Series. Cambridge University Press, 1991.

[Mil06] James S. Milne. *Arithmetic Duality Theorems*. Second edition. Available at https://www.jmilne.org/math/Books/index.html. BookSurge Publishing, 2006.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Trans. by Norbert Schappacher. First translated edition. Vol. 322. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1999.

[NSW20] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Second edition, corrected version 2.3. Vol. 323. Grundlehren der mathematischen Wissenschaften. Available at https://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/index-de.html. Springer-Verlag, 2020.

[Per87] Bernadette Perrin-Riou. "Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner". In: *Bulletin de la Société Mathématique de France* 115 (1987).

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

[Rub09] Karl Rubin. "Euler systems and Kolyvagin systems". In: IAS/Park City Mathematics Series. American Mathematical Society, 2009.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. First edition. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, 1994.

[Sil08] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Second edition. Vol. 106. Graduate Texts in Mathematics. Springer-Verlag, 2008.

[Ste20] Peter Stevenhagen. "Number rings". Available at https://websites.math.leidenuniv.nl/algebra/. 2020.

[Tat62] John Tate. "Duality theorems in Galois cohomology over number fields". In: Proceedings in the International Congress of Mathematicians. American Mathematical Society, 1962.

[Wes01a] Tom Weston. "The Euler system of Heegner points". Available at https://swc-math.github.io/aws/2001/notes.html. 2001.

[Wes01b] Tom Weston. "The modular curves $X_0(11)$ and $X_1(11)$". Available at https://swc-math.github.io/aws/2001/notes.html. 2001.

[Wil95] Andrew J. Wiles. "Modular elliptic curves and Fermat's Last Theorem". In: *Annals of Mathematics* 141 (1995).

[Zho23] Peter Zhou. "The modularity theorem". Available at https://math.uchicago.edu/~may/REU2023/. 2023.