Kolyvagin Systems

Barry Mazur

Karl Rubin

Author address:

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA
E-mail address: mazur@math.harvard.edu

Department of Mathematics, Stanford University, Stanford, CA 94305 USA
E-mail address: rubin@math.stanford.edu

Contents

Introduction 1
0.1. Selmer sheaves and Kolyvagin systems 1
0.2. Resemblance to the leading term of an L-function 2
0.3. Applications 3
0.4. Layout of the paper 4
0.5. Notation 5
0.6. Acknowledgments 5

Chapter 1. Local Cohomology Groups 7
1.1. Local conditions 7
1.2. The finite/singular homomorphism 10
1.3. Local duality 11

Chapter 2. Global Cohomology Groups and Selmer Structures 13
2.1. Selmer modules 13
2.2. Comparing Selmer modules 16
2.3. Global duality 16

Chapter 3. Kolyvagin Systems 19
3.1. Kolyvagin systems 19
3.2. Euler systems and Kolyvagin systems 23
3.3. Simplicial sheaves and Selmer groups 24
3.4. Sheaves and monodromy 26
3.5. Hypotheses on T, $\mathcal{F}$, and $\mathcal{P}$ 27
3.6. Choosing useful primes 30
3.7. Some remarks about hypothesis (H.6) 33

Chapter 4. Kolyvagin Systems over Principal Artinian Rings 35
4.1. The core Selmer module 35
4.2. Kolyvagin systems and the core rank 40
4.3. The sheaf of stub Selmer modules 41
4.4. Kolyvagin systems and the stub Selmer sheaf 45
4.5. Kolyvagin systems over principal artinian rings 48

Chapter 5. Kolyvagin Systems over Integral Domains 55
5.1. Kolyvagin systems over a field 55
5.2. Kolyvagin systems over a discrete valuation ring 56
5.3. Kolyvagin systems over Λ 60

Chapter 6. Examples 69
6.1. The multiplicative group 69

6.2. Elliptic curves 73
6.3. The multiplicative group, revisited 76

Appendix A. Proof of Theorem 3.2.4 79

Appendix B. Proof of Theorem 4.3.3, by Benjamin Howard 89

Bibliography 95

Abstract

Since their introduction by Kolyvagin, Euler systems have been used in several important applications in arithmetic algebraic geometry. For a p-adic Galois module T, Kolyvagin's machinery is designed to provide an upper bound for the size of the Selmer group associated to the Cartier dual T^*.

Given an Euler system, Kolyvagin produces a collection of cohomology classes which he calls "derivative" classes. It is these derivative classes which are used to bound the dual Selmer group.

The starting point of the present memoir is the observation that Kolyvagin's systems of derivative classes satisfy stronger interrelations than have previously been recognized. We call a system of cohomology classes satisfying these stronger interrelations a *Kolyvagin system*. We show that the extra interrelations give Kolyvagin systems an interesting rigid structure which in many ways resembles (an enriched version of) the "leading term" of an L-function.

By making use of the extra rigidity we also prove that Kolyvagin systems exist for many interesting representations for which no Euler system is known, and further that there are Kolyvagin systems for these representations which give rise to exact formulas for the size of the dual Selmer group, rather than just upper bounds.

Received by the editor November 2, 2002.

2000 *Mathematics Subject Classification.* Primary 11G40, 11F80; Secondary 11R23, 11R34, 11R42.

Introduction

Since their introduction by Kolyvagin in [**Ko**], Euler systems have been used in several important applications in arithmetic algebraic geometry ([**Ko**], [**Ka2**], [**Ru3**]). For a p-adic Galois module T attached to a motive over a number field K, Kolyvagin's machinery is designed to provide an upper bound for the size of the p^n-Selmer group associated to the Cartier dual T^* (for any $n > 0$), and it proceeds in three steps.

The first step is to establish an Euler system as input to his machine. Kolyvagin used the "classical" Euler systems of cyclotomic units, elliptic units, and Heegner points. More recently Kato constructed an Euler system of classes of algebraic K-theory attached to elliptic curves [**Ka2**]. This input provides one with a large collection of cohomology classes over abelian extensions of the base field K.

The second step gives as intermediate output a new collection of cohomology classes, which Kolyvagin calls "derivative" classes, this time over K itself with coefficients in certain quotient Galois modules.

The third step uses this system of derivative classes to obtain an upper bound on the size of the p^n-Selmer group attached to T^*, by constructing a large collection of linear functionals (on direct sums of local cohomology groups of the kernel of multiplication by p^n in T^*) with the property that the image of the Selmer group in question is in the kernel of these linear functionals.

The starting point of the present paper is the observation that Kolyvagin's systems of derivative classes satisfy stronger interrelations than have previously been recognized. If one defines (as we will) a *Kolyvagin system* to be a system of cohomology classes satisfying these stronger interrelations, one obtains an interesting rigid structure which in many ways resembles (an enriched version of) the "leading term" of an L-function. In this introduction we will try to explain what we mean by this, leaving precise definitions and assumptions to the main text of the article.

0.1. Selmer sheaves and Kolyvagin systems

Suppose R is a complete noetherian local ring with finite residue field of characteristic p, and T is a free R-module of finite rank with a continuous action of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

Imposing local conditions on cohomology classes in $H^1(\mathbf{Q}, T)$ allows us to define the basic Selmer R-module $\mathcal{H}(1) \subset H^1(\mathbf{Q}, T)$. The reason for the adjective "basic," and the "1" in the notation, is that this basic Selmer module is just one of a constellation of interrelated Selmer modules which are essential to the understanding of Kolyvagin systems. Namely, let $\mathcal{N}$ be the set of squarefree positive integers that are divisible only by primes where T is unramified. For every $n \in \mathcal{N}$ we define a Selmer module $\mathcal{H}(n) \subset H^1(\mathbf{Q}, T/I_nT)$ (where I_n is an explicitly defined ideal of R) by modifying the local Selmer conditions at primes dividing n.

Let $\mathcal{X}$ denote the graph whose set of vertices is $\mathcal{N}$, and whose edges join vertices of the form n and $n\ell$, where ℓ is prime. We package our Selmer modules into a natural sheaf of R-modules on the graph $\mathcal{X}$, which we denote by $\mathcal{H}$. The stalk at n is $\mathcal{H}(n)$, and if n and $n\ell$ are joined by an edge then there are homomorphisms comparing $\mathcal{H}(n)$ and $\mathcal{H}(n\ell)$. A Kolyvagin system for T is then defined to be a global section of $\mathcal{H}$, or in other words a collection of cohomology classes $\kappa_n \in \mathcal{H}(n) \subset H^1(\mathbf{Q}, T/I_nT)$ that are coherent with respect to the maps comparing $\mathcal{H}(n)$ and $\mathcal{H}(n\ell)$. We show that under suitable hypotheses an Euler system give rises (via Kolyvagin's construction) to a Kolyvagin system.

Denote by $\mathbf{KS}(T)$ the R-module of Kolyvagin systems for T. If R is a principal ideal domain then $\mathbf{KS}(T)$ is controlled by a single cohomological invariant $\chi(T)$ (see Definitions 4.1.8 and 4.1.11) which we call the *core rank* of T. The core rank is characterized by the fact that for every n (resp., for infinitely many n) the Selmer module $\mathcal{H}(n)$ contains (resp., is) a free R/I_n-module of rank $\chi(T)$. If R is a discrete valuation ring or a finite field, then under suitable hypotheses (see §3.5) we show (Theorems 5.2.10 and 5.1.1)[1] that if $\chi(T)$ is zero or one then $\mathbf{KS}(T)$ is a free R-module of rank $\chi(T)$. The case of core rank one occurs frequently in classical examples, and in that case we conclude that Kolyvagin systems exist and that there is a "primitive" one unique up to multiplication by a unit in R. This proves the existence of Kolyvagin systems for many interesting Galois representations T.

The rigid structure of Kolyvagin systems has surprised us. Here is an example of this. If R is a principal ideal domain, M an R-module, and r a nonnegative integer, define the *r-stub* of M to be the (unique) maximal R-submodule of M of the form $\mathfrak{m}^{\mathrm{length}(M/N)}M$, where $\mathfrak{m}$ is the maximal ideal of R and $N \subset M$ ranges over submodules of M that can be generated by r elements. The r-stub of M is a canonical submodule which can be generated by r elements. For example, if R is a field then the r-stub of M is M itself if $\dim_R(M) \leq r$, and zero otherwise.

Returning to our Selmer sheaf when R is a discrete valuation ring or a field, write $\mathcal{H}'(n)$ for the $\chi(T)$-stub of $\mathcal{H}(n)$. There is a natural sub-sheaf of R-modules $\mathcal{H}' \subset \mathcal{H}$ whose stalks are precisely the $\mathcal{H}'(n)$. Under fairly general hypotheses, we show (Theorems 4.4.1 and 4.4.3) that Kolyvagin systems (i.e., global sections of $\mathcal{H}$) are in fact sections of the sub-sheaf $\mathcal{H}'$. In other words, if $\boldsymbol{\kappa}$ is a Kolyvagin system then κ_n lies in the $\chi(T)$-stub $\mathcal{H}'(n)$ for every n. A Kolyvagin-type bound on the size of the Selmer module attached to T^* follows directly from this (Corollary 4.4.5).

If R is a field then every stub Selmer module $\mathcal{H}'(n)$ is either an R-vector space of dimension $\chi(T)$ or zero. In the special case mentioned above where R is a discrete valuation ring or a field and $\chi(T) = 1$, the stub Selmer modules $\mathcal{H}(n)$ are all cyclic, and for a primitive Kolyvagin system κ_n generates $\mathcal{H}'(n)$ for every n.

0.2. Resemblance to the leading term of an L-function

With notation as above, consider the following definitions.

- The *R-module of L-values* $\mathcal{L} \subset \mathcal{H}(1)$ is the image of the map $\mathbf{KS}(T) \to \mathcal{H}(1)$ that sends a Kolyvagin system $\boldsymbol{\kappa}$ to its value κ_1 in the stalk over the vertex 1.
- The *order of vanishing* of $\boldsymbol{\kappa}$ is $\min\{\nu(n) : \kappa_n \neq 0\}$ where $\nu(n)$ is the number of prime divisors of n,

[1] An essential step (Theorem 4.3.3) in the proof of this was supplied by Benjamin Howard. The authors thank him for including his proof of this result in Appendix B.

- If R is principal we will define a sequence of *elementary divisors* of $\boldsymbol{\kappa}$ (see Definitions 4.5.7 and 5.2.11).
- In §3.3 we give an explicit functorial construction of an R-module we call the *Kolyvagin-constructed dual Selmer module* attached to a Kolyvagin system.
- If I is an ideal of R then a Kolyvagin system for T gives a Kolyvagin system for the R/I-module T/IT. We will define the *blind spot* of $\mathbf{KS}(T)$. As a first approximation (see in Definition 3.1.5 for the precise definition), the blind spot is the set of ideals $I \subset R$ such that the natural homomorphism $\mathbf{KS}(T) \to \mathbf{KS}(T/IT)$ is identically zero.

We now attempt to justify the terminology of these definitions. Write $T^* = \mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty})$ for the Cartier dual of T. The choice of local Selmer conditions which we used to define the Selmer module $\mathcal{H}(1)$ provides also (by local duality) local Selmer conditions which we can use to define a Selmer module $\mathrm{Sel}(T^*) \subset H^1(\mathbf{Q}, T^*)$. (Hidden in the discussion above, but essential for the understanding of the Selmer sheaf $\mathcal{H}$, is the dual Selmer sheaf with stalks $\mathcal{H}^*(n) \subset H^1(\mathbf{Q}, T^*[I_n])$, where $\mathcal{H}^*(1) = \mathrm{Sel}(T^*)$.)

If R is a discrete valuation ring and $\chi(T) = 1$, then we show (see Theorem 5.2.14) that under suitable hypotheses the Fitting ideal of the quotient $\mathcal{H}(1)/\mathcal{L}$ of the Selmer module by the submodule of L-values is equal to the Fitting ideal of the Pontrjagin dual $\mathrm{Hom}(\mathrm{Sel}(T^*), \mathbf{Q}_p/\mathbf{Z}_p)$. If R is a discrete valuation ring or a field, $\chi(T) = 1$, and $\boldsymbol{\kappa}$ is a nonzero Kolyvagin system, then the R-corank of $\mathrm{Sel}(T^*)$ is the order of vanishing of $\boldsymbol{\kappa}$, and the elementary divisors of the quotient of $\mathrm{Sel}(T^*)$ by its maximal divisible submodule are the elementary divisors of $\boldsymbol{\kappa}$ (Theorem 5.2.12).

We will construct a map from the classical Selmer module $\mathrm{Sel}(T^*)$ to the Pontrjagin dual of our Kolyvagin-constructed dual Selmer module which, in good cases, we show to be an isomorphism (Theorem 4.5.12). I.e., in good cases we give a functorial construction of $\mathrm{Sel}(T^*)$ from the data given by a Kolyvagin system.

When the blind spot is nonempty we expect that our Kolyvagin-constructed dual Selmer module may be larger than the dual of $\mathrm{Sel}(T^*)$. It would be interesting to understand whether there is a connection between our Kolyvagin-constructed module and the extended Selmer modules defined by Nekovář in [**Ne**].

If R is an Iwasawa algebra, then the blind spot is related to the "exceptional zeros" of p-adic L-functions, and (as usual with suitable hypotheses) we show (Theorem 5.3.10) that away from the blind spot, the Fitting ideal of $\mathcal{H}(1)/\mathcal{L}$ is equal to the Fitting ideal of the Pontrjagin dual $\mathrm{Hom}(\mathrm{Sel}(T^*), \mathbf{Q}_p/\mathbf{Z}_p)$.

0.3. Applications

As discussed above, in "good" situations we get an equality of Fitting ideals

$$\mathrm{Fitt}(\mathcal{H}(1)/\mathcal{L}) = \mathrm{Fitt}(\mathrm{Sel}(T^*)).$$

If we have one Kolyvagin system, then we have one element of $\mathcal{L}$, and we get an upper bound for $\mathrm{Fitt}(\mathrm{Sel}(T^*))$ exactly as in the traditional application of an Euler system. But if we know *all* of $\mathcal{L}$, then we can determine $\mathrm{Fitt}(\mathrm{Sel}(T^*))$ exactly. In particular if the one Kolyvagin system we know is primitive, then it generates $\mathbf{KS}(T)$ and hence gives all of $\mathcal{L}$.

For example, fix an elliptic curve E defined over $\mathbf{Q}$ and let T be the p-adic Tate module $T_p(E)$ of E. Take $R = \mathbf{Z}_p$, and assume further that the p-adic representation $G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$ is surjective. Then all of the hypotheses mentioned above hold, and the core rank $\chi(T_p(E))$ is 1. Let $\boldsymbol{\kappa}^{\mathrm{Kato}} \in \mathbf{KS}(T_p(E))$ be the Kolyvagin system constructed from Kato's Euler system [**Ka2**]. If we have further that

$$\boldsymbol{\kappa}^{\mathrm{Kato}} \text{ is primitive} \tag{*}$$

(i.e., if there is at least one n such that κ_n^{Kato} is nonzero in $H^1(\mathbf{Q}, E[p])$), then the reasoning above shows that Kato's upper bound for the order of the Selmer group of E is sharp (Theorem 6.2.4).

In fact, the upper bound of Theorem 6.2.4 should not always be sharp, because it does not include the Tamagawa factors in the Birch and Swinnerton-Dyer conjecture. In Proposition 6.2.6 we show directly that if at least one of the Tamagawa factors is divisible by p, then $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is not primitive.

Continuing with the elliptic curve example, take R now to be the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$, where $\mathbf{Q}_\infty$ is the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$, and $T = T_p(E) \otimes \Lambda$. Kato's Euler system provides a Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Kato},\infty} \in \mathbf{KS}(T_p(E) \otimes \Lambda)$ and reasoning as above we deduce (Theorem 6.2.7) that if (*) holds (in fact a slightly weaker hypothesis suffices) then the Iwasawa main conjecture (relating the p-adic L-function of E with the p-power Selmer group of E over $\mathbf{Q}_\infty$) holds.

0.4. Layout of the paper

In Chapters 1 and 2 we introduce the local and global cohomology groups we will use, and recall basic facts about them. In particular in §2.1 we introduce the concept of a Selmer structure on a Galois module and its corresponding Selmer module.

In Chapter 3 we introduce the Selmer sheaf and Kolyvagin systems. In §3.2 we describe the connection between Euler systems and Kolyvagin systems, although the proof that the derivative classes of an Euler system form a Kolyvagin system is postponed until Appendix A. In §3.3 we define our Kolyvagin-constructed dual Selmer module. Section 3.4 studies general properties of sheaves on graphs, and §3.5 discusses several simplifying assumptions which we will make in most of the remainder of the paper.

In Chapter 4 we study Kolyvagin systems in their simplest setting, where the ring R of coefficients is a principal artinian local ring (for example, $\mathbf{Z}/p^k\mathbf{Z}$). We introduce our fundamental cohomological invariant, the "core rank" of T, in §4.1, and in the following sections we show that the rank of the R-module of Kolyvagin systems is zero, one, or infinity according as the core rank is zero, one, or greater than one, respectively. Along the way we prove in §4.4 that a Kolyvagin system, a priori a global section of the Selmer sheaf, is actually a global section of the stub-subsheaf. This extra information allows us in §4.5 to recover the structure of the Selmer group of T^* from a Kolyvagin system for T.

In Chapter 5 we prove analogous results first in the case where the ring of coefficients R is a discrete valuation ring (by reducing to quotients of R which are principal artinian local rings), and then in the case where R is an Iwasawa algebra (by reducing to quotients of R which are subrings of discrete valuation rings).

Finally, in Chapter 6 we illustrate our results with the basic examples: cyclotomic units and ideal class groups in §6.1, and then Kato's Kolyvagin system and Selmer groups of elliptic curves in §6.2. The reader may find it useful to follow these examples while reading the paper, rather than waiting until the end.

0.5. Notation

Fix a rational prime p. Throughout this paper, R will denote a complete, noetherian, local ring with finite residue field of characteristic p. Let $\mathfrak{m}$ denote the maximal ideal of R and $\Bbbk = R/\mathfrak{m}$ the residue field. The basic cases to keep in mind are $R = \mathbf{F}_p$, $R = \mathbf{Z}_p$, and $R = \Lambda$, a suitable Iwasawa algebra.

If A is an R-module and $x \in A$, then $\mathrm{Ann}_R(x) \subset R$ will denote the annihilator of x. If I is an ideal of R, we will write $A[I]$ for the submodule of A killed by I. If A is a $G_{\mathbf{Q}}$-module, we write $\mathbf{Q}(A)$ for the fixed field in $\bar{\mathbf{Q}}$ of the kernel of the map $G_{\mathbf{Q}} \to \mathrm{Aut}(A)$.

If a group H acts on a set X, then the subset of elements of X fixed by H is denoted X^H.

We write $\nu(n)$ for the number of distinct prime factors of a nonzero integer n.

0.6. Acknowledgments

The authors thank Benjamin Howard for his helpful comments on an earlier version of this paper, and the NSF for financial support.

CHAPTER 1

Local Cohomology Groups

For §§1.1-1.3, K will be a local field (archimedean or nonarchimedean), $\bar{K}$ a fixed separable algebraic closure of K, and $G_K = \mathrm{Gal}(\bar{K}/K)$.

If K is nonarchimedean let $\mathcal{O}$ be the ring of integers in K, $\mathbf{F}$ its residue field, and $K^{\mathrm{unr}} \subset \bar{K}$ the maximal unramified subfield of $\bar{K}$. Let $\mathcal{I}$ denote the inertia group $\mathrm{Gal}(\bar{K}/K^{\mathrm{unr}})$, and $G_{\mathbf{F}} = \mathrm{Gal}(K^{\mathrm{unr}}/K)$. These groups fit into the exact sequence

$$\{1\} \longrightarrow \mathcal{I} \longrightarrow G_K \longrightarrow G_{\mathbf{F}} \longrightarrow \{1\}. \tag{1}$$

Note that if $\bar{\mathbf{F}}$ is an algebraic closure of $\mathbf{F}$, then $G_{\mathbf{F}} \cong \mathrm{Gal}(\bar{\mathbf{F}}/\mathbf{F}) \cong \hat{\mathbf{Z}}$ (the latter isomorphism sending the Frobenius automorphism in $\mathrm{Gal}(\bar{\mathbf{F}}/\mathbf{F})$, $x \mapsto x^{|\mathbf{F}|}$, to $1 \in \hat{\mathbf{Z}}$).

Let T be an R-module endowed with a continuous G_K-action. By $H^*(K,T) = H^*(G_K,T)$ we mean cohomology computed with respect to continuous cochains. If K is nonarchimedean, the vanishing of $H^2(G_{\mathbf{F}}, T^{\mathcal{I}})$ yields the canonical exact sequence

$$0 \longrightarrow H^1(G_{\mathbf{F}}, T^{\mathcal{I}}) \longrightarrow H^1(K,T) \longrightarrow H^1(\mathcal{I},T)^{G_{\mathbf{F}}} \longrightarrow 0. \tag{2}$$

1.1. Local conditions

Definition 1.1.1. A *local condition* on T (over K) is a choice of an R-submodule of $H^1(K,T)$. If we refer to the local condition by a symbol, say $\mathcal{F}$, we will denote the corresponding R-submodule

$$H^1_{\mathcal{F}}(K,T) \subset H^1(K,T).$$

If $\mathcal{T}$ is a category whose objects are certain R-modules endowed with continuous R-linear G_K-action (and possibly equipped with further structure) and whose morphisms are certain R-module homomorphisms, a *local condition functorial over* $\mathcal{T}$ will mean a subfunctor (of one-dimensional G_K-cohomology)

$$T \mapsto H^1_{\mathcal{F}}(K,T) \subset H^1(K,T)$$

where T ranges through the objects of the category $\mathcal{T}$.

Example 1.1.2. Suppose T is an $R[[G_K]]$-module as above, and $\mathcal{F}$ is a local condition on T. If T' is a submodule of T and T'' is a quotient module, then $\mathcal{F}$ induces local conditions (also denoted by $\mathcal{F}$) on T' and T'', by taking $H^1_{\mathcal{F}}(K,T')$ and $H^1_{\mathcal{F}}(K,T'')$ to be the inverse image and image, respectively, of $H^1_{\mathcal{F}}(K,T)$ in $H^1(K,T')$ and $H^1_{\mathcal{F}}(K,T'')$ under the maps induced by

$$T' \hookrightarrow T, \qquad T \twoheadrightarrow T''.$$

In other words the local condition $\mathcal{F}$ "propagates" to submodules and quotients of T.

In particular if I is an ideal of R, then a local condition on T induces local conditions on T/IT and $T[I]$.

One can similarly propagate the local condition $\mathcal{F}$ to arbitrary subquotients of T. Namely, if $T_1 \subset T_2 \subset T$, then one can define a local condition on T_2/T_1 either by viewing it as a quotient of the submodule T_2 of T, or as a submodule of the quotient T/T_1 of T. It is an exercise to show that these two choices define the same local condition on the subquotient T_2/T_1.

Similarly, if $R \to R'$ is a homomorphism of complete noetherian local rings, then $\mathcal{F}$ induces a local condition on the R'-module $T \otimes_R R'$ by taking $H^1_{\mathcal{F}}(K, T \otimes R')$ to be the image in $H^1(K, T \otimes R')$ of $H^1_{\mathcal{F}}(K, T) \otimes R'$.

EXAMPLE 1.1.3. Let $\mathrm{Quot}_R(T)$ be the category whose objects are quotients T/IT for all ideals I of R, and where the morphisms from T/IT to T/JT consist of all scalar multiplications r such that $rI \subset J$. It is immediate that the local condition $\mathcal{F}$, propagated to the category $\mathrm{Quot}_R(T)$, is functorial over $\mathrm{Quot}_R(T)$.

Similarly one can define categories of submodules and subquotients of T, and again the propagated local conditions are functorial.

DEFINITION 1.1.4. A local condition $\mathcal{F}$ is *cartesian* on a category $\mathcal{T}$ of $R[[G_K]]$-modules (or on a category of such modules equipped with some extra structure) if $\mathcal{F}$ is functorial over $\mathcal{T}$ and for any injective $R[[G_K]]$-module homomorphism (in the category $\mathcal{T}$) $\alpha : T_1 \to T_2$ the square

$$\begin{array}{ccc} H^1_{\mathcal{F}}(K, T_1) & \hookrightarrow & H^1(K, T_1) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ H^1_{\mathcal{F}}(K, T_2) & \hookrightarrow & H^1(K, T_2) \end{array}$$

is cartesian.

Equivalently, $\mathcal{F}$ is cartesian on $\mathcal{T}$ if whenever $\alpha : T_1 \to T_2$ is injective, the local condition $\mathcal{F}$ on T_1 is the same as the local condition obtained by propagating $\mathcal{F}$ from T_2 to T_1.

LEMMA 1.1.5. *Suppose R is principal and artinian of length k, and suppose that the local condition $\mathcal{F}$ is cartesian on the category* $\mathrm{Quot}_R(T)$ *of Example 1.1.3. Then there is an integer r such that for $0 < i \leq k$,*

$$\mathrm{length}(H^0(K, T/\mathfrak{m}^i T)) - \mathrm{length}(H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T)) = ri$$

(where we use the same symbol $\mathcal{F}$ to denote the local condition propagated to all quotients of T).

PROOF. Let $\lambda(i) = \mathrm{length}(H^0(K, T/\mathfrak{m}^i T)) - \mathrm{length}(H^1_{\mathcal{F}}(K, T/m^i T))$.

Suppose $i, j \in \mathbf{Z}^+$ and $i + j \leq k$. Using the cartesian condition (for exactness in the center) and the definition of the propagation of $\mathcal{F}$ to $T/\mathfrak{m}^j T$ (for exactness on the right), the long exact cohomology sequence arising from

$$0 \longrightarrow T/\mathfrak{m}^i T \longrightarrow T/\mathfrak{m}^{i+j} T \longrightarrow T/\mathfrak{m}^j T \longrightarrow 0$$

restricts to an exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(K, T/\mathfrak{m}^i T) \longrightarrow H^0(K, T/\mathfrak{m}^{i+j} T) \longrightarrow H^0(K, T/\mathfrak{m}^j T) \\ \longrightarrow H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T) \longrightarrow H^1_{\mathcal{F}}(K, T/\mathfrak{m}^{i+j} T) \longrightarrow H^1_{\mathcal{F}}(K, T/\mathfrak{m}^j T) \longrightarrow 0. \end{aligned}$$

Thus $\lambda(i) + \lambda(j) = \lambda(i + j)$, and the lemma follows. □

DEFINITION 1.1.6. Most (but not all) of the local conditions we deal with in this paper will be of the following form. Suppose L is a (possibly infinite) extension of K in $\bar{K}$, and define

$$H^1_L(K,T) = H^1(L/K, T^{G_L}) = \ker[H^1(K,T) \to H^1(L,T)] \subset H^1(K,T).$$

It is clear that for every L this defines a local condition functorial over any category of $R[[G_K]]$-modules.

We have the following important special cases.

(i) the *unrestricted* or *relaxed* condition ($L = \bar{K}$)

$$H^1_{\text{relaxed}}(K,T) = H^1_{\bar{K}}(K,T) = H^1(K,T),$$

(ii) the *strict* condition ($L = K$)

$$H^1_{\text{strict}}(K,T) = H^1_K(K,T) = 0 \subset H^1(K,T),$$

(iii) the *unramified* condition ($L = K^{\text{unr}}$)

$$H^1_{\text{unr}}(K,T) = H^1_{K^{\text{unr}}}(K,T) = H^1(G_{\mathbf{F}}, T^I) \subset H^1(K,T).$$

If K is nonarchimedean and T is unramified (i.e., $\mathcal{I}$ acts trivially on T), we will also call this the *finite* condition and write $H^1_{\text{f}}(K,T) = H^1_{\text{unr}}(K,T) = H^1(G_{\mathbf{F}}, T)$.

(iv) the *L-transverse* condition (K nonarchimedean, and L/K totally ramified and abelian of degree $|\mathbf{F}^\times|$)

$$H^1_{L-\text{tr}}(K,T) = H^1_L(K,T) \subset H^1(K,T).$$

When $K = \mathbf{Q}_\ell$ and $L = \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)$, we will call this simply the *transverse* condition and write $H^1_{\text{tr}}(\mathbf{Q}_\ell, T) = H^1_{\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)}(\mathbf{Q}_\ell, T)$.

Suppose now that K is nonarchimedean and T is unramified. We will call the R-submodule $H^1_{\text{f}}(K,T)$ the *finite* part of $H^1(K,T)$, and we call the quotient $H^1_{\text{s}}(K,T) = H^1(K,T)/H^1_{\text{f}}(K,T) \cong H^1(\mathcal{I},T)^{G_{\mathbf{F}}}$ the *singular quotient* of $H^1(K,T)$. The exact sequence (2) thus can be written in this case as

$$0 \longrightarrow H^1_{\text{f}}(K,T) \longrightarrow H^1(K,T) \longrightarrow H^1_{\text{s}}(K,T) \longrightarrow 0. \tag{3}$$

If $c \in H^1(K,T)$ its image under projection to $H^1_{\text{s}}(K,T)$ will be denoted $c_{\text{s}} \in H^1_{\text{s}}(K,T)$.

REMARK 1.1.7. The unrestricted, strict, and unramified local conditions can be expressed as étale one-dimensional cohomology over Spec $\mathcal{O}$ of natural sheaf-theoretic extensions to Spec $\mathcal{O}$ of the G_K-module T viewed as an étale sheaf over Spec K. This does not seem to be the case with the transverse conditions.

REMARK 1.1.8. In general the local condition defined by an extension L of K will not be cartesian, nor will the propagation of the L-condition on a module T to its subquotients (see Example 1.1.2) coincide with the L-condition on the subquotients. However, for the finite condition we have the following lemma.

LEMMA 1.1.9. (i) *Suppose T is an unramified $R[[G_K]]$-module and T' is a subquotient of T. Then the local condition induced on T' by the finite condition on T is the same as the finite condition on T',*

(ii) *The finite condition is cartesian on any category of unramified $R[[G_K]]$-modules.*

PROOF. Suppose $T_1 \to T_2$ is a map of unramified $R[[G_K]]$-modules. Since they are unramified, the definition of H^1_{f} gives a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1_{\mathrm{f}}(K,T_1) & \longrightarrow & H^1(K,T_1) & \xrightarrow{d_1} & \mathrm{Hom}(\mathcal{I},T_1) \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} \\ 0 & \longrightarrow & H^1_{\mathrm{f}}(K,T_2) & \longrightarrow & H^1(K,T_2) & \xrightarrow{d_2} & \mathrm{Hom}(\mathcal{I},T_2). \end{array}$$

If $T_1 \twoheadrightarrow T_2$ is surjective, then $\mathrm{coker}(a) = H^2(K^{\mathrm{unr}}/K, \ker[T_1 \to T_2]) = 0$, and so $H^1_{\mathrm{f}}(K,T_2)$ is the image of $H^1_{\mathrm{f}}(K,T_1)$ in $H^1(K,T_2)$, as desired.

If $T_1 \hookrightarrow T_2$ is injective, then c is injective, so $b^{-1}(\ker(d_2)) = \ker(d_1)$, i.e., the inverse image of $H^1_{\mathrm{f}}(K,T_2)$ in $H^1(K,T_1)$ is $H^1_{\mathrm{f}}(K,T_1)$.

This proves (i), and (ii) is just (i) applied to the case of submodules. □

1.2. The finite/singular homomorphism

Suppose for this section that the local field K is nonarchimedean, and has residue characteristic $\ell \neq p$. Suppose also that the R-module T is of finite type, the action of G_K on T is unramified, and

$$|\mathbf{F}^\times| \cdot T = 0.$$

LEMMA 1.2.1. *There are canonical functorial isomorphisms*

(i) $H^1_{\mathrm{f}}(K,T) \cong T/(\mathrm{Fr}-1)T$,
(ii) $H^1_{\mathrm{s}}(K,T) \cong \mathrm{Hom}(\mathcal{I}, T^{\mathrm{Fr}=1})$ *and* $H^1_{\mathrm{s}}(K,T) \otimes \mathbf{F}^\times \cong T^{\mathrm{Fr}=1}$.

PROOF. This is well known; see for example [**Ru6**] Lemma 1.3.2. The isomorphism of (i) is induced by evaluating cocycle classes in $H^1(G_{\mathbf{F}}, T)$ on Frobenius. For (ii), the exact sequence (2) gives an isomorphism

$$H^1_{\mathrm{s}}(K,T) \cong \mathrm{Hom}(\mathcal{I},T)^{\mathrm{Fr}=1}.$$

Since $|\mathbf{F}^\times| \cdot T = 0$ and $\mathcal{I}/|\mathbf{F}^\times|\mathcal{I}$ is canonically isomorphic to $\mathbf{F}^\times$, we also have

$$\mathrm{Hom}(\mathcal{I},T)^{\mathrm{Fr}=1} = \mathrm{Hom}(\mathcal{I}/|\mathbf{F}^\times|\mathcal{I},T)^{\mathrm{Fr}=1} = \mathrm{Hom}(\mathbf{F}^\times,T)^{\mathrm{Fr}=1} = \mathrm{Hom}(\mathbf{F}^\times, T^{\mathrm{Fr}=1})$$

and (ii) follows. □

DEFINITION 1.2.2. Suppose that T is free of finite rank as an R-module, and that $\det(1-\mathrm{Fr} \mid T) = 0$. Define $P(x) \in R[x]$ by

$$P(x) = \det(1 - \mathrm{Fr}\, x \mid T).$$

Since $P(1) = 0$, there is a unique polynomial $Q(x) \in R[x]$ such that

$$(x-1)Q(x) = P(x) \quad \text{in } R[x].$$

By the Cayley-Hamilton theorem, $P(\mathrm{Fr}^{-1})$ annihilates T, so $Q(\mathrm{Fr}^{-1})T \subset T^{\mathrm{Fr}=1}$. We define the *finite-singular comparison map* ϕ^{fs}_ℓ on T to be the composition, using the isomorphisms of Lemma 1.2.1,

$$H^1_{\mathrm{f}}(K,T) \xrightarrow{\sim} T/(\mathrm{Fr}-1)T \xrightarrow{Q(\mathrm{Fr}^{-1})} T^{\mathrm{Fr}=1} \xrightarrow{\sim} H^1_{\mathrm{s}}(K,T) \otimes \mathbf{F}^\times.$$

LEMMA 1.2.3. *Suppose that R is artinian, $|\mathbf{F}^\times| \cdot R = 0$, and T is free of finite rank over R. Suppose further that $T/(\mathrm{Fr}-1)T$ is a free R-module of rank one. Then* $\det(1-\mathrm{Fr} \mid T) = 0$ *and the maps*

$$Q(\mathrm{Fr}^{-1}) : T/(\mathrm{Fr}-1)T \longrightarrow T^{\mathrm{Fr}=1}, \quad \phi^{\mathrm{fs}} : H^1_{\mathrm{f}}(K,T) \longrightarrow H^1_{\mathrm{s}}(K,T) \otimes \mathbf{F}^\times$$

of Definition 1.2.2 are isomorphisms. In particular both $H^1_{\mathrm{f}}(K,T)$ and $H^1_{\mathrm{s}}(K,T)$ are free of rank one over R.

PROOF. Choose an R-basis $\{x_1,\dots,x_d\}$ of T such that $\{x_2,\dots,x_d\}$ is a basis of $(\mathrm{Fr}-1)T$. With this basis it is clear that $\det(1-\mathrm{Fr}\mid T)=0$.

That ϕ^{fs} is an isomorphism will follow immediately once we show that $Q(\mathrm{Fr}^{-1})$ is an isomorphism, and then the fact that $H^1_{\mathrm{f}}(K,T)$ and $H^1_{\mathrm{s}}(K,T)$ are free of rank one will follow from Lemma 1.2.1(i) and (ii).

It remains to show that $Q(\mathrm{Fr}^{-1})$ is an isomorphism. When R is a field this is Corollary A.2.6 of [**Ru6**]. Applying that case to the $R/\mathfrak{m}$-module $T/\mathfrak{m}T$ and using Nakayama's Lemma we see that $Q(\mathrm{Fr}^{-1})$ is surjective. The exact sequence

$$0\longrightarrow T^{\mathrm{Fr}=1}\longrightarrow T\xrightarrow{\mathrm{Fr}-1} T\longrightarrow T/(\mathrm{Fr}-1)T\longrightarrow 0$$

shows that $T/(\mathrm{Fr}-1)T$ and $T^{\mathrm{Fr}=1}$ have the same length, so $Q(\mathrm{Fr}^{-1})$ is an isomorphism. □

Now fix an abelian extension L/K which is totally and tamely ramified, and moreover is a maximal such (abelian, totally, tamely ramified) extension of K. There is a natural isomorphism $\mathrm{Gal}(L/K)\cong\mathbf{F}^\times$. (When $K=\mathbf{Q}_\ell$ we will take $L=K(\boldsymbol{\mu}_\ell)$.)

Since L is fixed we will suppress it from the notation and write simply H^1_{tr} for the local condition $H^1_{L-\mathrm{tr}}$ of Definition 1.1.6(iv).

LEMMA 1.2.4. *The transverse subgroup $H^1_{\mathrm{tr}}(K,T)\subset H^1(K,T)$ projects isomorphically to $H^1_{\mathrm{s}}(K,T)$ in* (3)*. In other words,* (3) *has a functorial splitting (depending on L)*

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

PROOF. Since L/K is totally ramified and T is unramified, $T^{G_L}=T^{G_K}=T^{\mathrm{Fr}=1}$. Hence we have a commutative diagram

$$\begin{array}{ccccccc}
H^1_{\mathrm{tr}}(K,T) & \hookrightarrow & H^1(K,T) & \twoheadrightarrow & H^1_{\mathrm{s}}(K,T) & \xrightarrow{\sim} & \mathrm{Hom}(\mathcal{I},T^{\mathrm{Fr}=1}) \\
\downarrow\sim & & & & & & \uparrow\sim \\
H^1(L/K,T^{G_L}) & & \xrightarrow{\sim} & & \mathrm{Hom}(\mathrm{Gal}(L/K),T^{\mathrm{Fr}=1}) & \xrightarrow{\sim} & \mathrm{Hom}(\mathcal{I}/|\mathbf{F}^\times|\mathcal{I},T^{\mathrm{Fr}=1})
\end{array}$$

in which the all maps marked as such are isomorphisms (the upper right map by Lemma 1.2.1(ii)). This proves the lemma. □

1.3. Local duality

DEFINITION 1.3.1. Define the *dual* of T to be the $R[[G_K]]$-module

$$T^*=\mathrm{Hom}(T,\boldsymbol{\mu}_{p^\infty}).$$

We have the (perfect) local Tate cup product pairing

$$\langle\ ,\ \rangle : H^1(K,T)\times H^1(K,T^*)\longrightarrow H^2(K,\boldsymbol{\mu}_{p^\infty})\xrightarrow{\sim}\mathbf{Q}_p/\mathbf{Z}_p.$$

A local condition $\mathcal{F}$ for T determines a local condition $\mathcal{F}^*$ for T^*, by taking $H^1_{\mathcal{F}^*}(K,T^*)$ to be the orthogonal complement of $H^1_{\mathcal{F}}(K,T)$ under the Tate pairing $\langle\ ,\ \rangle$.

Clearly the dual of the unrestricted local condition in the strict condition, and the dual of the strict condition is the unrestricted condition. The next proposition says that (on suitable modules T) the finite and transverse conditions are self-dual.

PROPOSITION 1.3.2. *Suppose K is nonarchimedean of residue characteristic different from p, and T is unramified.*

(i) *$H^1_{\mathrm{f}}(K,T)$ and $H^1_{\mathrm{f}}(K,T^*)$ are orthogonal complements under $\langle\ ,\ \rangle$.*
(ii) *If $|\mathbf{F}^\times|\cdot T=0$ and L/K is a totally ramified abelian extension of degree $|\mathbf{F}^\times|$, then $H^1_{\mathrm{tr}}(K,T)$ and $H^1_{\mathrm{tr}}(K,T^*)$ are orthogonal complements under $\langle\ ,\ \rangle$.*

PROOF. The first assertion is (for example) Theorem I.2.6 of [**Mi**]. Assertion (ii) will follow from (i) and Lemma 1.2.4 once we show that $H^1_{\mathrm{tr}}(K,T)$ and $H^1_{\mathrm{tr}}(K,T^*)$ are orthogonal.

Suppose first that $R=\mathbf{Z}_p$ and $T=\mathbf{Z}/p^k\mathbf{Z}$ (with trivial G_K-action) with p^k dividing $|\mathbf{F}^\times|$. Then $\boldsymbol{\mu}_{p^k}\subset K^\times$ and we can identify

$$H^1_{\mathrm{tr}}(K,T)=\mathrm{Hom}(\mathrm{Gal}(L/K),\mathbf{Z}/p^k\mathbf{Z})\cong\mathrm{Hom}(K^\times/\mathbf{N}_{L/K}L^\times,\mathbf{Z}/p^k\mathbf{Z}),$$
$$H^1_{\mathrm{tr}}(K,T^*)=\mathrm{Hom}(\mathrm{Gal}(L/K),\boldsymbol{\mu}_{p^k})\cong\ker[K^\times/(K^\times)^{p^k}\to L^\times/(L^\times)^{p^k}]$$

by class field theory and Kummer theory, respectively, and the cup product pairing is induced by the natural pairing

$$\mathrm{Hom}(K^\times,\mathbf{Z}/p^k\mathbf{Z})\times K^\times\longrightarrow\mathbf{Z}/p^k\mathbf{Z}.$$

Suppose $\alpha\in\ker[K^\times\to L^\times/(L^\times)^{p^k}]$, say $\alpha=\beta^{p^k}$ with $\beta\in L^\times$. Then a simple computation shows that $\mathbf{N}_{L/K}\beta=\alpha^{|\mathbf{F}^\times|/p^k}$. Since $K^\times/\mathbf{N}_{L/K}L^\times$ is cyclic of order $|\mathbf{F}^\times|$, α is divisible by p^k in $K^\times/\mathbf{N}_{L/K}L^\times$ and so α is sent to zero by every element of $\mathrm{Hom}(K^\times/\mathbf{N}_{L/K}L^\times,\mathbf{Z}/p^k\mathbf{Z})$. This proves (ii) in this case.

In general, since T is unramified and L/K is totally ramified we have $T^{G_L}=T^{G_K}$, $(T^*)^{G_L}=(T^*)^{G_K}$, and hence

$$H^1_{\mathrm{tr}}(K,T)=H^1(L/K,T^{G_L})=H^1(L/K,T^{G_K})=H^1_{\mathrm{tr}}(K,T^{G_K}),$$
$$H^1_{\mathrm{tr}}(K,T^*)=H^1(L/K,(T^*)^{G_L})=H^1(L/K,(T^*)^{G_K})=H^1_{\mathrm{tr}}(K,(T^{G_K})^*).$$

Writing $T^{G_K}\cong\oplus\mathbf{Z}/p^{k_i}\mathbf{Z}$, the general case of (ii) follows from the case $T=\mathbf{Z}/p^k\mathbf{Z}$ above. □

EXAMPLE 1.3.3. Suppose $\mathcal{F}$ is a local condition on T and I is an ideal of R. There are two ways to induce a local condition on $T^*[I]$: we can induce $\mathcal{F}$ to the quotient T/IT and then to the dual $(T/IT)^*=T^*[I]$, or we can induce $\mathcal{F}$ to the dual T^* and then to the submodule $T^*[I]$. It is an easy exercise to show that these give the same local condition on $T^*[I]$.

CHAPTER 2

Global Cohomology Groups and Selmer Structures

For the rest of this paper, T will be a finitely generated R-module with a continuous action of $G_{\mathbf{Q}}$, which is unramified outside a finite set of rational primes.

Global notation. Let $\bar{\mathbf{Q}} \subset \mathbf{C}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and for each rational prime ℓ fix an algebraic closure $\overline{\mathbf{Q}}_\ell$ of $\mathbf{Q}_\ell$ containing $\bar{\mathbf{Q}}$. If $\ell = \infty$, then $\mathbf{Q}_\ell = \mathbf{R}$ and we take $\overline{\mathbf{Q}}_\ell = \mathbf{C}$. Let $\mathcal{D}_\ell = \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/\mathbf{Q}_\ell)$, which we identify with a closed subgroup of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. In other words $\mathcal{D}_\ell$ is a particular decomposition group at ℓ in $G_{\mathbf{Q}}$, and $H^1(\mathcal{D}_\ell, T) = H^1(\mathbf{Q}_\ell, T)$. Let $\mathcal{I}_\ell \subset \mathcal{D}_\ell$ be the inertia group, and $\mathrm{Fr}_\ell \in \mathcal{D}_\ell/\mathcal{I}_\ell$ the Frobenius element. If T is unramified at ℓ, then $\mathcal{D}_\ell/\mathcal{I}_\ell$ acts on T, and hence so does Fr_ℓ. If we choose a different decomposition group at ℓ, then the action of Fr_ℓ changes by conjugation in $G_{\mathbf{Q}}$.

If T is unramified at ℓ, the *transverse submodule* of $H^1(\mathbf{Q}_\ell, T)$ is the submodule

$$H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T) = H^1(\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell, T^{\mathcal{D}_\ell})$$

of Definition 1.1.6(iv) with $L = \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)$.

If $c \in H^1(\mathbf{Q}, T)$ we will write c_ℓ for the image of c under the localization map $H^1(\mathbf{Q}, T) \to H^1(\mathbf{Q}_\ell, T)$. If further $\ell \neq p$, T is unramified at ℓ, and $(\ell - 1)T = 0$, then we write $c_\ell = c_{\ell,\mathrm{f}} + c_{\ell,\mathrm{tr}}$, where $c_{\ell,\mathrm{f}}$ and $c_{\ell,\mathrm{tr}}$ are the projections of c_ℓ under the decomposition $H^1(\mathbf{Q}_\ell, T) \cong H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T) \oplus H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$ of Lemma 1.2.4.

2.1. Selmer modules

Definition 2.1.1. A *Selmer structure* $\mathcal{F}$ on T is a collection of the following data:

- a finite set $\Sigma(\mathcal{F})$ of places of $\mathbf{Q}$, including ∞, p, and all primes where T is ramified,
- for every $\ell \in \Sigma(\mathcal{F})$ (including $\ell = \infty$), a local condition (in the sense of Definition 1.1.1) on T viewed as an $R[[\mathcal{D}_\ell]]$-module, i.e., a choice of R-submodule
$$H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) \subset H^1(\mathbf{Q}_\ell, T).$$

If $\ell \notin \Sigma(\mathcal{F})$ we will also write $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$.

Let $\mathbf{SS}(T)$ denote the set of Selmer structures on T.

If $\mathcal{F}$ is a Selmer structure, we define the *Selmer module* $H^1_{\mathcal{F}}(\mathbf{Q}, T) \subset H^1(\mathbf{Q}, T)$ to be the kernel of the sum of restriction maps

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

where $\mathbf{Q}_{\Sigma(\mathcal{F})}$ denotes the maximal extension of $\mathbf{Q}$ which is unramified outside $\Sigma(\mathcal{F})$. In other words, $H^1_{\mathcal{F}}(\mathbf{Q}, T)$ consists of all classes which are unramified (or equivalently, finite) outside of $\Sigma(\mathcal{F})$ and which locally at ℓ belong to $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ for every $\ell \in \Sigma(\mathcal{F})$.

There is a natural partial ordering on the set $\mathbf{SS}(T)$. Namely, we will say that $\mathcal{F} \leq \mathcal{F}'$ if and only if

- $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) \subset H^1_{\mathcal{F}'}(\mathbf{Q}_\ell, T)$ if $\ell \in \Sigma(\mathcal{F}) \cap \Sigma(\mathcal{F}')$,
- $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) \subset H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ if $\ell \in \Sigma(\mathcal{F}) - \Sigma(\mathcal{F}')$,
- $H^1_{\mathcal{F}'}(\mathbf{Q}_\ell, T) \supset H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ if $\ell \in \Sigma(\mathcal{F}') - \Sigma(\mathcal{F})$.

If $\mathcal{F} \leq \mathcal{F}'$ then we clearly have $H^1_{\mathcal{F}}(\mathbf{Q}, T) \subset H^1_{\mathcal{F}'}(\mathbf{Q}, T)$.

EXAMPLE 2.1.2. Let $R = \mathbf{Z}/p^k\mathbf{Z}$ and $T = \mathbf{Z}/p^k\mathbf{Z}$ with trivial Galois action. Let $\Sigma(\mathcal{F}) = \{p, \infty\}$, $H^1_{\mathcal{F}}(\mathbf{R}, \mathbf{Z}/p^k\mathbf{Z}) = 0$, and $H^1_{\mathcal{F}}(\mathbf{Q}_p, \mathbf{Z}/p^k\mathbf{Z}) = H^1_{\mathrm{unr}}(\mathbf{Q}_p, \mathbf{Z}/p^k\mathbf{Z})$. Then $H^1(\mathbf{Q}, \mathbf{Z}/p^k\mathbf{Z}) = \mathrm{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/p^k\mathbf{Z})$, and $H^1_{\mathcal{F}}(\mathbf{Q}, \mathbf{Z}/p^k\mathbf{Z})$ is the subgroup of unramified homomorphisms. Since $\mathbf{Q}$ has no abelian unramified extensions, $H^1_{\mathcal{F}}(\mathbf{Q}, \mathbf{Z}/p^k\mathbf{Z}) = 0$.

Still with $R = \mathbf{Z}/p^k\mathbf{Z}$, let $T = \boldsymbol{\mu}_{p^k}$. Let $\Sigma(\mathcal{F}) = \{p, \infty\}$, $H^1_{\mathcal{F}}(\mathbf{R}, \boldsymbol{\mu}_{p^k}) = 0$, and $H^1_{\mathcal{F}}(\mathbf{Q}_p, \mathbf{Z}/p^k\mathbf{Z}) = H^1(\mathbf{Q}_p, \mathbf{Z}/p^k\mathbf{Z})$. Then $H^1(\mathbf{Q}, \mathbf{Z}/p^k\mathbf{Z}) = \mathbf{Q}^\times/(\mathbf{Q}^\times)^{p^k}$, and $H^1_{\mathcal{F}}(\mathbf{Q}, \mathbf{Z}/p^k\mathbf{Z})$ is the subgroup of totally positive p-units, i.e., $H^1_{\mathcal{F}}(\mathbf{Q}, \mathbf{Z}/p^k\mathbf{Z}) = p^{\mathbf{Z}}/p^{p^k\mathbf{Z}}$.

For generalizations of these examples, involving ideal class groups and units of abelian extensions of $\mathbf{Q}$, see §6.1.

EXAMPLE 2.1.3. Let $R = \mathbf{Z}/p^k\mathbf{Z}$ and $T = E[p^k]$ where E is an elliptic curve defined over $\mathbf{Q}$. Let $\Sigma(\mathcal{F})$ be any finite set of places containing p, ∞, and the primes where E has bad reduction. If $\ell \in \Sigma(\mathcal{F})$, let $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, E[p^k])$ be the image of $E(\mathbf{Q}_\ell)/p^kE(\mathbf{Q}_\ell)$ in $H^1(\mathbf{Q}_\ell, E[p^k])$ under the natural Kummer map. Then $H^1_{\mathcal{F}}(\mathbf{Q}, E[p^k])$ is the classical p^k-Selmer group of E.

See §6.2 for much more on this example.

LEMMA 2.1.4. *If $(T/\mathfrak{m}T)^{G_{\mathbf{Q}}} = 0$ and S is a quotient of T then $S^{G_{\mathbf{Q}}} = 0$.*

PROOF. Since the $\mathbb{k}[[G_{\mathbf{Q}}]]$-module $T/\mathfrak{m}T$ has no nontrivial Galois invariants, the same is true of its quotient $S/\mathfrak{m}S$. Further, if $i > 1$ then $\mathfrak{m}^{i-1}S/\mathfrak{m}^iS$ is a quotient of $S \otimes (\mathfrak{m}^{i-1}/\mathfrak{m}^i) \cong (S/\mathfrak{m}S)^{\dim_{\mathbb{k}}(\mathfrak{m}^{i-1}/\mathfrak{m}^i)}$ so it follows by induction that $(S/\mathfrak{m}^iS)^{G_{\mathbf{Q}}} = 0$. Since $S = \varprojlim S/\mathfrak{m}^iS$ we have $S^{G_{\mathbf{Q}}} = 0$. □

PROPOSITION 2.1.5. *The Selmer module $H^1_{\mathcal{F}}(\mathbf{Q}, T)$ is a finitely generated R-module. If R is an integral domain, T is a torsion-free R-module, and $(T/\mathfrak{m}T)^{G_{\mathbf{Q}}} = 0$, then $H^1_{\mathcal{F}}(\mathbf{Q}, T)$ is a torsion-free R-module.*

PROOF. It will suffice to prove the proposition with $H^1_{\mathcal{F}}(\mathbf{Q}, T)$ replaced by the larger module $H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T)$. The first assertion is well-known, see for example [**PR3**] Appendix A.1. For the second, if $\alpha \in R$ then cohomology of the exact sequence $0 \to T \xrightarrow{\alpha} T \to T/\alpha T \to 0$ gives a surjective map

$$(T/\alpha T)^{G_{\mathbf{Q}}} \twoheadrightarrow H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T)[\alpha].$$

so by Lemma 2.1.4 we see that if $(T/\mathfrak{m}T)^{G_{\mathbf{Q}}} = 0$ then $H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T)$ has no α-torsion. □

EXAMPLE 2.1.6. Suppose that $\mathcal{F}$ is a Selmer structure and Σ' is a finite set of primes containing $\Sigma(\mathcal{F})$. We can extend $\mathcal{F}$ to $\mathcal{F}'$ with $\Sigma(\mathcal{F}') = \Sigma'$ by taking $H^1_{\mathcal{F}'}(\mathbf{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ for $\ell \in \Sigma' - \Sigma(\mathcal{F})$. Then $\mathcal{F} \leq \mathcal{F}'$, $\mathcal{F}' \leq \mathcal{F}$, and $H^1_{\mathcal{F}}(\mathbf{Q}, T) = H^1_{\mathcal{F}'}(\mathbf{Q}, T)$, so we will identify $\mathcal{F}$ and $\mathcal{F}'$ inside $\mathbf{SS}(T)$.

EXAMPLE 2.1.7. A Selmer structure $\mathcal{F}$ on T induces a Selmer structure (also denoted by $\mathcal{F}$) on every subquotient T' of T as follows. Keep the same set $\Sigma(\mathcal{F})$, and for $\ell \in \Sigma(\mathcal{F})$ take $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T')$ be the local condition on T' induced by the one on T (as in Example 1.1.2). This construction defines a map $\mathbf{SS}(T) \to \mathbf{SS}(T')$.

In particular if I is an ideal of R, then a Selmer structure on T induces Selmer structures on T/IT and $T[I]$.

Similarly, if $R \to R'$ is a homomorphism of complete noetherian local rings, then there is a natural map $\mathbf{SS}(T) \to \mathbf{SS}(T \otimes_R R')$: a Selmer structure $\mathcal{F}$ on the R-module T induces a Selmer structure (denoted $\mathcal{F} \otimes R'$, or simply $\mathcal{F}$) on the R'-module $T \otimes_R R'$ with the same set $\Sigma(\mathcal{F})$ by taking $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T \otimes R')$ to be the image in $H^1(\mathbf{Q}_\ell, T \otimes R')$ of $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) \otimes R'$, for $\ell \in \Sigma(\mathcal{F})$.

EXAMPLE 2.1.8. Suppose $\mathcal{F}$ is a Selmer structure and ℓ is a prime not in $\Sigma(\mathcal{F})$. There are several natural ways to extend $\mathcal{F}$ to a new Selmer structure $\mathcal{F}'$ with $\Sigma(\mathcal{F}') = \Sigma(\mathcal{F}) \cup \{\ell\}$, which will be important in what follows. We can take $H^1_{\mathcal{F}'}(\mathbf{Q}_\ell, T)$ to be 0, or all of $H^1(\mathbf{Q}_\ell, T)$. If we take $H^1_{\mathcal{F}'}(\mathbf{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ then we have identified $\mathcal{F}'$ with $\mathcal{F}$ (see Example 2.1.6). Finally, if we can take $H^1_{\mathcal{F}'}(\mathbf{Q}_\ell, T) = H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$.

We can repeat these constructions with several primes, and we will use the following notation. If $a, b, c \in \mathbf{Z}^+$ are relatively prime, and c is not divisible by any primes in $\Sigma(\mathcal{F})$, we write $\mathcal{F}^b_a(c)$ for the Selmer structure defined by

- $\Sigma(\mathcal{F}^b_a(c)) = \Sigma(\mathcal{F}) \cup \{\ell : \ell \mid abc\}$,
- $H^1_{\mathcal{F}^b_a(c)}(\mathbf{Q}_\ell, T) = \begin{cases} H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) & \text{if } \ell \in \Sigma(\mathcal{F}) \text{ and } \ell \nmid ab \\ 0 & \text{if } \ell \mid a, \\ H^1(\mathbf{Q}_\ell, T) & \text{if } \ell \mid b, \\ H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T) & \text{if } \ell \mid c. \end{cases}$

In other words, $\mathcal{F}^b_a(c)$ consists of $\mathcal{F}$ together with the strict condition at primes dividing a, the unrestricted condition at primes dividing b, and the transverse condition at primes dividing c.

If any of a, b, c are equal to 1, we will suppress them from the notation. If $a' \mid a$, $b \mid b'$, and $c = c'$ then $\mathcal{F}^b_a(c) \le \mathcal{F}^{b'}_{a'}(c')$, and otherwise there will be in general no order relation between these Selmer structures. In particular for every n we have $\mathcal{F}_n \le \mathcal{F} \le \mathcal{F}^n$ and $\mathcal{F}_n \le \mathcal{F}(n) \le \mathcal{F}^n$.

EXAMPLE 2.1.9 (Universal deformations). Let $\Bbbk$ be a finite field and V an absolutely irreducible finite dimensional continuous representation of $G_{\mathbf{Q}}$ over $\Bbbk$. Suppose further that V is unramified outside of $\Sigma = \{p, \infty\}$.

Let T and R denote the universal deformation and universal deformation ring attached to V and Σ (see [**Ma1**]). That is, R is a complete noetherian local ring with residue field $\Bbbk$, T is a free R-module of rank $\dim_{\Bbbk}(V)$, and T comes with a continuous R-linear action of $G_{\mathbf{Q}}$, unramified outside Σ, and an isomorphism of $\Bbbk[[G_{\mathbf{Q}}]]$-modules $\iota : T \otimes \Bbbk \xrightarrow{\sim} V$. Moreover, the triple (R, T, ι) is universal in the evident sense (see [**Ma1**]).

Define a Selmer structure on T by $\Sigma(\mathcal{F}) = \Sigma$, $H^1_{\mathcal{F}}(\mathbf{R}, T) = H^1(\mathbf{R}, T)$ and $H^1_{\mathcal{F}}(\mathbf{Q}_p, T) = H^1(\mathbf{Q}_p, T)$. We will call this the *universal deformation Selmer module* attached to V and S.

2.2. Comparing Selmer modules

DEFINITION 2.2.1. Suppose now that T is free over R, $\ell \neq p, \infty$ is prime, and T is unramified at ℓ. Let $P_\ell(x) = \det(1 - \mathrm{Fr}_\ell\, x \mid T) \in R[x]$, and let I_ℓ be the ideal of R generated by $\ell - 1$ and $P_\ell(1)$.

Let $\mathcal{P}$ denote a set of rational primes, disjoint from $\Sigma(\mathcal{F})$. Generally $\mathcal{P}$ will be infinite; for example it could be the set of all primes not in $\Sigma(\mathcal{F})$. Let $\mathcal{N} = \mathcal{N}(\mathcal{P}) \subset \mathbf{Z}^+$ denote the set of squarefree products of primes in $\mathcal{P}$ (with the convention that $1 \in \mathcal{N}$). If $n \in \mathcal{N}$ let

$$I_n = \sum_{\ell \mid n} I_\ell \subset R$$

and let

$$G_n = \bigotimes_{\ell \mid n} \mathbf{F}_\ell^\times = \bigotimes_{\ell \mid n} \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_\ell)/\mathbf{Q}).$$

Since each $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_\ell)/\mathbf{Q})$ is cyclic of order $\ell - 1$, we see that $G_n \otimes (R/I_n)$ is free of rank one over R/I_n. By convention, we set $G_1 = \mathbf{Z}_p$.

If ℓ is a prime dividing n, then I_ℓ annihilates T/I_nT, so we can apply the results of §1.2 to the local cohomology group $H^1(\mathbf{Q}_\ell, T/I_nT)$. In particular we will write

$$\phi_\ell^{\mathrm{fs}} : H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/I_nT) \longrightarrow H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_nT) \otimes G_\ell$$

for the finite-singular map of Definition 1.2.2 with $K = \mathbf{Q}_\ell$.

EXAMPLE 2.2.2. Suppose $\mathcal{P}$ is a set of primes as above and $n \in \mathcal{N}$. Recall that the Selmer structure $\mathcal{F}(n)$ is the Selmer structure $\mathcal{F}$ modified by replacing the finite local condition at primes dividing n by the transverse local condition. In what follows we will be interested in the modules $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n$ for $n \in \mathcal{N}$.

If ℓ is a prime and $n\ell \in \mathcal{N}$, then we can compare $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n$ and $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T/I_{n\ell}T) \otimes G_{n\ell}$ by localizing at ℓ and using the finite-singular map ϕ_ℓ^{fs}:

$$\begin{array}{ccc} & & H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n \\ & & \Big\downarrow{\scriptstyle \mathrm{loc}_\ell} \\ & & H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_n \\ & & \Big\downarrow{\scriptstyle \phi_\ell^{\mathrm{fs}} \otimes 1} \\ H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T/I_{n\ell}T) \otimes G_{n\ell} & \xrightarrow{\mathrm{loc}_\ell} & H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}. \end{array} \tag{4}$$

2.3. Global duality

DEFINITION 2.3.1. The *dual* of T is the $R[[G_{\mathbf{Q}}]]$-module

$$T^* = \mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty}).$$

For every prime $\ell \leq \infty$ we have the local Tate pairing

$$\langle\ ,\ \rangle_\ell : H^1(\mathbf{Q}_\ell, T) \times H^1(\mathbf{Q}_\ell, T^*) \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p$$

as in §1.3. If $c \in H^1(\mathbf{Q}, T)$ and $d \in H^1(\mathbf{Q}, T^*)$ we will write $\langle c, d\rangle_\ell$ for $\langle c_\ell, d_\ell\rangle_\ell$.

Just as every local condition on T determines a local condition on T^* (Definition 1.3.1), a Selmer structure $\mathcal{F}$ for T determines a Selmer structure $\mathcal{F}^*$ for T^*. Namely, take $\Sigma(\mathcal{F}^*) = \Sigma(\mathcal{F})$, and for $\ell \in \Sigma(\mathcal{F})$ take $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*)$ to be the local condition

induced by $\mathcal{F}$: the orthogonal complement of $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ under $\langle\ ,\ \rangle_\ell$. If $\mathcal{F} \leq \mathcal{F}'$ then $(\mathcal{F}')^* \leq \mathcal{F}^*$.

EXAMPLE 2.3.2. By Proposition 1.3.2, the dual $\mathcal{F}^b_a(c)^*$ of the Selmer structure $\mathcal{F}^b_a(c)$ is $(\mathcal{F}^*)^b_a(c)$.

LEMMA 2.3.3. *The Selmer module $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$ is co-finitely generated, i.e., the R-module* $\mathrm{Hom}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*), \mathbf{Q}_p/\mathbf{Z}_p)$ *is finitely generated.*

PROOF. As in the proof of Lemma 2.1.4, $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \subset H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T^*)$ so it is enough to show that $H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T^*)$ is co-finitely generated. This is a standard result, see for example [**PR3**] Appendix A.1. □

THEOREM 2.3.4. *Suppose that $\mathcal{G}_1$, $\mathcal{G}_2$ are Selmer structures and $\mathcal{G}_1 \leq \mathcal{G}_2$.*

(i) *There are exact sequences*

$$0 \longrightarrow H^1_{\mathcal{G}_1}(\mathbf{Q}, T) \longrightarrow H^1_{\mathcal{G}_2}(\mathbf{Q}, T) \xrightarrow{\mathrm{loc}^{\mathcal{G}_2}_{\mathcal{G}_1}} \bigoplus_\ell H^1_{\mathcal{G}_2}(\mathbf{Q}_\ell, T)/H^1_{\mathcal{G}_1}(\mathbf{Q}_\ell, T),$$

$$0 \longrightarrow H^1_{\mathcal{G}_2^*}(\mathbf{Q}, T^*) \longrightarrow H^1_{\mathcal{G}_1^*}(\mathbf{Q}, T^*) \xrightarrow{\mathrm{loc}^{\mathcal{G}_1^*}_{\mathcal{G}_2^*}} \bigoplus_\ell H^1_{\mathcal{G}_1^*}(\mathbf{Q}_\ell, T^*)/H^1_{\mathcal{G}_2^*}(\mathbf{Q}_\ell, T^*)$$

where the sums are over primes ℓ such that $H^1_{\mathcal{G}_2}(\mathbf{Q}_\ell, T) \neq H^1_{\mathcal{G}_1}(\mathbf{Q}_\ell, T)$, and the maps $\mathrm{loc}^{\mathcal{G}_2}_{\mathcal{G}_1}$, $\mathrm{loc}^{\mathcal{G}_1^*}_{\mathcal{G}_2^*}$ are the natural localization maps.

(ii) *The images $\mathrm{loc}^{\mathcal{G}_2}_{\mathcal{G}_1}$ and $\mathrm{loc}^{\mathcal{G}_1^*}_{\mathcal{G}_2^*}$ are orthogonal complements with respect to the pairing $\sum_\ell \langle\ ,\ \rangle_\ell$.*

PROOF. Assertion (i) is immediate from the definition of these Selmer groups. The second statement is part of Poitou-Tate global duality; see for example [**T**] Theorem 3.1 or [**Mi**] Theorem I.4.10 (see also [**Ru6**] Theorem 1.7.3). □

The next proposition is Proposition 1.6 of [**Wi**], adapted to include the case $p = 2$. It is a consequence of Poitou-Tate global duality, and the proof is the same as in [**Wi**].

PROPOSITION 2.3.5. *If T is finite, then*

$$\begin{aligned}\mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}, T)) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) \\ = \mathrm{length}(H^0(\mathbf{Q}, T)) - \mathrm{length}(H^0(\mathbf{Q}, T^*)) \\ - \sum_{\ell \in \Sigma(\mathcal{F})} (\mathrm{length}(H^0(\mathbf{Q}_\ell, T)) - \mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T))).\end{aligned}$$

COROLLARY 2.3.6. *Suppose that R is artinian and T is free of finite rank over R. Suppose $n \in \mathbf{Z}^+$ is not divisible by any primes in $\Sigma(\mathcal{F})$, and further that every prime ℓ dividing n satisfies the hypotheses of Lemma 1.2.3: $I_\ell = 0$ and $T/(\mathrm{Fr}_\ell - 1)T$ is free of rank one over R. Then*

$$\begin{aligned}\mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}, T)) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) \\ = \mathrm{length}(H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)) - \mathrm{length}(H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)).\end{aligned}$$

PROOF. By Lemma 1.2.3, $\mathrm{length}(H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)) = \mathrm{length}(H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T))$ for every ℓ dividing n, so the right-hand side of Proposition 2.3.5 is unchanged when we replace $\mathcal{F}$ by $\mathcal{F}(n)$.

(Alternatively, the corollary can be seen by applying Theorem 2.3.4 first with $(\mathcal{G}_1, \mathcal{G}_2) = (\mathcal{F}, \mathcal{F}^n)$ and then with $(\mathcal{G}_1, \mathcal{G}_2) = (\mathcal{F}(n), \mathcal{F}^n)$.) $\square$

CHAPTER 3

Kolyvagin Systems

We assume for the rest of this paper that T is free of finite rank over R, in addition to being a $G_{\mathbf{Q}}$-module which is unramified outside finitely many primes.

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

3.1. Kolyvagin systems

DEFINITION 3.1.1. If X is a simplicial complex, and $\mathcal{C}$ a category, a *simplicial sheaf* $\mathcal{S}$ on X with values in $\mathcal{C}$ is a rule assigning:

- to each simplex σ in X, an object $\mathcal{S}(\sigma)$ of $\mathcal{C}$, and
- to each pair (σ, τ) of simplices of X such that σ is a face of τ (of codimension one), a morphism $\mathcal{S}(\sigma) \to \mathcal{S}(\tau)$ in the category $\mathcal{C}$.

Note that such a simplicial sheaf gives rise to a sheaf on the topological realization of X which is locally constant on the open stars of simplices of X, and whose set of sections on the open star of a simplex σ is just $\mathcal{S}(\sigma)$. A morphism $\mathcal{S} \to \mathcal{S}'$ of sheaves on X is a collection of morphisms $\mathcal{S}(\sigma) \to \mathcal{S}'(\sigma)$ for each simplex σ in X, which commute with the face-to-simplex morphisms of $\mathcal{S}$ and $\mathcal{S}'$ in the obvious sense.

In this paper we will only be concerned with the case where X is a graph. In that case, if V is the set of vertices of X and E is the set of edges, a *simplicial sheaf* $\mathcal{S}$ on X with values in the category of R-modules is a collection of the following data:

- an R-module $\mathcal{S}(v)$ (the stalk of X at v) for every vertex $v \in V$,
- an R-module $\mathcal{S}(e)$ for every edge $e \in E$,
- an R-module map $\psi_v^e : \mathcal{S}(v) \to \mathcal{S}(e)$ whenever the vertex v is an endpoint of the edge e.

A global section of $\mathcal{S}$ is a collection $\{\kappa_v \in \mathcal{S}(v) : v \in V\}$ such that for every edge $e \in E$, if e has endpoints v, v' then $\psi_v^e(\kappa_v) = \psi_{v'}^e(\kappa_{v'})$ in $\mathcal{S}(e)$. We write $\Gamma(\mathcal{S}) = \mathcal{S}(X)$ for the R-module of global sections of $\mathcal{S}$.

DEFINITION 3.1.2. Suppose $(T, \mathcal{F}, \mathcal{P})$ is a Selmer triple. We define a graph $\mathcal{X} = \mathcal{X}(\mathcal{P})$ by taking the set of vertices of $\mathcal{X}$ to be $\mathcal{N} = \mathcal{N}(\mathcal{P})$ (Definition 2.2.1), and whenever $n, n\ell \in \mathcal{N}$ (with ℓ prime) we join n and $n\ell$ by an edge.

The *Selmer sheaf* associated to $(T, \mathcal{F}, \mathcal{P})$ is the simplicial sheaf $\mathcal{H} = \mathcal{H}_{(T,\mathcal{F},\mathcal{P})}$ of R-modules on $\mathcal{X}$ defined as follows. Take

- $\mathcal{H}(n) = H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n$ for $n \in \mathcal{N}$,

and if e is the edge joining n and $n\ell$ we take

- $\mathcal{H}(e) = H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}$,

- $\psi^e_{nl} : H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T/I_{n\ell}T) \otimes G_{n\ell} \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}$ is localization at ℓ followed by projection to H^1_{s},
- $\psi^e_n : H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n \longrightarrow H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}$ is the composition of localization at ℓ with the map ϕ^{fs}_ℓ of Definition 1.2.2 (see Example 2.2.2)

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n \longrightarrow H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_n \longrightarrow H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}.$$

We call $\mathcal{H}(n) = H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n$ the *Selmer stalk* at n.

Definition 3.1.3. A *Kolyvagin system* for $(T, \mathcal{F}, \mathcal{P})$ is a global section (over $\mathcal{X}(\mathcal{P})$) of the Selmer sheaf $\mathcal{H}_{(T,\mathcal{F},\mathcal{P})}$. We write $\mathbf{KS}(T, \mathcal{F}, \mathcal{P})$, or simply $\mathbf{KS}(T)$ when there is no risk of confusion, for the R-module of Kolyvagin systems $\Gamma(\mathcal{H})$.

Concretely, a Kolyvagin system for $(T, \mathcal{F}, \mathcal{P})$ is a collection of cohomology classes

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

such that if ℓ is prime and $n\ell \in \mathcal{N}$,

$$(\kappa_{n\ell})_{\ell,s} = \phi^{\mathrm{fs}}_\ell(\kappa_n) \quad \text{in } H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}. \tag{5}$$

In other words, the images of κ_n and $\kappa_{n\ell}$ in $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_{n\ell}T) \otimes G_{n\ell}$ coincide in the diagram (4).

For examples of Kolyvagin systems, see the next section.

Remark 3.1.4. The assignments

$$(T, \mathcal{F}, \mathcal{P}) \mapsto \mathcal{H}_{(T,\mathcal{F},\mathcal{P})}, \qquad (T, \mathcal{F}, \mathcal{P}) \mapsto \mathbf{KS}(T, \mathcal{F}, \mathcal{P})$$

have the following functorial properties (where we suppress the indices which are not varying).

- Commutation with direct sums: There are natural isomorphisms

$$\mathcal{H}_{(T_1 \oplus T_2, \mathcal{F}_1 \oplus \mathcal{F}_2)} \cong \mathcal{H}_{(T_1,\mathcal{F}_1)} \oplus \mathcal{H}_{(T_2,\mathcal{F}_2)},$$
$$\mathbf{KS}(T_1 \oplus T_2, \mathcal{F}_1 \oplus \mathcal{F}_2) \cong \mathbf{KS}(T_1, \mathcal{F}_1) \oplus \mathbf{KS}(T_2, \mathcal{F}_2).$$

- Change of ring: If $R \to R'$ is a homomorphism of complete local noetherian rings we have a natural homomorphism of sheaves of R'-modules over $\mathcal{X}$

$$\mathcal{H}_{(T,\mathcal{F})} \otimes_R R' \longrightarrow \mathcal{H}_{(T \otimes_R R', \mathcal{F} \otimes_R R')},$$
$$\mathbf{KS}(T, \mathcal{F}) \otimes_R R' \longrightarrow \mathbf{KS}(T \otimes_R R', \mathcal{F} \otimes_R R').$$

- Change of $\mathcal{P}$: If $\mathcal{P}' \subset \mathcal{P}$ then $\mathcal{H}_{T,\mathcal{P}'}$ is the restriction of $\mathcal{H}_{T,\mathcal{P}}$ to the subgraph $\mathcal{X}(\mathcal{P}') \subset \mathcal{X}(\mathcal{P})$, and there is a natural map $\mathbf{KS}(T, \mathcal{P}) \to \mathbf{KS}(T, \mathcal{P}')$.
- Change of $\mathcal{F}$: If $\mathcal{F}' \leq \mathcal{F}$, and $\mathcal{P}$ is disjoint from $\Sigma(\mathcal{F}) \cup \Sigma(\mathcal{F}')$, then $\mathcal{H}_{T,\mathcal{F}'}$ is naturally a subsheaf of R-modules in $\mathcal{H}_{T,\mathcal{F}}$, and $\mathbf{KS}(T, \mathcal{F}') \subset \mathbf{KS}(T, \mathcal{F})$.

Definition 3.1.5. If $\boldsymbol{\kappa}$ is a nonzero Kolyvagin system, the *order of vanishing* of $\boldsymbol{\kappa}$ is

$$\mathrm{ord}(\boldsymbol{\kappa}) = \min\{\nu(n) : \kappa_n \neq 0\}$$

where as usual $\nu(n)$ is the number of prime divisors of n.

The *module of L-values* of T is

$$\mathcal{L}(T) = \{\kappa_1 : \boldsymbol{\kappa} \in \mathbf{KS}(T)\} \subset H^1_{\mathcal{F}}(\mathbf{Q}, T).$$

Under suitable hypotheses, we would like to relate

- $\mathrm{ord}(\boldsymbol{\kappa})$ and $\mathrm{corank}_R(H^1_{\mathcal{F}^*}(\mathbf{Q},T^*))$,
- the Fitting ideals of $H^1_{\mathcal{F}}(\mathbf{Q},T)/\mathcal{L}(T)$ and $\mathrm{Hom}(H^1_{\mathcal{F}^*}(\mathbf{Q},T^*),\mathbf{Q}_p/\mathbf{Z}_p)$.

See in particular Theorem 5.1.1 (for R a field), Theorems 5.2.12 and 5.2.14 (for R a discrete valuation ring), and Theorem 5.3.10 (for R an Iwasawa algebra).

Definition 3.1.6. If $k\in\mathbf{Z}^+$ let $\mathcal{P}_k$ be the set of primes $\ell\notin\Sigma(\mathcal{F})$ satisfying

- $T/(\mathfrak{m}^kT+(\mathrm{Fr}_\ell-1)T)$ is free of rank one over $R/\mathfrak{m}^k$, and
- $I_\ell\subset\mathfrak{m}^k$.

Then $\mathcal{P}_1\supset\mathcal{P}_2\supset\mathcal{P}_3\supset\cdots$. Define

$$\overline{\mathbf{KS}}(T)=\overline{\mathbf{KS}}(T,\mathcal{F},\mathcal{P})=\varprojlim_k\left(\varinjlim_j\mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}\cap\mathcal{P}_j)\right)$$

with respect to the functorial maps of Remark 3.1.4. There is a natural map $\mathbf{KS}(T)\to\overline{\mathbf{KS}}(T)$, which in general need not be either injective or surjective. For example if R is artinian, then the kernel of this map consists of Kolyvagin systems whose restriction to $\mathcal{N}(\mathcal{P}\cap\mathcal{P}_j)$ is zero for large j. We will show that in many cases of interest (Corollary 4.5.3 and Proposition 5.2.9) the map $\mathbf{KS}(T)\to\overline{\mathbf{KS}}(T)$ is an isomorphism.

If $\bar{\boldsymbol{\kappa}}\in\overline{\mathbf{KS}}(T)$ then we have a well-defined element $\bar\kappa_1\in\varprojlim H^1_{\mathcal{F}}(\mathbf{Q},T/\mathfrak{m}^kT)=H^1_{\mathcal{F}}(\mathbf{Q},T)$. We can define $\mathrm{ord}(\bar{\boldsymbol{\kappa}})$ by an obvious modification of Definition 3.1.5 above. Essentially all of our results about Kolyvagin systems will apply equally to $\overline{\mathbf{KS}}(T)$, although we will not always state this explicitly.

The *blind spot* of $\boldsymbol{\kappa}$ is the set of ideals $I\subset R$ such that the image of $\boldsymbol{\kappa}$ under the composition

$$\mathbf{KS}(T)\longrightarrow\mathbf{KS}(T/I)\longrightarrow\overline{\mathbf{KS}}(T/I)$$

is zero. In other words, I is *not* in the blind spot if for some $k\in\mathbf{Z}^+$, the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/(I,\mathfrak{m}^k)T,\mathcal{P}\cap\mathcal{P}_j)$ is nonzero for every $j\in\mathbf{Z}^+$. In particular, if the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/I)$ is zero then I is in the blind spot of $\boldsymbol{\kappa}$.

The blind spot of the module of Kolyvagin systems for T is the intersection over all $\boldsymbol{\kappa}\in\mathbf{KS}(T)$ of the blind spot of $\boldsymbol{\kappa}$.

Remark 3.1.7. Suppose $\boldsymbol{\kappa}$ is a Kolyvagin system and $n\ell\in\mathcal{N}$. Then $\kappa_{n\ell}\in H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},T/I_{n\ell}T)$, so in particular $(\kappa_{n\ell})_\ell\in H^1_{\mathrm{tr}}(\mathbf{Q}_\ell,T/I_nT)$. Thus by Lemma 1.2.4 and (5), $(\kappa_{n\ell})_\ell$ is completely determined by $(\kappa_n)_\ell$.

The requirement that $\kappa_n\in H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},T/I_nT)$ in the definition of a Kolyvagin system is stronger than what is needed for standard applications found in the literature (bounding the size of the Selmer groups of the dual $G_{\mathbf{Q}}$-module T^*). For those purposes (see for example [**Ru6**]) the following collections of classes will suffice.

Definition 3.1.8. Define a sheaf $\hat{\mathcal{H}}$ of R-modules on $\mathcal{X}$ as follows. Take

- $\hat{\mathcal{H}}(n)=H^1_{\mathcal{F}^n}(\mathbf{Q},T/I_nT)\otimes G_n$ for $n\in\mathcal{N}$,

and define $\hat{\mathcal{H}}(e)$ and the maps ψ^e_{nl}, ψ^e_n exactly as in Definition 3.1.2. Clearly $\mathcal{H}$ is a subsheaf of $\hat{\mathcal{H}}$.

A *weak Kolyvagin system* for $(T,\mathcal{F},\mathcal{P})$ is a global section of the sheaf $\hat{\mathcal{H}}$. Concretely, a weak Kolyvagin system is a collection of cohomology classes

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

satisfying (5).

REMARK 3.1.9. In a weak Kolyvagin system, $(\kappa_n)_{\ell,\mathrm{s}}$ is determined, for every prime ℓ dividing n, by the κ_d for d properly dividing n. Equivalently, κ_n is uniquely determined modulo $H^1_{\mathcal{F}}(\mathbf{Q}, T/I_nT)$ by the κ_d for d properly dividing n.

In a Kolyvagin system (see Remark 3.1.7), κ_n is determined modulo $H^1_{\mathcal{F}}(\mathbf{Q},T)\cap H^1_{\mathcal{F}(n)}(\mathbf{Q},T) = H^1_{\mathcal{F}_n}(\mathbf{Q}, T/I_nT)$ by the κ_d for d properly dividing n, and for sufficiently divisible n this group will be zero.

The following example exhibits this lack of rigidity of weak Kolyvagin systems, as compared to Kolyvagin systems.

EXAMPLE 3.1.10. Suppose $p > 2$, $R = \mathbf{Z}_p$ and $T = \mathbf{Z}_p(1)$. Kummer theory shows that $H^1(\mathbf{Q}, T)$ is the p-adic completion of $\mathbf{Q}^\times$. Define $\mathcal{F}$ by $\Sigma(\mathcal{F}) = \{p, \infty\}$, $H^1_{\mathcal{F}}(\mathbf{Q}_p, T) = H^1(\mathbf{Q}_p, \mathbf{Z}_p(1))$, and $H^1_{\mathcal{F}}(\mathbf{R}, T) = 0$. Let $\mathcal{P}$ be the set of all primes different from p.

For every squarefree n prime to p, and every prime ℓ dividing n, we have a commutative diagram (the upper isomorphism is Kummer theory, and the lower isomorphism is Lemma 1.2.4)

$$\begin{array}{ccc} H^1_{\mathcal{F}^n}(\mathbf{Q}, T/I_nT) & \xrightarrow{\sim} & \mathbf{Z}[1/(pn)]^\times \otimes (\mathbf{Z}_p/I_n) \\ \big\downarrow & & \big\downarrow{\scriptstyle \mathrm{ord}_\ell} \\ H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T/I_nT) & \xrightarrow{\sim} & \mathbf{Z}_p/I_n. \end{array}$$

We can build a weak Kolyvagin system inductively as follows.

Choose any $\kappa_1 \in H^1(\mathbf{Q}, \mathbf{Z}_p(1))$. Next, suppose n is a positive squarefree integer prime to p, and we have chosen κ_t for every proper divisor t of n. Choose $\kappa_n \in \mathbf{Z}[1/(pn)]^\times \otimes (\mathbf{Z}_p/I_n) \otimes G_n$ so that $\mathrm{ord}_\ell(\kappa_n) = \phi^{\mathrm{fs}}_\ell(\kappa_{n/\ell})$ in the diagram above. (This determines κ_n up to a power of p; take any such choice.) In the limit this process will construct a weak Kolyvagin system for T. Because of the choices involved at each step, this will produce infinitely many weak Kolyvagin systems $\boldsymbol{\kappa}$ with the same κ_1.

Most of the weak Kolyvagin systems constructed in this way will *not* be Kolyvagin systems. We will see in §5.2 that in this setting every choice of κ_1 extends *uniquely* to a Kolyvagin system.

EXAMPLE 3.1.11. Suppose $H^1_{\mathcal{F}}(\mathbf{Q}, T/IT) = 0$ for every ideal $I \subset R$. We will show that every weak Kolyvagin system for T must be identically zero. More precisely, if $\boldsymbol{\kappa}$ is a weak Kolyvagin system, we will show by induction on the number of primes dividing n that $\kappa_n = 0$ for every $n \in \mathcal{N}$.

By definition, $\kappa_1 \in H^1_{\mathcal{F}}(\mathbf{Q}, T) = 0$. Suppose that $\kappa_d = 0$ for every d properly dividing n. We need to show that $\kappa_n = 0$.

We have $\kappa_n \in H^1_{\mathcal{F}^n}(\mathbf{Q}, T/I_nT) \otimes G_n$, but the coherence relations (5) show that $(\kappa_n)_{\ell,\mathrm{s}} = 0$ for every prime ℓ dividing n. Hence $\kappa_n \in H^1_{\mathcal{F}}(\mathbf{Q}, T/I_nT) \otimes G_n = 0$.

EXAMPLE 3.1.12. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T, \mathcal{F}, \mathcal{P})$ and $n \in \mathcal{N}$. Let $\mathcal{P}(n)$ be the set of primes in $\mathcal{P}$ not dividing n. If $\xi \in \mathrm{Hom}(G_n, R/I_n)$ then the collection $\boldsymbol{\kappa}^{(n)}$ defined by

$$\kappa^{(n)}_m = \kappa_{nm} \otimes \xi \quad \text{for } m \in \mathcal{N} \text{ prime to } n$$

is a Kolyvagin system for $(T/I_nT, \mathcal{F}(n), \mathcal{P}(n))$. (We view $\otimes\xi$ here as a map from $G_{nm} \otimes (R/I_n) = G_m \otimes G_n \otimes (R/I_n)$ to $G_m \otimes (R/I_n)$ for every m.) This construction

defines a homomorphism

$$\mathbf{KS}(T,\mathcal{F},\mathcal{P})\otimes \mathrm{Hom}(G_n,R/I_n)\to \mathbf{KS}(T/I_nT,\mathcal{F}(n),\mathcal{P}(n)).$$

(Recall that $\mathrm{Hom}(G_n,R/I_n)$ is a free, rank-one (R/I_n)-module.)

3.2. Euler systems and Kolyvagin systems

Suppose for this section that R is the ring of integers of a finite extension of $\mathbf{Q}_p$. For similar results when R is an Iwasawa algebra, see §5.3.

DEFINITION 3.2.1. We define a canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T by

- $\Sigma(\mathcal{F}_{\mathrm{can}})=\{\ell : T \text{ is ramified at } \ell\}\cup\{p,\infty\}$,
- if $\ell\in\Sigma(\mathcal{F}_{\mathrm{can}})$ and $\ell\neq p,\infty$ then
$$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell,T)=\ker[H^1(\mathbf{Q}_\ell,T)\to H^1(\mathbf{Q}_\ell^{\mathrm{unr}},T\otimes\mathbf{Q}_p)],$$
- $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_p,T)=H^1(\mathbf{Q}_p,T)$,
- $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{R},T)=H^1(\mathbf{R},T)$.

If I is an ideal of R we define the canonical Selmer structure on T/IT to be $\mathcal{F}_{\mathrm{can}}\otimes R/I$, the Selmer structure induced by $\mathcal{F}_{\mathrm{can}}$ on T/IT. (Note that this depends on T, not only on T/IT.) We will write simply $\mathcal{F}_{\mathrm{can}}$ instead of $\mathcal{F}_{\mathrm{can}}\otimes R/I$. It is not true in general that $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_p,T/IT)=H^1(\mathbf{Q}_p,T/IT)$; see Lemma A.1.

DEFINITION 3.2.2. Fix a set $\mathcal{P}$ of primes, different from p, where T is unramified (so $(T,\mathcal{F}_{\mathrm{can}},\mathcal{P})$ is a Selmer triple), and a (possibly infinite) abelian extension $\mathcal{K}$ of $\mathbf{Q}$. An *Euler system* $\mathbf{c}$ for $(T,\mathcal{P},\mathcal{K})$ is a collection

$$\{c_F\in H^1(F,T) : F\subset\mathcal{K}, F/\mathbf{Q}\text{ finite}\}$$

such that whenever $F\subset F'\subset\mathcal{K}$ and $F'/\mathbf{Q}$ is finite,

$$\mathbf{N}_{F'/F}c_{F'}=\Big(\prod P_\ell(\mathrm{Fr}_\ell^{-1})\Big)\,c_F.$$

Here $\mathbf{N}_{F'/F}$ is the corestriction map from F' to F, the product is over primes $\ell\in\mathcal{P}$ which ramify in $F'/\mathbf{Q}$ but not in $F/\mathbf{Q}$, and $P_\ell(x)=\det(1-\mathrm{Fr}_\ell\ x\mid T)$ as in Definition 2.2.1.

Let $\mathbf{ES}(T,\mathcal{P},\mathcal{K})$ (or simply $\mathbf{ES}(T)$, if there is no danger of confusion) denote the collection of Euler systems for $(T,\mathcal{P},\mathcal{K})$. Then $\mathbf{ES}(T)$ is a $\mathbf{Z}_p[[G_{\mathbf{Q}}]]$-module.

REMARK 3.2.3. The "Euler factors" $P_\ell(\mathrm{Fr}_\ell^{-1})$ in Definition 3.2.2 are slightly different from the ones used in [**Ru6**] Definition 2.1.1. However, it is easy to switch back and forth between the two choices, and they give equivalent theories and isomorphic modules $\mathbf{ES}(T)$. See §9.6 of [**Ru6**]. We use the present choice here because it simplifies the formulas in the proof of Theorem 3.2.4.

THEOREM 3.2.4. *Suppose that $\mathcal{K}$ contains the maximal abelian p-extension of $\mathbf{Q}$ which is unramified outside of p and $\mathcal{P}$, and*

(a) *$T/(\mathrm{Fr}_\ell-1)T$ is a cyclic R-module for every $\ell\in\mathcal{P}$,*

(b) *$\mathrm{Fr}_\ell^{p^k}-1$ is injective on T for every $\ell\in\mathcal{P}$ and every $k\geq 0$.*

Then there is a canonical homomorphism $\mathbf{ES}(T)\to\overline{\mathbf{KS}}(T,\mathcal{F}_{\mathrm{can}},\mathcal{P})$ which is $G_{\mathbf{Q}}$-equivariant (with $G_{\mathbf{Q}}$ acting trivially on $\overline{\mathbf{KS}}(T)$) with the property that if $\mathbf{c}$ maps to $\boldsymbol{\kappa}$, then $\kappa_1=c_{\mathbf{Q}}$.

If further $H^0(\mathbf{Q}_p, T^*)$ is a divisible R-module, then there is a canonical $G_{\mathbf{Q}}$-equivariant homomorphism $\mathbf{ES}(T) \to \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ with the property that if $\mathbf{c}$ maps to $\boldsymbol{\kappa}$, then $\kappa_1 = c_{\mathbf{Q}}$.

The proof of this theorem is given in Appendix A. If we let $\{\kappa_n\}$ denote the collection of derivative classes of the Euler system $\mathbf{c}$ as defined for example in Chapter 4 of [**Ru6**], then the results of that chapter show that this collection is a weak Kolyvagin system. A minor modification of these classes gives a Kolyvagin system. Since the proof is tedious and unrelated to the rest of this paper, we defer it to Appendix A.

REMARK 3.2.5. Suppose $\rho : \mathrm{Gal}(\mathcal{K}/\mathbf{Q}) \to R^\times$ is a character of finite order. Writing $\mathcal{P}_\rho = \{\ell \in \mathcal{P} : \rho \text{ is unramified at } \ell\}$, and again writing $\mathcal{F}_{\mathrm{can}}$ for the canonical Selmer structure on $T \otimes \rho$, we get a new Selmer triple $(T \otimes \rho, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_\rho)$.

As in §2.4 of [**Ru6**], if we fix a generator of the free rank-one R-module ρ, we obtain a map

$$\mathbf{ES}(T, \mathcal{P}, \mathcal{K}) \to \mathbf{ES}(T \otimes \rho, \mathcal{P}_\rho, \mathcal{K})$$

with the property that if $\mathbf{c} \mapsto \mathbf{c}^\rho$ and L is the fixed field of the kernel of ρ, then the image of $c^\rho_{\mathbf{Q}}$ under the composition

$$H^1(\mathbf{Q}, T \otimes \rho) \xrightarrow{\mathrm{res}} H^1(L, T \otimes \rho) \cong H^1(L, T)$$

is $\sum_{\delta \in \mathrm{Gal}(L/\mathbf{Q})} \rho(\delta) c^\delta_L$. Thus, using Theorem 3.2.4 (and increasing the ring R as necessary, to include the values of ρ), an Euler system for T gives rise to a Kolyvagin system for $T \otimes \rho$ for every character ρ of finite order of $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$.

It is not difficult to show that the Kolyvagin systems obtained in this way "interpolate", in the sense that if $\rho \equiv \rho' \pmod{\mathfrak{m}^k}$, then the induced Kolyvagin systems coincide in $\mathbf{KS}((T/\mathfrak{m}^k T) \otimes \rho) = \mathbf{KS}((T/\mathfrak{m}^k T) \otimes \rho')$.

REMARK 3.2.6. In Theorem 3.2.4 above, we require that $\mathcal{K}$ contains the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$. In other words, the Euler system "extends in the p-direction", and in particular each class c_F is a universal norm from $F\mathbf{Q}_\infty$.

As discussed in §9.1 of [**Ru6**], it is possible to remove this requirement if we replace it with some other appropriate condition. The following variant of Theorem 3.2.4 is proved by combining §9.1 of [**Ru6**] with the proof of Theorem 3.2.4 in Appendix A.

THEOREM 3.2.7. *Suppose that $\mathcal{K}$ contains the maximal abelian p-extension of $\mathbf{Q}$ which is unramified outside of some cofinite set of primes containing $\mathcal{P}$, and that* (a) *and* (b) *of Theorem 3.2.4 hold. Suppose in addition that $c_F \in H^1_{\mathcal{F}_{\mathrm{can}}}(F, T)$ for every F and that there is a $\gamma \in G_{\mathbf{Q}}$ such that $\gamma - 1$ kills $\boldsymbol{\mu}_{p^\infty}$ and $\gamma - 1$ is injective on T. Then there is a canonical homomorphism $\mathbf{ES}(T) \to \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}})$ with the property that if $\mathbf{c}$ maps to $\boldsymbol{\kappa}$, then $\kappa_1 = c_{\mathbf{Q}}$.*

If further $H^0(\mathbf{Q}_p, T^*)$ is a divisible R-module, then this homomorphism factors through a map $\mathbf{ES}(T) \to \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$.

For examples of Euler systems and applications of the corresponding Kolyvagin systems, see §6.1 and §6.2.

3.3. Simplicial sheaves and Selmer groups

Suppose $\mathcal{P}$ is a set of primes, $\mathcal{X} = \mathcal{X}(\mathcal{P})$ is the graph defined in Definition 3.1.2, and $\mathcal{S}$ is a (simplicial) sheaf on $\mathcal{X}$ as in Definition 3.1.1. If ℓ is prime and

$n\ell \in \mathcal{N}$, we will write $e_{n,n\ell}$ for the edge in $\mathcal{X}$ joining the vertices n and $n\ell$, and we will write simply e_ℓ for $e_{1,\ell}$.

DEFINITION 3.3.1. Suppose further that for every edge $e_{n,n\ell}$ we have an isomorphism of edge stalks

$$\mathcal{S}(e_{n,n\ell}) \xrightarrow{\sim} \mathcal{S}(e_\ell) \tag{6}$$

Using these isomorphisms to identify $\mathcal{S}(e_{n,n\ell})$ and $\mathcal{S}(e_\ell)$, we define for every vertex n of $\mathcal{X}$

$$\psi_n : \mathcal{S}(n) \longrightarrow \bigoplus_{\ell|n} \mathcal{S}(e_\ell)$$

by $\psi_n = \oplus_{\ell|n} \psi_n^{e_{n/\ell,n}}$, where $\psi_n^{e_{n/\ell,n}} : \mathcal{S}(n) \to \mathcal{S}(e_{n/\ell,n})$ is the vertex-to-edge map of $\mathcal{S}$.

If $\boldsymbol{\kappa}$ is a global section of $\mathcal{S}$, then for every $n \in \mathcal{N}$ and $j > 0$ we define the *Kolyvagin-constructed dual Selmer group* by

$$\mathrm{Sel}^*(\boldsymbol{\kappa}; n) = \Big(\bigoplus_{\ell|n} \mathcal{S}(e_\ell)\Big) \Big/ \Big(\sum_{d|n} \psi_d(R\kappa_d)\Big)$$

If $n \mid m$ there is a natural map $\mathrm{Sel}^*(\boldsymbol{\kappa}; n) \to \mathrm{Sel}^*(\boldsymbol{\kappa}; m)$, and we define

$$\mathrm{Sel}^*(\boldsymbol{\kappa}) = \varinjlim_{n \in \mathcal{N}} \mathrm{Sel}^*(\boldsymbol{\kappa}; n).$$

EXAMPLE 3.3.2. Fix a Selmer triple $(T, \mathcal{F}, \mathcal{P})$, and let $\mathcal{S}$ be the Selmer sheaf $\mathcal{H}_{(T,\mathcal{F},\mathcal{P})}$ of Definition 3.1.2.

Suppose first that $I_\ell = 0$ for every $\ell \in \mathcal{P}$. (For example, this will be true if R is artinian, say $\mathfrak{m}^k = 0$, and $\mathcal{P} = \mathcal{P}_k$ where $\mathcal{P}_k$ is as in Definition 3.1.6.) Then for every $n \in \mathcal{N}$ we have $\mathcal{S}(e_{n,n\ell}) = H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T) \otimes G_{n\ell}$. Fixing a generator of G_ℓ for every $\ell \in \mathcal{P}$ induces isomorphisms $\mathcal{S}(e_{n,n\ell}) \cong \mathcal{S}(e_\ell) \cong H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$ as in (6), and with these identifications we have $\mathrm{Sel}^*(\boldsymbol{\kappa})$ as above for every $\boldsymbol{\kappa} \in \mathbf{KS}(T)$.

PROPOSITION 3.3.3. *With notation and assumptions as in Example 3.3.2, for every $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ there is a canonical map*

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \longrightarrow \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}), \mathbf{Q}_p/\mathbf{Z}_p)$$

with kernel $\cap_{n\in\mathcal{N}} H^1_{\mathcal{F}^*_n}(\mathbf{Q}, T^*)$.

PROOF. Global duality (Theorem 2.3.4) gives an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1_{\mathcal{F}^*_n}(\mathbf{Q}, T^*) &\longrightarrow H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \\ &\longrightarrow \mathrm{Hom}\big((\bigoplus_{\ell|n} H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T))/\mathrm{image}(H^1_{\mathcal{F}^n}(\mathbf{Q}, T)), \mathbf{Q}_p/\mathbf{Z}_p\big). \end{aligned}$$

Since $\kappa_d \in H^1_{\mathcal{F}^n}(\mathbf{Q}, T) \otimes G_d$ for every d dividing n, the proposition follows directly from this. □

If $\mathcal{P}$ is large enough so that $\cap_{n\in\mathcal{N}} H^1_{\mathcal{F}^*_n}(\mathbf{Q}, T^*) = 0$, then the map of Proposition 3.3.3 will be injective. Under suitable hypotheses on T and $\boldsymbol{\kappa}$ (see Theorem 4.5.12) we will show that this map is surjective as well, so that $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \cong \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}), \mathbf{Q}_p/\mathbf{Z}_p)$.

DEFINITION 3.3.4. Fix a Selmer triple $(T, \mathcal{F}, \mathcal{P})$, but we no longer assume that $I_\ell = 0$ for $\ell \in \mathcal{P}$. For $k \geq 0$ let $\mathcal{S}_k$ be the Selmer sheaf $\mathcal{H}_{(T/\mathfrak{m}^k T, \mathcal{F}, \mathcal{P}\cap\mathcal{P}_k)}$ where $\mathcal{P}_k$ is as in Definition 3.1.6. In particular $I_\ell = 0$ in $R/\mathfrak{m}^k$ for every $\ell \in \mathcal{P}_k$, so we can

apply Example 3.3.2 and Proposition 3.3.3 to $\mathcal{S}_k$. If $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ let $\boldsymbol{\kappa}^{(k)}$ denote the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/\mathfrak{m}^k T)$. The maps $T/\mathfrak{m}^k \twoheadrightarrow T/\mathfrak{m}^j$ for $j < k$ induce maps $\mathrm{Sel}^*(\boldsymbol{\kappa}^{(k)}) \to \mathrm{Sel}^*(\boldsymbol{\kappa}^{(j)})$, and we define

$$\mathrm{Sel}^*_\infty(\boldsymbol{\kappa}) = \varprojlim_k \mathrm{Sel}^*(\boldsymbol{\kappa}^{(k)}).$$

For every $j < k$ we have a commutative diagram

$$\begin{array}{ccc} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}^k]) & \longrightarrow & \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}^{(k)}), \mathbf{Q}_p/\mathbf{Z}_p) \\ \uparrow & & \uparrow \\ H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}^j]) & \longrightarrow & \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}^{(j)}), \mathbf{Q}_p/\mathbf{Z}_p) \end{array}$$

where the horizontal maps are from Proposition 3.3.3. Passing to the limit and using that $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \xrightarrow{\sim} \varinjlim H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}^k])$, we get a canonical map

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \longrightarrow \mathrm{Hom}(\mathrm{Sel}^*_\infty(\boldsymbol{\kappa}), \mathbf{Q}_p/\mathbf{Z}_p).$$

3.4. Sheaves and monodromy

Suppose for this section that $\mathcal{S}$ is a sheaf on a graph X, as in Definition 3.1.1.

Definition 3.4.1. If v and w are vertices of X, a *path* in X from v to w is a sequence of vertices $(v = v_1, v_2, \ldots, v_k = w)$ in X such that for each i, v_i and v_{i+1} are joined by an edge e_i. The graph X is *connected* if every pair of vertices v, w there is a path from v to w. A *loop* in X (at v) is a path from v to v.

Let r be a positive integer. We say that $\mathcal{S}$ is *locally free of rank* r if all the R-modules $\mathcal{S}(v)$, $\mathcal{S}(e)$ are free of rank r and all the maps ψ^e_v are isomorphisms. If $\mathcal{S}$ is locally free and $P = (v_1, v_2, \ldots, v_k)$ is a path in X, we can define an isomorphism $\psi_P : \mathcal{S}(v_1) \xrightarrow{\sim} \mathcal{S}(v_k)$ by

$$\psi_P = (\psi^{e_{k-1}}_{v_k})^{-1} \circ \psi^{e_{k-1}}_{v_{k-1}} \circ (\psi^{e_{k-2}}_{v_{k-1}})^{-1} \circ \cdots \circ (\psi^{e_1}_{v_2})^{-1} \circ \psi^{e_1}_{v_1}.$$

We say that $\mathcal{S}$ has *trivial monodromy* if $\mathcal{S}$ is locally free and for every vertex v of X and every loop P at v, ψ_P is the identity map in $\mathrm{Aut}(\mathcal{S}(v))$.

Definition 3.4.2. We say that $\mathcal{S}$ is *locally cyclic* if all the R-modules $\mathcal{S}(v)$, $\mathcal{S}(e)$ are cyclic and all the maps ψ^e_v are surjective.

If $\mathcal{S}$ is locally cyclic then a *surjective path* (relative to $\mathcal{S}$) from v to w is a path $(v = v_1, v_2, \ldots, v_k = w)$ in X such that for each i, if v_i and v_{i+1} are joined by the edge e_i, then $\psi^{e_i}_{v_{i+1}}$ is an isomorphism. We say that the vertex v is a *hub* of $\mathcal{S}$ if for every vertex w there is an $\mathcal{S}$-surjective path from v to w.

Suppose now that the sheaf $\mathcal{S}$ is locally cyclic. If $P = (v_1, v_2, \ldots, v_k)$ is a surjective path in X, we can define a surjective map $\psi_P : \mathcal{S}(v_1) \to \mathcal{S}(v_k)$ by

$$\psi_P = (\psi^{e_{k-1}}_{v_k})^{-1} \circ \psi^{e_{k-1}}_{v_{k-1}} \circ (\psi^{e_{k-2}}_{v_{k-1}})^{-1} \circ \cdots \circ (\psi^{e_1}_{v_2})^{-1} \circ \psi^{e_1}_{v_1}$$

since all the inverted maps are isomorphisms. We will say that $\mathcal{S}$ has *trivial monodromy* if whenever v, w, w' are vertices, P, P' are surjective paths $(v, \ldots, w)$ and $(v, \ldots, w')$, and w, w' are joined by an edge e, then $\psi^e_w \circ \psi_P = \psi^e_{w'} \circ \psi_{P'} \in \mathrm{Hom}(\mathcal{S}(v), \mathcal{S}(e))$. In particular for every pair v, w of vertices and and every pair P, P' of surjective paths from v to w, we require that $\psi_P = \psi_{P'} \in \mathrm{Hom}(\mathcal{S}(v), \mathcal{S}(w))$.

REMARK 3.4.3. If $\mathcal{S}$ is locally free of rank one, then it is also locally cyclic, every path is a surjective path, and the definitions of "trivial monodromy" in Definitions 3.4.1 and 3.4.2 are equivalent. If $\mathcal{S}$ is locally free of rank one and connected, then every vertex is a hub.

Recall that a global section of $\mathcal{S}$ is a collection of elements $\kappa_v \in \mathcal{S}(v)$ for every vertex v, which are compatible with respect to the maps ψ_v^e.

PROPOSITION 3.4.4. *Suppose $\mathcal{S}$ is locally cyclic and v is a hub of $\mathcal{S}$.*

(i) *The map $f_v : \Gamma(\mathcal{S}) \to \mathcal{S}(v)$ defined by $\boldsymbol{\kappa} \mapsto \kappa_v$ is injective, and is surjective if and only if $\mathcal{S}$ has trivial monodromy.*
(ii) *$\Gamma(\mathcal{S})$ is (noncanonically) isomorphic to an ideal of R.*
(iii) *If $\boldsymbol{\kappa} \in \Gamma(\mathcal{S})$, and if u is a vertex such that $\kappa_u \neq 0$ and κ_u generates $\mathfrak{m}^i\mathcal{S}(u)$ for some $i \in \mathbf{Z}^+$, then κ_w generates $\mathfrak{m}^i\mathcal{S}(w)$ for every vertex w.*

PROOF. For every vertex w fix a surjective path P_w from v to w. If $\boldsymbol{\kappa} \in \Gamma(\mathcal{S})$ then $\kappa_w = \psi_{P_w}(\kappa_v)$ for every w, so the map f_v of (i) is injective.

Now fix $c \in \mathcal{S}(v)$ and for every vertex w define $\kappa_w = \psi_{P_w}(c)$. If $\mathcal{S}$ has trivial monodromy then this is independent of the choice of P_w, and defines a global section $\boldsymbol{\kappa}$. Thus c is in the image of f_v and hence f_v is surjective as well.

Conversely, suppose f_v is surjective. Then for every $c \in \mathcal{S}(v)$ we can find $\boldsymbol{\kappa} \in \Gamma(\mathcal{S})$ with $\kappa_v = c$. If w, w' are vertices connected by an edge e, then we must have

$$\psi_w^e \circ \psi_{P_w}(c) = \psi_w^e(\kappa_w) = \psi_{w'}^e(\kappa_{w'}) = \psi_{w'}^e \circ \psi_{P_{w'}}(c) \in \mathcal{S}(e).$$

Thus $\mathcal{S}$ has trivial monodromy.

This proves (i), (ii) is immediate from (i), and (iii) follows from the surjectivity of the maps ψ_{P_w}. □

DEFINITION 3.4.5. A global section $\kappa \in \Gamma(\mathcal{S})$ will be called *primitive* if for every vertex v, $\kappa(v) \in \mathcal{S}(v)$ is a generator of the R-module $\mathcal{S}(v)$.

It follows from Proposition 3.4.4 that a locally cyclic sheaf $\mathcal{S}$ has a primitive global section if and only if $\mathcal{S}$ has trivial monodromy.

3.5. Hypotheses on T, $\mathcal{F}$, and $\mathcal{P}$

In this section we record and discuss several hypotheses which will play a role in the following sections. Fix a Selmer triple $(T, \mathcal{F}, \mathcal{P})$.

Consider the following properties:

(H.0) T is a free R-module of finite rank.

(H.1) $T/\mathfrak{m}T$ is an absolutely irreducible $\Bbbk[G_{\mathbf{Q}}]$-representation.

(H.2) There is a $\tau \in G_{\mathbf{Q}}$ such that $\tau = 1$ on $\boldsymbol{\mu}_{p^\infty}$ and $T/(\tau - 1)T$ is free of rank one over R.

(H.3) $H^1(\mathbf{Q}(T, \boldsymbol{\mu}_{p^\infty})/\mathbf{Q}, T/\mathfrak{m}T) = H^1(\mathbf{Q}(T, \boldsymbol{\mu}_{p^\infty})/\mathbf{Q}, T^*[\mathfrak{m}]) = 0$.

(H.4) Either
  (H.4a) $\mathrm{Hom}_{\mathbf{F}_p[[G_{\mathbf{Q}}]]}(T/\mathfrak{m}T, T^*[\mathfrak{m}]) = 0$, or
  (H.4b) $p > 4$.

(H.5) $\mathcal{P}_t \subset \mathcal{P} \subset \mathcal{P}_1$ for some $t \in \mathbf{Z}^+$, where for $k \in \mathbf{Z}^+$ $\mathcal{P}_k$ is given by Definition 3.1.6.

(H.6) For every $\ell \in \Sigma(\mathcal{F})$, the local condition $\mathcal{F}$ at ℓ is cartesian (in the sense of Definition 1.1.4) on the category $\mathrm{Quot}_R(T)$ of quotients of T of Example 1.1.3.

These hypotheses hold in many, but not all, cases of interest. See §6.1 and §6.2, especially Lemmas 6.1.5 and 6.2.3. We have already assumed that (H.0) holds.

Remark 3.5.1. Note that (H.2) holds trivially when $\mathrm{rank}(T) = 1$, with $\tau = 1$. The condition $\mathcal{P} \subset \mathcal{P}_1$ in (H.5) is reasonably harmless because we can always replace $\mathcal{P}$ by $\mathcal{P} \cap \mathcal{P}_1$. Condition (H.6) holds trivially when R is a field, because in that case category $\mathrm{Quot}_R(T)$ has only two objects, 0 and T.

Also, if $R \twoheadrightarrow R'$ is a surjective homomorphism of (complete) local rings and T satisfies (H.i), then so does $T \otimes_R R'$ viewed as an $R'[[G_{\mathbf{Q}}]]$-module, for any $i = 0, \ldots, 4$.

Condition (H.1) implies that $T^*[\mathfrak{m}]$ is also an absolutely irreducible $\Bbbk[[G_{\mathbf{Q}}]]$-representation.

Lemma 3.5.2. *Suppose that* (H.3) *holds. Then for every subquotient S of T or of T^*, $S^{G_{\mathfrak{Q}}} = 0$.*

Proof. It follows from (H.3) that $(T/\mathfrak{m}T)^{G_{\mathfrak{Q}}} = T^*[\mathfrak{m}]^{G_{\mathfrak{Q}}} = 0$. If S is a subquotient of T, then $S^{G_{\mathfrak{Q}}} = 0$ by Lemma 2.1.4.

The proof for subquotients of T^* is similar, applying Lemma 2.1.4 to the finitely generated R-module $\mathrm{Hom}(T^*, \mathbf{Q}_p/\mathbf{Z}_p)$. □

Lemma 3.5.3. *Suppose that* (H.1) *and* (H.3) *hold, and I is an ideal of R. Then the inclusion $T^*[I] \hookrightarrow T^*$ induces an isomorphism*

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[I]) \xrightarrow{\sim} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[I].$$

Proof. Suppose first that I is principal with a generator β. Cohomology of the exact sequences

$$0 \longrightarrow T^*[I] \longrightarrow T^* \xrightarrow{\beta} IT^* \longrightarrow 0$$

$$0 \longrightarrow IT^* \longrightarrow T^* \longrightarrow T^*/IT^* \longrightarrow 0$$

gives (writing $G = \mathrm{Gal}(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q})$, and using Lemma 3.5.2 to obtain the zeros on the left)

$$0 \longrightarrow H^1(G, T^*[I]) \longrightarrow H^1(G, T^*) \xrightarrow{\beta} H^1(G, IT^*)$$

$$0 \longrightarrow H^1(G, IT^*) \longrightarrow H^1(G, T^*).$$

Thus we have an isomorphism

$$H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T^*[I]) \xrightarrow{\sim} H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T^*)[I] \tag{7}$$

in this case.

By induction the isomorphism (7) extends to all ideals I: if $I = (\beta_1, \ldots, \beta_i)$ just apply (7) with R replaced by $R' = R/(\beta_1, \ldots, \beta_{i-1})$, T replaced by $T \otimes R'$, and $I = \beta_i R'$.

The Selmer structure $\mathcal{F}^*$ on $T^*[I]$ is the one induced on it (as a submodule) by the Selmer structure $\mathcal{F}^*$ on T^* (see Example 1.3.3). Consider the commutative

diagram

$$\begin{array}{ccccc} 0 \to H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[I]) & \to H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T^*[I]) & \to \bigoplus_{\ell\in\Sigma(\mathcal{F})} H^1(\mathbf{Q}_\ell, T^*[I])/H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*[I]) \\ \downarrow & \downarrow & \downarrow \\ 0 \to H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[I] & \to H^1(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q}, T^*)[I] & \to \bigoplus_{\ell\in\Sigma(\mathcal{F})} H^1(\mathbf{Q}_\ell, T^*)/H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*). \end{array}$$

The rows are exact by definition of $H^1_{\mathcal{F}^*}$, (7) shows that the center vertical map is an isomorphism, and by definition of the induced Selmer structure the right-hand vertical map is injective. Therefore the left-hand vertical map is an isomorphism, which proves the lemma. □

LEMMA 3.5.4. *Suppose R is artinian and principal of length k, T satisfies* (H.0), (H.1), (H.3), *and* (H.6), *$0 < i \le k$, and π is a generator of $\mathfrak{m}$. Then the injection $\pi^{k-i} : T/\mathfrak{m}^i T \hookrightarrow T$ induces isomorphisms*

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

and $H^1_{\mathcal{F}}(\mathbf{Q}, T)[\mathfrak{m}^i] = \ker[H^1_{\mathcal{F}}(\mathbf{Q}, T) \to H^1_{\mathcal{F}}(\mathbf{Q}, T/\mathfrak{m}^{k-i}T)]$.

PROOF. As in the proof of Lemma 3.5.3 (using Lemma 3.5.2), cohomology of the exact sequences

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

shows that $[\pi^{k-i}] : H^1(\mathbf{Q}, T/\mathfrak{m}^i T) \to H^1(\mathbf{Q}, T)[\mathfrak{m}^i]$ is an isomorphism.

It is easy to check that $[\pi^{k-i}]$ maps $H^1_{\mathcal{F}}(\mathbf{Q}, T/\mathfrak{m}^i T)$ into $H^1_{\mathcal{F}}(\mathbf{Q}, T)[\mathfrak{m}^i]$. To prove the lemma we need to show that $[\pi^{k-i}]^{-1}H^1_{\mathcal{F}}(\mathbf{Q}, T)$ satisfies the local conditions to lie in $H^1_{\mathcal{F}}(\mathbf{Q}, T/\mathfrak{m}^i T)$. For primes $\ell \in \Sigma(\mathcal{F})$ this holds by (H.6), so suppose $\ell \notin \Sigma(\mathcal{F})$. We need to show that $[\pi^{k-i}]^{-1}H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T) \subset H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/\mathfrak{m}^i T)$.

Writing $\mathcal{I}_\ell$ for the inertia group in $G_{\mathbf{Q}_\ell}$, we have a diagram with exact rows

$$\begin{array}{ccccc} 0 \hookrightarrow H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/\mathfrak{m}^i T) & \longrightarrow & H^1(\mathbf{Q}_\ell, T/\mathfrak{m}^i T) & \longrightarrow & \mathrm{Hom}(\mathcal{I}_\ell, T/\mathfrak{m}^i T) \\ \downarrow{\scriptstyle [\pi^{k-i}]} & & \downarrow{\scriptstyle [\pi^{k-i}]} & & \downarrow{\scriptstyle [\pi^{k-i}]} \\ 0 \hookrightarrow H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T) & \longrightarrow & H^1(\mathbf{Q}_\ell, T) & \longrightarrow & \mathrm{Hom}(\mathcal{I}_\ell, T). \end{array}$$

The right-hand vertical map is injective, so if $c \in H^1(\mathbf{Q}_\ell, T/\mathfrak{m}^i T)$ and $[\pi^{k-i}]c$ is unramified, then c is unramified. □

DEFINITION 3.5.5. Recall the set $\mathcal{P}_k$ of Definition 3.1.6, and let $\mathcal{N}_k = \mathcal{N}(\mathcal{P}_k)$ be the corresponding set of positive integers as in Definition 2.2.1: all squarefree products of primes in $\mathcal{P}_k$.

LEMMA 3.5.6. *Suppose $k \in \mathbf{Z}^+$ and T satisfies* (H.0), *and p^d generates the kernel of the map $\mathbf{Z}_p \to R/\mathfrak{m}^k$.*

(i) *Suppose $\tau \in G_{\mathbf{Q}}$ satisfies* (H.2). *If $\ell \notin \Sigma(\mathcal{F})$ and the Frobenius class of ℓ in $\mathrm{Gal}(\mathbf{Q}(T/\mathfrak{m}^k T, \boldsymbol{\mu}_{p^d})/\mathbf{Q})$ is the conjugacy class of τ, then $\ell \in \mathcal{P}_k$.*

(ii) *Suppose R is principal and artinian of length k, and $\ell \in \mathcal{P}_k$. Then $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$, and $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T^*)$ are free of rank one over R, and the map ϕ_ℓ^{fs} of Definition 1.2.2 is an isomorphism.*

PROOF. If the Frobenius of ℓ in $\mathrm{Gal}(\mathbf{Q}(T/\mathfrak{m}^k T, \boldsymbol{\mu}_{p^k})/\mathbf{Q})$ belongs to the conjugacy class of τ, then

$$T/(\mathfrak{m}^k T + (\mathrm{Fr}_\ell - 1)T) = T/(\mathfrak{m}^k T + (\tau - 1)T)$$

which is free of rank one over $R/\mathfrak{m}^k$ by (H.2). Further

$$P_\ell(1) = \det(1 - \mathrm{Fr}_\ell | T) \equiv \det(1 - \tau \mid T) = 0 \pmod{\mathfrak{m}^k}$$

and, writing $\varepsilon_{\mathrm{cycl}}$ for the cyclotomic character,

$$\ell - 1 = \varepsilon_{\mathrm{cycl}}(\mathrm{Fr}_\ell) - 1 \equiv \varepsilon_{\mathrm{cycl}}(\tau) - 1 = 0 \pmod{p^d}$$

so $I_\ell \subset \mathfrak{m}^k$. Thus $\ell \in \mathcal{P}_k$, which proves (i).

For (ii), suppose $\ell \in \mathcal{P}_k$. Then Lemma 1.2.3 shows that $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ and $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$ are free of rank one and ϕ_ℓ^{fs} is an isomorphism. Local duality (Proposition 1.3.2) gives perfect pairings

$$H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*) \times H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T) \to \mathbf{Q}_p/\mathbf{Z}_p, \quad H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T^*) \times H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T) \to \mathbf{Q}_p/\mathbf{Z}_p.$$

Since R is artinian and principal we conclude that $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$ and $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T^*)$ are free of rank one over R as well. □

3.6. Choosing useful primes

In this section we apply the Cebotarev theorem carefully to produce primes with properties that we will need in the following sections. For this section we assume that R is artinian and principal, and that T is an $R[[G_{\mathbf{Q}}]]$-module satisfying the Hypotheses (H.0-5) of §3.5. In particular, it is (only) for the results of this section that we use (H.4).

Note that T^* also satisfies (H.0-5), so the arguments below for T apply equally to T^*.

This section is devoted to the proofs of the following two propositions.

PROPOSITION 3.6.1. *Suppose $c_1, c_2 \in H^1(\mathbf{Q}, T)$ and $c_3, c_4 \in H^1(\mathbf{Q}, T^*)$ are all nonzero. For every $k \in \mathbf{Z}^+$ there is a set $S \subset \mathcal{P}_k$ of positive density such that for every $\ell \in S$, the localizations $(c_i)_\ell$ are all nonzero.*

PROPOSITION 3.6.2. *Fix a finite R-submodule $C \subset H^1(\mathbf{Q}, T)$, a homomorphism $\phi : C \to R$, and $k \in \mathbf{Z}^+$. Suppose that the image of $R \to \mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \mathrm{End}(T)$.*

(i) *There is a set $S \subset \mathcal{P}_k$ of positive density such that for every $\ell \in S$,*

$$\ker[\mathrm{loc}_\ell : C \to H^1(\mathbf{Q}_\ell, T)] = \ker(\phi)$$

where loc_ℓ is localization at ℓ.

(ii) *Suppose in addition that* (H.4a) *holds, that D is a finite submodule of $H^1(\mathbf{Q}, T^*)$, and that $\psi : D \to R$ is a homomorphism. Then there is a set $S \subset \mathcal{P}_k$ of positive density such that for every $\ell \in S$,*

$$\ker[\mathrm{loc}_\ell : C \to H^1(\mathbf{Q}_\ell, T)] = \ker(\phi), \quad \ker[\mathrm{loc}_\ell : D \to H^1(\mathbf{Q}_\ell, T^*)] = \ker(\psi).$$

Propositions 3.6.1 and 3.6.2 will be proved below.

Increasing k if necessary, we may assume that $\mathfrak{m}^k = 0$. Let $F = \mathbf{Q}(T, \boldsymbol{\mu}_{p^k}) = \mathbf{Q}(T, T^*, \boldsymbol{\mu}_{p^k})$, and note that F is a finite Galois extension of $\mathbf{Q}$. Fix $\tau \in G_{\mathbf{Q}}$ satisfying (H.2).

Suppose that $C \subset H^1(\mathbf{Q}, T)$ is a finite submodule, and consider the composition

$$C \xrightarrow{\text{res}_F} H^1(F,T)^{G_{\mathfrak{Q}}} = \text{Hom}(G_F, T)^{G_{\mathfrak{Q}}} \longrightarrow \text{Hom}(G_F, T/(\tau-1)T). \tag{8}$$

The first map is injective by (H.3). If f belongs to the kernel of the last map then the image of f is a $G_{\mathbf{Q}}$-stable subgroup of $(\tau-1)T$. Using (H.1) and (H.2) we conclude that $f = 0$, and hence the composition (8) is injective. Let F_C be the smallest extension of F such that the image of C in $\text{Hom}(G_F, T)$ factors through $\text{Gal}(F_C/F)$. Then $F_C/\mathbf{Q}$ is Galois, and $\text{Gal}(F/\mathbf{Q})$ acts on $\text{Gal}(F_C/F)$ by conjugation.

Proof of Proposition 3.6.1. Let C_i be the R-module generated by c_i. Let F, F_{C_1}, and F_{C_2} be as defined above, and F_{C_3}, F_{C_4} the analogous fields defined with T^* instead of T. We will write simply F_i for F_{C_i}.

Define $H_1, H_2 \subset G_F$ by

$$H_i = \{\gamma \in G_F : c_i(\tau\gamma) = 0 \text{ in } T/(\tau-1)T\}.$$

Note that $c_i(\tau\gamma)$ is well-defined in $T/(\tau-1)T$ since γ acts trivially on T. Define H_3, H_4 similarly with T^* in place of T.

If $\gamma \in G_F - H_i$ and ℓ is a rational prime whose Frobenius conjugacy class in $\text{Gal}(F_i/\mathbf{Q})$ is the class of $\tau\gamma$, then $(c_i)_\ell \neq 0$ and Lemma 3.5.6(i) shows that $\ell \in \mathcal{P}_k$.

Let μ be Haar measure on G_F, normalized so that $\mu(G_F) = 1$, and let $\bar{c}_i$ be the image of c_i in $\text{Hom}(G_F, T/(\tau-1)T)$ under (8). For every i, H_i is either empty or a coset of $\ker(\bar{c}_i)$, so

$$\mu(H_i) \leq 1/|\bar{c}_i(G_F)| \leq 1/p \tag{9}$$

the last inequality by the injectivity of (8).

Suppose first that (H.4b) holds. Then $\mu(H_i) \leq 1/5$, so

$$\mu(H_1 \cup H_2 \cup H_3 \cup H_4) < 1 = \mu(G_F).$$

Choose a $\gamma \in G_F - (H_1 \cup H_2 \cup H_3 \cup H_4)$, and let S be the set of rational primes whose Frobenius conjugacy class in $\text{Gal}(F_1F_2F_3F_4/\mathbf{Q})$ is the class of $\tau\gamma$. Then S satisfies the conclusions of the proposition.

Now suppose hypothesis (H.4a) holds, so $T/\mathfrak{m}T$ and $T^*[\mathfrak{m}]$ have no nonzero isomorphic $\mathbf{F}_p[[G_{\mathbf{Q}}]]$-subquotients. The map (8) identifies $\text{Gal}(F_1F_2/F)$ (resp. $\text{Gal}(F_3F_4/F)$) with a $\mathbf{Z}_p[[G_{\mathbf{Q}}]]$-stable submodule of $\text{Hom}_R(C_1 + C_2, T)$ (resp. of $\text{Hom}_R(C_3 + C_4, T^*)$), so it follows that $F_1F_2 \cap F_3F_4 = F$.

Suppose that $H_1 \cup H_2 = G_F$. By (9) this is only possible if $p = 2$ and $\ker(\bar{c}_1) = \ker(\bar{c}_2)$ is a subgroup of index 2 in G_F. Since $T/(\tau-1)T$ is free of rank one over R, we conclude that $R\bar{c}_1 = \bar{c}_2$. It follows from the injectivity of (8) that $Rc_1 = Rc_2$ and $H_1 = H_2$, so $H_1 \cup H_2$ cannot be equal to G_F.

Similarly $H_3 \cup H_4 \neq G_F$. Choose $\gamma \in G_F - (H_1 \cup H_2)$ and $\gamma^* \in G_F - (H_3 \cup H_4)$. Again, if S is the set of rational primes whose Frobenius conjugacy class in $\text{Gal}(F_1F_2/\mathbf{Q})$ (resp. $\text{Gal}(F_3F_4/\mathbf{Q})$) is the class of $\tau\gamma$ (resp. of $\tau\gamma^*$), then S satisfies the conclusions of the proposition. □

Lemma 3.6.3. *Suppose that the image of $R \to \text{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \text{End}(T)$.*

(i) *The map* $\mathrm{Gal}(F_C/F) \to \mathrm{Hom}_R(C,T)$ *induced by the first part of* (8) *is a* $\mathbf{Z}_p[[G_{\mathbf{Q}}]]$*-isomorphism.*
(ii) *The map* $\mathrm{Gal}(F_C/F) \to \mathrm{Hom}_R(C,T/(\tau-1)T)$ *induced by* (8) *is surjective.*

Proof. We will prove (i), and then (ii) follows from assumption (H.2).

The map of (i) is $\mathrm{Gal}(F/\mathbf{Q})$-equivariant, so its image is $\mathbf{Z}_p[[G_{\mathbf{Q}}]]$-stable and hence by our assumption is an R-submodule of $\mathrm{Hom}_R(C,T)$. We give $\mathrm{Gal}(F_C/F)$ the structure of an R-module by identifying it with its image in $\mathrm{Hom}_R(C,T)$. In particular every Jordan-Holder factor of $\mathrm{Gal}(F_C/F)$ is a Jordan-Holder factor of T, and hence (since $T/\mathfrak{m}T$ is irreducible by (H.1)) is equal to $T/\mathfrak{m}T$.

With this definition, the composition (8) factors through an injection of R-modules

$$C \hookrightarrow \mathrm{Hom}_{R[[G_{\mathbf{Q}}]]}(\mathrm{Gal}(F_C/F),T).$$

Now using the fact that R is artinian and principal we have

$$\mathrm{Hom}_{R[[G_{\mathbf{Q}}]]}(T/\mathfrak{m}T,T) = \mathrm{Hom}_{R[[G_{\mathbf{Q}}]]}(T/\mathfrak{m}T,T[\mathfrak{m}]) \cong \mathrm{Hom}_{R[[G_{\mathbf{Q}}]]}(T/\mathfrak{m}T,T/\mathfrak{m}T)$$

which is free of rank one over $\Bbbk$ since $T/\mathfrak{m}T$ is absolutely irreducible. Hence we see by induction on the length of $\mathrm{Gal}(F_C/F)$ that

$$\mathrm{length}(C) \leq \mathrm{length}(\mathrm{Hom}_{R[[G_{\mathbf{Q}}]]}(\mathrm{Gal}(F_C/F),T)) \leq \frac{\mathrm{length}(\mathrm{Gal}(F_C/F))}{\mathrm{rank}_R(T)}.$$

By definition the map of (i) is injective, so it must be surjective as well. □

Proof of Proposition 3.6.2. Suppose k is large enough so that $\mathfrak{m}^k = 0$. With F and F_C as above, let G be the subgroup of $\mathrm{Gal}(F_C/\mathbf{Q})$ generated by $\mathrm{Gal}(F_C/F)$ and τ. There is a well-defined evaluation homomorphism

$$\mathrm{ev} : G \to \mathrm{Hom}(C,T/(\tau-1)T)$$

where $\mathrm{ev}(\gamma)$ is evaluation of cocycles at γ.

Fix an isomorphism $\eta : T/(\tau-1)T \xrightarrow{\sim} R$. By Lemma 3.6.3(ii) we can find $\gamma \in \mathrm{Gal}(F_C/F)$ so that

$$\mathrm{ev}(\gamma) = (\eta^{-1} \circ \phi) - \mathrm{ev}(\tau).$$

Fix such a γ. If ℓ is a rational prime whose Frobenius in $\mathrm{Gal}(F_C/F)$ is the conjugacy class of $\tau\gamma$, and such that every element of C is finite at ℓ, then the composition

$$C \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T) \xrightarrow{\sim} T/(\mathrm{Fr}_\ell - 1)T = T/(\tau-1)T$$

is the map

$$\mathrm{ev}(\mathrm{Fr}_\ell) = \mathrm{ev}(\tau\gamma) = \eta^{-1} \circ \phi$$

so in particular $\ker(\mathrm{loc}_\ell) = \ker(\phi)$. Also by Lemma 3.5.6(i) $\ell \in \mathcal{P}_k$, so this proves (i).

Now repeat the argument above with T replaced by T^* and C replaced by D. Then with the obvious notation, there is an element $\delta \in \mathrm{Gal}(F_D/F)$ such that if ℓ is a rational prime whose Frobenius in $\mathrm{Gal}(F_D/F)$ is the conjugacy class of $\tau\delta$, and such that every element of D is finite at ℓ, then $\ker(\mathrm{loc}_\ell) = \ker(\psi)$ in D.

We claim that $F_C \cap F_D = F$. For by Lemma 3.6.3(i), every simple subquotient of the $\mathbf{Z}_p[[G_{\mathbf{Q}}]]$-module $\mathrm{Gal}(F_C \cap F_D/F)$ is isomorphic both to a subquotient of $T/\mathfrak{m}T$ and to a subquotient of $T^*[\mathfrak{m}]$. By our assumption (H.4a) every such module must be zero.

Now define S to be the set of rational primes whose Frobenius in $\mathrm{Gal}(F_C/F)$ (resp. $\mathrm{Gal}(F_D/F)$) is the conjugacy class of $\tau\gamma$ (resp. $\tau\delta$), and such that every element of C and every element of D is finite at ℓ. Then S satisfies the conclusions of (ii). □

3.7. Some remarks about hypothesis (H.6)

In practice, the conditions (H.0) through (H.6) of §3.5 are generally straightforward to verify with the possible exception of (H.6). In this section we discuss (H.6), and give sufficient conditions for it to hold.

LEMMA 3.7.1. *Suppose R is a discrete valuation ring and for every $\ell \in \Sigma(\mathcal{F})$ the R-module $H^1(\mathbf{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ is torsion-free. Then for every $k \in \mathbf{Z}^+$,*

(i) *the induced Selmer structure on the $R/\mathfrak{m}^k$-module $T/\mathfrak{m}^k T$ satisfies* (H.6),
(ii) *the map $T \to T/\mathfrak{m}^k T$ induces an injection*

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

whose cokernel has order bounded independently of k.

PROOF. Fix a prime $\ell \in \Sigma(\mathcal{F})$, integers i, j, with $0 < i \leq j \leq k$, and a generator π of $\mathfrak{m}$. Consider the diagram with exact rows (all cohomology groups are over $\mathbf{Q}_\ell$)

$$\begin{array}{ccccccccc}
H^1(T) & \xrightarrow{\pi^i} & H^1(T) & \longrightarrow & H^1(T/\mathfrak{m}^i T) & \longrightarrow & H^2(T)[\mathfrak{m}^i] & \longrightarrow & 0 \\
{\scriptstyle \mathrm{id}}\downarrow & & {\scriptstyle \pi^{j-i}}\downarrow & & {\scriptstyle [\pi^{j-i}]}\downarrow & & \downarrow{\scriptstyle \cap} & & \\
H^1(T) & \xrightarrow{\pi^j} & H^1(T) & \longrightarrow & H^1(T/\mathfrak{m}^j T) & \longrightarrow & H^2(T)[\mathfrak{m}^j] & \longrightarrow & 0.
\end{array}$$

Suppose $c \in H^1(\mathbf{Q}_\ell, T/\mathfrak{m}^i T)$ and $[\pi^{j-i}]c \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T/\mathfrak{m}^j T)$. To prove that (H.6) holds for $T/\mathfrak{m}^k T$, we need to show that $c \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T/\mathfrak{m}^i T)$.

By definition (Example 2.1.7) of the Selmer structure on $T/\mathfrak{m}^j T$, the fact that $[\pi^{j-i}]c \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T/\mathfrak{m}^j T)$ means that there is a $d' \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ whose image in $H^1(\mathbf{Q}_\ell, T/\mathfrak{m}^j T)$ is $[\pi^{j-i}]c$. From the diagram it follows that there is a $d \in H^1(\mathbf{Q}_\ell, T)$ whose image in $H^1(\mathbf{Q}_\ell, T/\mathfrak{m}^i T)$ is c. But then $\pi^{j-i}d - d' \in \pi^j H^1(\mathbf{Q}_\ell, T)$, so adjusting d if necessary we may assume that $\pi^{j-i}d = d'$. If $H^1(\mathbf{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ is torsion-free then we conclude that $d \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$, and hence $c \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T/\mathfrak{m}^i T)$. This proves (i).

Write $G = \mathrm{Gal}(\mathbf{Q}_{\Sigma(\mathcal{F})}/\mathbf{Q})$. Let f denote the map of (ii) and C its cokernel. By definition we have an injection

$$H^1(G, T)/H^1_{\mathcal{F}}(\mathbf{Q}, T) \hookrightarrow \bigoplus_{\ell \in \Sigma(\mathcal{F})} H^1(\mathbf{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T), \tag{10}$$

and the R-modules on the right are all torsion-free by our assumption on the $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$. Therefore $H^1(G, T)/H^1_{\mathcal{F}}(\mathbf{Q}, T)$ is torsion-free as well. This proves the injectivity of the map g_1 in

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_{\mathcal{F}}(\mathbf{Q}, T)/\mathfrak{m}^k & \xrightarrow{f} & H^1_{\mathcal{F}}(\mathbf{Q}, T/\mathfrak{m}^k) & \longrightarrow & C & \longrightarrow & 0 \\
 & & {\scriptstyle g_1}\downarrow & & {\scriptstyle g_2}\downarrow & & {\scriptstyle g_3}\downarrow & & \\
0 & \longrightarrow & H^1(G, T)/\mathfrak{m}^k & \longrightarrow & H^1(G, T/\mathfrak{m}^k) & \longrightarrow & H^2(G, T)[\mathfrak{m}^k] & \longrightarrow & 0.
\end{array}$$

It follows that f is injective, and hence both rows of the diagram are exact. Since g_2 is injective we have a snake lemma isomorphism

$$\ker(g_3) \xrightarrow{\sim} \ker[\mathrm{coker}(g_1) \to \mathrm{coker}(g_2)],$$

and the latter is the kernel of the composition

$$\begin{aligned} H^1(G,T)/(H^1_{\mathcal{F}}(\mathbf{Q},T) + \mathfrak{m}^k H^1(G,T)) \\ \longrightarrow \bigoplus_{\ell\in\Sigma(\mathcal{F})} H^1(\mathbf{Q}_\ell,T)/(H^1_{\mathcal{F}}(\mathbf{Q}_\ell,T) + \mathfrak{m}^k H^1(\mathbf{Q}_\ell,T) \\ \longrightarrow \bigoplus_{\ell\in\Sigma(\mathcal{F})} H^1(\mathbf{Q}_\ell,T/\mathfrak{m}^k T)/H^1_{\mathcal{F}}(\mathbf{Q}_\ell,T/\mathfrak{m}^k T). \end{aligned}$$

Another straightforward diagram-chasing argument shows that the second map is injective. The kernel of the first map is $D[\mathfrak{m}^k]$ where D is the cokernel of (10). Thus we have

$$\mathrm{length}(C) \le \mathrm{length}(D[\mathfrak{m}^k]) + \mathrm{length}(H^2(G,T)[\mathfrak{m}^k]).$$

Since D and $H^2(G,T)$ are finitely-generated R-modules, this is bounded independently of k. This proves (ii). □

Remark 3.7.2. Suppose R is the integer ring of a local field. If $H^1_{\mathcal{F}}(\mathbf{Q}_\ell,T)$ is the subgroup $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T)$ defined by Bloch and Kato [**BK**], then $H^1(\mathbf{Q}_\ell,T)/H^1_{\mathcal{F}}(\mathbf{Q}_\ell,T)$ is torsion-free and Lemma 3.7.1(i) shows that (H.6) is satisfied for all quotients of R. Similarly if $H^1_{\mathcal{F}}(\mathbf{Q}_\ell,T) = H^1(\mathbf{Q}_\ell,T)$ then Lemma 3.7.1 applies.

Lemma 3.7.3. *Suppose that R is artinian and principal, $\mathcal{F}$ satisfies* (H.6)*, and $j \in \mathbf{Z}^+$. Then the induced Selmer structure on the $R/\mathfrak{m}^j$-module $T/\mathfrak{m}^j T$ satisfies* (H.6).

Proof. This clear from the statement of (H.6), since $\mathrm{Quot}_R(T/\mathfrak{m}^j T)$ is a subcategory of $\mathrm{Quot}_R(T)$. □

Lemma 3.7.4. *Suppose R is artinian and principal of length k,* (H.2) *holds, $\mathcal{F}$ satisfies* (H.6)*, and $n \in \mathcal{N}_k$. Then $\mathcal{F}(n)$ satisfies* (H.6).

Proof. Fix a prime ℓ dividing n; we need to check the condition of (H.6) for ℓ.

Fix a generator π of $\mathfrak{m}$, and $0 < i \le k$. We have a commutative diagram, where the left-hand horizontal maps come from the splitting of Lemma 1.2.4, and the isomorphisms on the right are from Lemma 1.2.1(i)

$$\begin{array}{ccccc} H^1(\mathbf{Q}_\ell,T/\mathfrak{m}^i T) & \longrightarrow & H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T/\mathfrak{m}^i T) & \xrightarrow{\sim} & T/(\pi^i,\mathrm{Fr}_\ell - 1)T \\ \downarrow{\scriptstyle [\pi^{k-i}]} & & \downarrow{\scriptstyle [\pi^{k-i}]} & & \downarrow{\scriptstyle [\pi^{k-i}]} \\ H^1(\mathbf{Q}_\ell,T) & \longrightarrow & H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T) & \xrightarrow{\sim} & T/(\mathrm{Fr}_\ell - 1)T. \end{array}$$

We have $\ell \in \mathcal{P}_k$, so $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T)$ (resp. $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T/\mathfrak{m}^i T)$) is free of rank one over R (resp. over $R/\mathfrak{m}^i$) by Lemma 3.5.6(ii). Hence the right-hand and center vertical maps are injective. Thus if $c \in H^1(\mathbf{Q}_\ell,T/\mathfrak{m}^i T)$ and $[\pi^{k-i}]c$ projects to zero in $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T)$, then c projects to zero in $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T/\mathfrak{m}^i T)$, i.e., $c \in H^1_{\mathcal{F}(n)}(\mathbf{Q}_\ell,T/\mathfrak{m}^i T)$. This proves the lemma. □

CHAPTER 4

Kolyvagin Systems over Principal Artinian Rings

We now study Kolyvagin systems in the simplest setting, where R is artinian and principal (e.g., $R = \mathbf{Z}/p^k\mathbf{Z}$). In Chapter 5 we will study Kolyvagin systems over integral domains by reducing to the case of principal artinian rings.

We assume for all of Chapter 4 that R is a principal local artinian ring, and we let $k = \text{length}(R)$, i.e., $\mathfrak{m}^k = 0$ and $\mathfrak{m}^{k-1} \neq 0$. Clearly the quotient of a discrete valuation ring by the k-th power of its maximal ideal is such a ring; conversely it is not difficult to show that every principal local artinian ring is a quotient of a discrete valuation ring (but we will not need this).

We fix for all of Chapter 4 a Selmer triple $(T, \mathcal{F}, \mathcal{P})$ satisfying hypotheses (H.0) through (H.6) of §3.5. By propagating the Selmer structure $\mathcal{F}$ to quotients of T we get Selmer triples $(T/\mathfrak{m}^i T, \mathcal{F}, \mathcal{P})$ (with R replaced by $R/\mathfrak{m}^i$) for $0 < i \leq k$. We will usually suppress $\mathcal{F}$ and $\mathcal{P}$ from the notation. By restricting to $\mathcal{P} \cap \mathcal{P}_k$, we will also assume that $\mathcal{P} \subset \mathcal{P}_k$. Thus $\mathcal{N} \subset \mathcal{N}_k$, so for all $n \in \mathcal{N}$ the ideal I_n vanishes, and the stalk of the Selmer sheaf $\mathcal{H}$ at n is $\mathcal{H}(n) = H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \otimes G_n$. Also, for every ℓ in $\mathcal{P}$, Lemma 3.5.6(ii) shows that $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$, and $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T^*)$ are free of rank one over R, and ϕ^{fs}_ℓ is an isomorphism.

Note that since R is principal artinian, T^* is also a free R-module; this is not true for general R.

Since we will use it frequently, we let $\bar{T} = T/\mathfrak{m}T$. Then $\bar{T}^* = T^*[\mathfrak{m}]$.

4.1. The core Selmer module

LEMMA 4.1.1. *Suppose $n \in \mathcal{N}$ and $0 < i \leq k$.*

(i) *The exact sequence $0 \to T/\mathfrak{m}^i T \to T \to T/\mathfrak{m}^{k-i}T \to 0$ induces an isomorphism $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/\mathfrak{m}^i T) \cong H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}^i]$ and an exact sequence*

$$0 \longrightarrow H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}^i] \longrightarrow H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \longrightarrow H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/\mathfrak{m}^{k-i}T).$$

(ii) *The inclusion $T^*[\mathfrak{m}^i] \hookrightarrow T^*$ induces an isomorphism*

$$H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*[\mathfrak{m}^i]) \xrightarrow{\sim} H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)[\mathfrak{m}^i].$$

PROOF. By Lemma 3.7.4, $(T, \mathcal{F}(n), \mathcal{P})$ satisfies the hypotheses (H.0) through (H.6). Thus (i) follows from Lemma 3.5.4, and (ii) follows from Lemma 3.5.3. □

DEFINITION 4.1.2. For every $n \in \mathcal{N}$ define

$$\lambda(n, T) = \text{length}(H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)) = \text{length}(\mathcal{H}(n)),$$
$$\lambda(n, T^*) = \text{length}(H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)).$$

Note that the second definition is equivalent to the first applied to T^*, since $\mathcal{F}(n)^* = \mathcal{F}^*(n)$ by Example 2.3.2. These definitions apply equally well when T is replaced by $T/\mathfrak{m}^i$ for $i \in \mathbf{Z}^+$.

PROPOSITION 4.1.3. *If $n \in \mathcal{N}$ then*

$$\lambda(n,\bar{T}) = 0 \iff \lambda(n,T) = 0, \qquad \lambda(n,\bar{T}^*) = 0 \iff \lambda(n,T^*) = 0.$$

PROOF. By Lemma 4.1.1 we have

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}(n)}(\mathbf{Q},T)[\mathfrak{m}], \qquad H^1_{\mathcal{F}(n)^*}(\mathbf{Q},\bar{T}^*) = H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*)[\mathfrak{m}]$$

and the proposition follows. □

PROPOSITION 4.1.4. *The differences $\lambda(n,T) - \lambda(n,T^*)$ are independent of $n \in \mathcal{N}$.*

PROOF. This follows immediately from Corollary 2.3.6 and Lemma 3.5.6(ii). □

THEOREM 4.1.5. *There are nonnegative integers r, s, one of which can be taken to be zero, such that for every $n \in \mathcal{N}$ there is a noncanonical isomorphism*

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},T) \oplus R^r \cong H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*) \oplus R^s.$$

PROOF. Since R is principal, every finitely generated R-module is a direct sum of cyclic modules $R/\mathfrak{m}^{j_i}$. It follows that the isomorphism class of an R-module B is determined by the numerical function on $\{1,2,\dots,k\}$

$$i \mapsto \text{length}(B[\mathfrak{m}^i]).$$

Thus to prove the theorem we need to show that there is an integer t such that

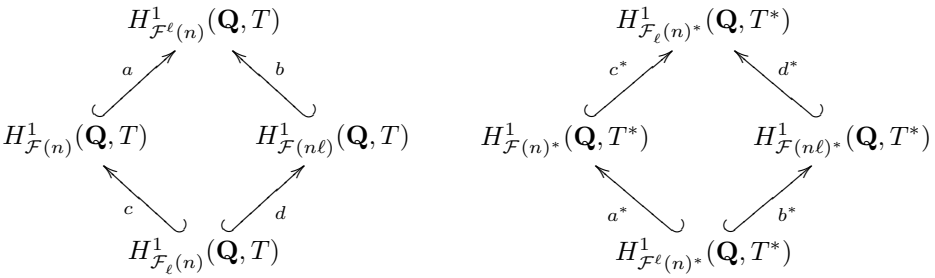
$$\text{length}(H^1_{\mathcal{F}(n)}(\mathbf{Q},T)[\mathfrak{m}^i]) - \text{length}(H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*)[\mathfrak{m}^i]) = ti$$

for $1 \le i \le k$ and for every $n \in \mathcal{N}$. By Lemma 4.1.1 the left-hand side of this equation is $\lambda(n,T/m^iT) - \lambda(n,T^*[m^i])$, which is independent of n by Proposition 4.1.4, so we need only consider $n = 1$.

Proposition 2.3.5 gives a formula for $\lambda(n,T/m^iT) - \lambda(n,T^*[m^i])$ in which the first two terms are zero by Lemma 3.5.2, and the others are linear in i by Lemma 1.1.5 and hypothesis (H.6). Therefore $\lambda(n,T/m^iT) - \lambda(n,T^*[m^i])$ has the desired form, and the theorem follows. □

The next lemma is an application of the Global Duality Theorem 2.3.4, and is crucial in many of the calculations that follow.

LEMMA 4.1.6. *Suppose ℓ is prime and $n\ell \in \mathcal{N}$. We have the following diagrams of inclusions, in which the labels on the arrows are the lengths of the corresponding cyclic cokernels.*



These lengths satisfy

(i) $0 \le a, b, c, d, a^*, b^*, c^*, d^* \le k$,

(ii) $a + c = b + d$, $a^* + c^* = b^* + d^*$,
(iii) $a + a^* = b + b^* = c + c^* = d + d^* = k$,
(iv) $a \geq d$, $b \geq c$, $c^* \geq b^*$, $d^* \geq a^*$.

PROOF. By definition

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) = \ker[H^1_{\mathcal{F}^\ell(n)}(\mathbf{Q}, T) \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)],$$
$$H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T) = \ker[H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)],$$

etc. The two diagrams come from the definitions in this way. Since $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$, and $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T^*)$ are all free of rank one over R by Lemma 3.5.6(ii), the inequalities (i) hold. The equalities (ii) are immediate from the diagrams.

The equality $a + a^* = k$ follows from the Global Duality Theorem 2.3.4 with $\mathcal{G}_1 = \mathcal{F}(n)$ and $\mathcal{G}_2 = \mathcal{F}^\ell(n)$, and similarly for the other three equalities of (iii). Finally, by definition $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \cap H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T) = H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T)$. The first two inequalities of (iv) follow from this, and the other two similarly with $(T, \mathcal{F})$ replaced by $(T^*, \mathcal{F}^*)$. □

LEMMA 4.1.7. *Suppose $n\ell \in \mathcal{N}$ with ℓ prime.*

(i) $|\lambda(n\ell, T) - \lambda(n, T)| \leq k$ *and* $|\lambda(n\ell, T^*) - \lambda(n, T^*)| \leq k$.
(ii) *If the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ is surjective, then*

$$H^1_{\mathcal{F}(n\ell)^*}(\mathbf{Q}, T^*) = H^1_{\mathcal{F}^\ell(n)^*}(\mathbf{Q}, T^*) \subset H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*).$$

(iii) *The image of the composition*

$$\mathfrak{m}^{\lambda(n,T^*)} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T) \xrightarrow{\phi^{\mathrm{fs}}_\ell} H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$$

is equal to the image of $\mathfrak{m}^{\lambda(n\ell,T^*)} H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T) \xrightarrow{\mathrm{loc}_\ell} H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$.

(iv) *If both localization maps*

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T), \qquad H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$$

are nonzero, then $\lambda(n\ell, \bar{T}) = \lambda(n, \bar{T}) - 1$ and $\lambda(n\ell, \bar{T}^*) = \lambda(n, \bar{T}^*) - 1$.

PROOF. Consider the diagrams of Lemma 4.1.6. Assertion (i) is immediate. Recall (Lemma 3.5.6(ii)) that $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$, and $H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T^*)$ are free of rank one over R, and ϕ^{fs}_ℓ is an isomorphism.

If the localization map in (ii) is surjective, then $c = k$ in the left-hand diagram of Lemma 4.1.6. Therefore by (iii) and (iv) of that lemma, $b^* = 0$, which proves (ii).

To prove (iii) it is enough to show that $\mathrm{length}(C_n) = \mathrm{length}(C_{n\ell})$ where C_n and $C_{n\ell}$ are the images of $\mathfrak{m}^{\lambda(n,T^*)} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$ and $\mathfrak{m}^{\lambda(n\ell,T^*)} H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T)$, respectively, under localization at ℓ. The left-hand diagram of Lemma 4.1.6 shows that

$$\mathrm{length}(C_n) = \max\{0, c - \lambda(n, T^*)\}, \qquad \mathrm{length}(C_{n\ell}) = \max\{0, d - \lambda(n\ell, T^*)\}.$$

The right-hand diagram shows that

$$\lambda(n, T^*) - \lambda(n\ell, T^*) = d^* - c^* = c - d,$$

so $\mathrm{length}(C_n) = \mathrm{length}(C_{n\ell})$.

For (iv), if the localization maps in question are nonzero, then using Lemma 4.1.1 we see that the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T}), \quad H^1_{\mathcal{F}(n)^*}(\mathbf{Q},\bar{T}^*) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T}^*)$$

are surjective. By (ii) we have $\lambda(n\ell,\bar{T}^*) = \lambda(n,\bar{T}^*)-1$, and so by Proposition 4.1.4 $\lambda(n\ell,\bar{T}) = \lambda(n,\bar{T}) - 1$. □

Definition 4.1.8. If $m \in \mathcal{N}$ and either $\lambda(m,T) = 0$ or $\lambda(m,T^*) = 0$, we say that m is a *core* vertex (of the graph $\mathcal{X}$ of Definition 3.1.2). By Proposition 4.1.3, this definition is unchanged if we replace T by $\bar{T}$.

Recall that $\nu(n)$ denote the number of prime divisors of $n \in \mathbf{Z}^+$.

Corollary 4.1.9. *Let* $r = \min\{\dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T}), \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q},\bar{T}^*)\}$ *and* $j \geq k$.

(i) *If* n *is a core vertex then* $\nu(n) \geq r$.
(ii) *There are core vertices* $n \in \mathcal{N}_j$ *with* $\nu(n) = r$.
(iii) *For every* $m \in \mathcal{N}_j$ *there are core vertices* $n \in \mathcal{N}_j$ *divisible by* m.

Proof. The first assertion follows from Lemma 4.1.7(i).

Suppose $m \in \mathcal{N}_j$ is not a core vertex, so $\lambda(m,\bar{T}) > 0$ and $\lambda(m,\bar{T}^*) > 0$. It follows easily from Proposition 3.6.1 and Lemma 4.1.7(iv) that there is an $\ell \in \mathcal{P}_j$ such that $\lambda(m\ell,\bar{T}) = \lambda(m,\bar{T}) - 1$ and $\lambda(m\ell,\bar{T}^*) = \lambda(m,\bar{T}^*) - 1$. Proceeding inductively, after r steps we reach an multiple $n \in \mathcal{N}_j$ of m satisfying $\nu(n) = \nu(m) + r$ and $\lambda(n,\bar{T})\lambda(n,\bar{T}^*) = 0$.

This argument proves (iii), and when $m = 1$ it proves (ii). □

Theorem 4.1.10. *Suppose that* $n \in \mathcal{N}$ *is a core vertex. Then* $H^1_{\mathcal{F}(n)}(\mathbf{Q},T)$ *and* $H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*)$ *are free* R*-modules. The ranks of these modules are independent of the choice of core vertex* n*, and one of them is zero.*

Proof. This is immediate from Theorem 4.1.5. □

Definition 4.1.11. The *core Selmer rank* of T is the rank of the free R-module $H^1_{\mathcal{F}(n)}(\mathbf{Q},T)$ for any core vertex n. We will denote the core rank of T by $\chi(T)$. Similarly we define $\chi(T^*) = \mathrm{rank}_R(H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*))$ for any core vertex n. By Theorem 4.1.10 these nonnegative integers are well-defined, independent of the choice of n, and one of them is zero.

Example 4.1.12. Suppose that R is a quotient of a discrete valuation ring D, and $T = T_0 \otimes R$ where T_0 is a free D-module of finite rank with a continuous action of $G_{\mathbf{Q}}$, unramified outside a finite set of primes. Then the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T induced from T_0 (Definition 3.2.1) satisfies (H.6) by Lemma 3.7.1. We will show in Theorem 5.2.15 below that

$$\chi(T,\mathcal{F}_{\mathrm{can}}) = \mathrm{rank}_D T_0^- + \mathrm{corank}_D H^0(\mathbf{Q}_p,T_0^*)$$

where T_0^- denotes the submodule of T_0 on which (some fixed) complex conjugation acts by -1.

See §6.1 and §6.2, especially Propositions 6.1.6 and 6.2.2, for important examples with $\chi(T) = 1$.

Theorem 4.1.13. (i) *If* $\chi(T) > 0$ *then* $\chi(T^*) = 0$ *and for every* $i \geq 0$ *and every* $n \in \mathcal{N}$,

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},T/\mathfrak{m}^iT) \cong (R/\mathfrak{m}^i)^{\chi(T)} \oplus H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*[\mathfrak{m}^i])$$

(ii) *If $\chi(T) = 0$ then for every $i \geq 0$ and every $n \in \mathcal{N}$,*

$$H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*[\mathfrak{m}^i]) \cong (R/\mathfrak{m}^i)^{\chi(T^*)} \oplus H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/\mathfrak{m}^i T).$$

PROOF. Taking n to be a core vertex shows that $r = \chi(T^*)$ and $s = \chi(T)$ in Theorem 4.1.5, so for $i \geq k$ the theorem is immediate from Theorem 4.1.5. Taking the $\mathfrak{m}^i$-torsion and applying Lemma 4.1.1 proves the theorem for arbitrary i. □

COROLLARY 4.1.14. *If $\chi(T) > 0$ then for every $n \in \mathcal{N}$*

$$\lambda(n, T) - \lambda(n, T^*) = k\chi(T).$$

If $\chi(T) = 0$ then for every $n \in \mathcal{N}$

$$\lambda(n, T) - \lambda(n, T^*) = -k\chi(T^*).$$

PROOF. This follows immediately from Theorem 4.1.13. □

DEFINITION 4.1.15. Suppose $\chi(T) > 0$, so $\chi(T^*) = 0$. If $\nu(n)$ is less than $\dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*)$ then Lemma 4.1.7(i) (applied to $\bar{T}$) shows that $\lambda(n, \bar{T}^*) > 0$, and hence n is not a core vertex. On the other hand, Corollary 4.1.9(ii) shows that there exist core vertices n with $\nu(n) = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*)$; we will call such an n a *leading vertex*.

Note that if 1 is a core vertex (i.e., if $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) = 0$) then 1 is the only leading vertex.

THEOREM 4.1.16. *Suppose (in addition to our other standard hypotheses) that $\chi(T) > 0$, that 1 is not a core vertex, that (H.4a) holds, and that the image of $R \to \mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \mathrm{End}(T)$.*

Suppose $\mathcal{L} \subset H^1_{\mathcal{F}}(\mathbf{Q}, T)$ and $\dim_{\Bbbk}(\mathcal{L}[\mathfrak{m}]) = \chi(T)$. Then there are infinitely many leading vertices $n \in \mathcal{N}$ such that $\mathcal{L} \subset H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$.

PROOF. Let $j = \dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q}, \bar{T}) - \chi(T)$. Then by Lemma 4.1.1 and Theorem 4.1.13(i),

$$j = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*) = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[\mathfrak{m}] \geq 1$$

and

$$j = \dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q}, T)[\mathfrak{m}] - \dim_{\Bbbk}(\mathcal{L}[\mathfrak{m}]).$$

Choose homomorphisms $\phi_1, \ldots, \phi_j : H^1_{\mathcal{F}}(\mathbf{Q}, T) \to R$ such that $\cap_i \ker(\phi_i) = \mathcal{L}$ and $\psi_1, \ldots, \psi_j : H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \to R$ such that $\cap_i \ker(\psi_i) = 0$. Using Proposition 3.6.2(ii) choose primes $\ell_1, \ldots, \ell_j \in \mathcal{P}$ so that for every i,

$$\ker[\mathrm{loc}_{\ell_i} : H^1_{\mathcal{F}}(\mathbf{Q}, T) \to H^1(\mathbf{Q}_{\ell_i}, T)] = \ker(\phi_i),$$
$$\ker[\mathrm{loc}_{\ell_i} : H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \to H^1(\mathbf{Q}_{\ell_i}, T^*)] = \ker(\psi_i).$$

In particular if $n = \prod_i \ell_i$ then $\nu(n) = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*)$ and $\mathcal{L} = H^1_{\mathcal{F}_n}(\mathbf{Q}, T) \subset H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$, so we only need to show that n is a core vertex. Since Proposition 3.6.2 provides infinitely many ℓ_i with the desired properties, this will give infinitely many suitable n.

By construction we have injections

$$H^1_{\mathcal{F}}(\mathbf{Q}, \bar{T})/\mathcal{L}[\mathfrak{m}] \hookrightarrow \bigoplus_i H^1_{\mathrm{f}}(\mathbf{Q}_{\ell_i}, \bar{T}), \qquad H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*) \hookrightarrow \bigoplus_i H^1_{\mathrm{f}}(\mathbf{Q}_{\ell_i}, \bar{T}^*).$$

Applying Lemma 4.1.7(iv) inductively to $n_i = \prod_{t \leq i} \ell_t$ shows that $\lambda(n_i, \bar{T}^*) = j - i$, so $n = n_j$ is a core vertex as desired, and the proof is complete. □

REMARK 4.1.17. Theorem 4.1.16 is not true without the assumption that the image of $R \to \mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \mathrm{End}(T)$. Consider the case where $R = \Bbbk$ is a field, and $T = T_0 \otimes \Bbbk$ with an $\mathbf{F}_p[[G_{\mathbf{Q}}]]$-module T_0. Then $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*) = H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T_0^*) \otimes \Bbbk$ for every n, so only $\mathbf{F}_p$-rational subspaces $\mathcal{L}$ can occur as the stalk at a leading vertex.

4.2. Kolyvagin systems and the core rank

The existence or nonexistence of Kolyvagin systems is completely determined by the core Selmer rank. Namely,

$$\chi(T) = 0 \Rightarrow \mathbf{KS}(T) = 0,$$
$$\chi(T) = 1 \Rightarrow \mathbf{KS}(T) \text{ is free of rank one over } R,$$
$$\chi(T) > 1 \Rightarrow \mathbf{KS}(T) \text{ contains a free } R\text{-module of rank } r \text{ for every } r.$$

The first assertion is Theorem 4.2.2 below. The other two will follow using Howard's Theorem 4.3.3 and (for the second one) the other results of §4.3 and §4.4. See §4.5.

LEMMA 4.2.1. *Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ and $n \in \mathcal{N}$. If $\ell \in \mathcal{P}$ is such that*

(a) *localization at ℓ maps $\mathfrak{m}^{\lambda(n,T^*)} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$ to zero,*
(b) $\kappa_{n\ell} \in \mathfrak{m}^{\lambda(n\ell,T^*)} H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T) \otimes G_{n\ell}$,

then $(\kappa_n)_\ell = 0$.

PROOF. Let c and d be as in the left-hand diagram of Lemma 4.1.6. Then

$$\lambda(n\ell, T) = \lambda(n, T) - c + d.$$

It follows from condition (a) that $c \le \lambda(n, T^*)$, and then by Proposition 4.1.4 $d \le \lambda(n\ell, T^*)$. Thus it follows from (b) that $(\kappa_{n\ell})_\ell = 0$. Now by definition of a Kolyvagin system, we conclude that $(\kappa_n)_\ell = 0$. □

THEOREM 4.2.2. *If the core rank $\chi(T) = 0$, then $\mathbf{KS}(T) = 0$.*

PROOF. Since $\chi(T) = 0$, Theorem 4.1.13 shows that $\lambda(n, T) \le \lambda(n, T^*)$ for every $n \in \mathcal{N}$. In particular $\mathfrak{m}^{\lambda(n,T^*)} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) = 0$ for every n, so condition (a) of Lemma 4.2.1 is always satisfied.

Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T)$. We will prove that $\kappa_n = 0$ for every $n \in \mathcal{N}$ by induction on $\lambda(n, \bar{T})$. If $\lambda(n, \bar{T}) = 0$ then $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) = 0$ by Proposition 4.1.3, and there is nothing to prove.

Choose $n \in \mathcal{N}$ with $\lambda(n, \bar{T}) > 0$, and suppose that $\kappa_n \ne 0$. Since $\chi(T) = 0$, Theorem 4.1.13 shows that $\lambda(n, \bar{T}^*) > 0$ as well. Therefore we can use Proposition 3.6.1 to choose a prime ℓ satisfying

(a) $(\kappa_n)_\ell \ne 0$,
(b) the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T), \quad H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$$

are both nonzero.

It follows from (b) and Lemma 4.1.7(iv) that $\lambda(n\ell, \bar{T}) < \lambda(n, \bar{T})$. Hence our induction hypothesis applies, and so $\kappa_{n\ell} = 0$. In particular we can apply Lemma 4.2.1 to conclude that $(\kappa_n)_\ell = 0$, which contradicts (a). Hence $\kappa_n = 0$. □

4.3. The sheaf of stub Selmer modules

We define a subsheaf of the Selmer sheaf $\mathcal{H} = \mathcal{H}_T = \mathcal{H}_{(T,\mathcal{F},\mathcal{P})}$ of Definition 3.1.2 as follows.

DEFINITION 4.3.1. The *sheaf of stub Selmer modules* $\mathcal{H}' = \mathcal{H}'_{(T,\mathcal{F},\mathcal{P})} \subset \mathcal{H}_T$ is the subsheaf of $\mathcal{H}$ defined by

- $\mathcal{H}'(n) = \mathfrak{m}^{\lambda(n,T^*)}\mathcal{H}(n) = \mathfrak{m}^{\lambda(n,T^*)}H^1_{\mathcal{F}(n)}(\mathbf{Q},T)\otimes G_n \subset \mathcal{H}(n)$ if $n \in \mathcal{N}$,
- $\mathcal{H}'(e)$ is the image of $\mathcal{H}'(n)$ in $\mathcal{H}(e) = H^1_{\mathrm{s}}(\mathbf{Q}_\ell,T)\otimes G_{n\ell}$ under the vertex-to-edge map of $\mathcal{H}$, if e is an edge joining n and $n\ell$,

and the vertex-to-edge maps are the restrictions of those of the sheaf $\mathcal{H}$:

- $\mathcal{H}'(n) \to \mathcal{H}'(e)$ is localization at ℓ followed by ϕ^{fs}_ℓ,
- $\mathcal{H}'(n\ell) \to \mathcal{H}'(e)$ is localization at ℓ.

The latter map is well-defined (its image lies in $\mathcal{H}'(e)$), and both maps are surjective, by Lemma 4.1.7(iii).

Clearly we have $\Gamma(\mathcal{H}') \subset \Gamma(\mathcal{H})$.

LEMMA 4.3.2. *Suppose $n \in \mathcal{N}$. Then $\mathcal{H}'(n) = 0$ if $\lambda(n,T^*) \geq k$, and otherwise $\mathcal{H}'(n)$ is free of rank $\chi(T)$ over $R/\mathfrak{m}^{k-\lambda(n,T^*)}$. If $x \in \mathcal{H}'(n)$ then $x \in \mathfrak{m}^{k-\mathrm{length}(Rx)}\mathcal{H}(n)$.*

PROOF. This is immediate from Theorem 4.1.13. □

The following theorem is due to Benjamin Howard. The authors thank him for including his proof as Appendix B of this paper.

THEOREM 4.3.3 (Howard).

(i) *For every n the map $\Gamma(\mathcal{H}') \to \mathcal{H}'(n)$ is surjective.*
(ii) *If $\chi(T) = 1$, then $\Gamma(\mathcal{H}')$ has a free R-submodule of rank one.*
(iii) *If $\chi(T) > 1$, then for every d, $\Gamma(\mathcal{H}')$ has a free R-submodule of rank d.*

THEOREM 4.3.4. *Suppose $\chi(T) = 1$. Then the sheaf $\mathcal{H}'$ is locally cyclic and connected, and every $n \in \mathcal{N}$ with $\lambda(n,T^*) = 0$ is a hub.*

Before proving Theorem 4.3.4 we give the following corollary.

COROLLARY 4.3.5. *Suppose that $\chi(T) = 1$. Then the locally cyclic sheaf $\mathcal{H}'$ has trivial monodromy, and $\Gamma(\mathcal{H}')$ is free of rank one over R.*

PROOF. Fix n so that $\lambda(n,T^*) = 0$. Using Theorem 4.1.13(i) we see that

$$\mathcal{H}'(n) \cong H^1_{\mathcal{F}(n)}(\mathbf{Q},T) \cong R \oplus H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*) = R$$

is free of rank one over R. Howard's Theorem 4.3.3 shows that $\Gamma(\mathcal{H}')$ contains a free, rank-one R-submodule, so the corollary follows by Theorem 4.3.4 and Proposition 3.4.4(i). □

The rest of this section is devoted to the proof of Theorem 4.3.4. The reader may prefer to skip to the applications in the following sections.

We assume for the rest of this section that $\chi(T) = 1$. The heart of the proof is a study of the restriction of $\mathcal{H}'$ to a subgraph $\mathcal{X}^0$ defined as follows.

DEFINITION 4.3.6. Define a subgraph $\mathcal{X}^0 = \mathcal{X}^0(T, \mathcal{F}, \mathcal{P})$ of the graph $\mathcal{X} = \mathcal{X}(\mathcal{P})$ of Definition 3.1.2 as follows. The vertices of $\mathcal{X}^0$ are the core vertices of $\mathcal{X}$, the $n \in \mathcal{N}$ with $\lambda(n, \bar{T}^*) = 0$. We join n and $n\ell$ by an edge in $\mathcal{X}^0$ if and only if the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T})$ is nonzero (equivalently, is an isomorphism).

Now define the sheaf $\mathcal{H}^0$ on $\mathcal{X}^0$ to be the restriction of the Selmer sheaf $\mathcal{H}$ of Definition 3.1.2 to $\mathcal{X}^0$. Then $\mathcal{H}^0$ is also the restriction of the stub Selmer sheaf $\mathcal{H}'$ to $\mathcal{X}^0$, since the vertices of $\mathcal{X}^0$ are precisely those n for which $\mathcal{H}'(n) = \mathcal{H}(n)$, and the edges are those e for which $\mathcal{H}'(e) = \mathcal{H}(e)$.

LEMMA 4.3.7. *The sheaf $\mathcal{H}^0$ is locally free of rank one.*

PROOF. By Proposition4.1.3, if n is a vertex of $\mathcal{X}^0$ then $\lambda(n, T^*) = 0$ so by Lemma 4.3.2, $\mathcal{H}^0(n)$ is free of rank one.

Suppose e is an edge joining n and $n\ell$ in $\mathcal{X}^0$. As usual we have $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) = H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}]$ and $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T}) = H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)[\mathfrak{m}]$, and $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$, $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ are both free of rank one, so the nontriviality of $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T})$ implies that $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ is an isomorphism. Now by Lemmas 4.1.7(iii) and 3.5.6(ii) the maps from $\mathcal{H}^0(n)$ and $\mathcal{H}^0(n\ell)$ to $\mathcal{H}^0(e)$ are both isomorphisms. □

The key to the proof of Theorem 4.3.4 is the fact that the graph $\mathcal{X}^0$ is connected (Theorem 4.3.12 below). Since $\mathcal{X}^0$ was defined in terms of $\bar{T}$, we can work with $\bar{T}$ and $\Bbbk$ instead of T and R.

LEMMA 4.3.8. *Suppose n and $n\ell$ are vertices of $\mathcal{X}^0$. The following are equivalent.*

(i) *There is an edge of $\mathcal{X}^0$ joining n and $n\ell$.*
(ii) *The localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T})$ is nonzero.*
(iii) *The localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T})$ is an isomorphism.*
(iv) *The localization map $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, \bar{T})$ is nonzero.*
(v) *The localization map $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, \bar{T})$ is an isomorphism.*
(vi) $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \neq H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T})$.

PROOF. By the various definitions (i) is equivalent to (ii), (ii) is equivalent to the assertion $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \not\subset H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T})$, and (iv) is equivalent to the assertion $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T}) \not\subset H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T})$. Since (using Lemma 3.5.6(ii))

$$\dim_{\Bbbk} H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) = \dim_{\Bbbk} H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T}) = \dim_{\Bbbk} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T}) = \dim_{\Bbbk} H^1_{\mathrm{s}}(\mathbf{Q}_\ell, \bar{T}) = 1,$$

the remaining equivalences follow. □

LEMMA 4.3.9. *Suppose n and $n\ell$ are vertices of the graph $\mathcal{X}^0$. Then there is a path in $\mathcal{X}^0$ from n to $n\ell$.*

PROOF. If n and $n\ell$ are connected by an edge there is nothing to prove. So suppose not, i.e., the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T})$ is zero. Then by Lemma 4.3.8 we have $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) = H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, \bar{T})$.

Further, in the diagrams of Lemma 4.1.6 we have $c = 0$, so $c^* = 1$. By definition of $\mathcal{X}^0$ we have $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, \bar{T}^*) = 0$, so we deduce that $\dim_{\Bbbk} H^1_{\mathcal{F}_\ell(n)^*}(\mathbf{Q}, \bar{T}^*) = 1$.

Now applying Proposition 3.6.1 we can choose (using (H.5)) a prime $q \in \mathcal{P}$, prime to $n\ell$, such that the localization maps

(a) $H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}(n\ell)}(\mathbf{Q},\bar{T}) \xrightarrow{\sim} H^1_{\mathrm{f}}(\mathbf{Q}_q,\bar{T})$,
(b) $H^1_{\mathcal{F}_\ell(n)^*}(\mathbf{Q},\bar{T}^*) \xrightarrow{\sim} H^1_{\mathrm{f}}(\mathbf{Q}_q,\bar{T}^*)$

are both isomorphisms. By Lemma 4.1.7(ii) it follows from (a) that nq and $n\ell q$ are both vertices of $\mathcal{X}^0$, and there is an edge from n to nq and from $n\ell$ to $n\ell q$.

By (b) we have $H^1_{\mathcal{F}^q_\ell(n)^*}(\mathbf{Q},\bar{T}^*) = 0$, so applying Theorem 2.3.4 with $\mathcal{G}_1 = \mathcal{F}^q_\ell(n)$ and $\mathcal{G}_2 = \mathcal{F}^q(n)$ shows that the localization map $H^1_{\mathcal{F}^q(n)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T})$ is nonzero. From the left-hand diagram of Lemma 4.1.6 (with ℓ replaced by q), using that $H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \neq H^1_{\mathcal{F}(nq)}(\mathbf{Q},\bar{T})$ by Lemma 4.3.8, we see that $H^1_{\mathcal{F}^q(n)}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \oplus H^1_{\mathcal{F}(nq)}(\mathbf{Q},\bar{T})$. Since the image of $H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T})$ in $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T})$ is zero, we conclude that the image of $H^1_{\mathcal{F}(nq)}(\mathbf{Q},\bar{T})$ in $H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T})$ is nonzero. Therefore there is an edge in $\mathcal{X}^0$ joining nq to $n\ell q$, and so there is a path $(n, nq, n\ell q, n\ell)$ in $\mathcal{X}^0$ from n to $n\ell$. □

PROPOSITION 4.3.10. *Suppose n is a vertex of $\mathcal{X}^0$ and $\nu(n) \geq \dim_{\mathbb{k}} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T})$. Then there is a vertex m of $\mathcal{X}^0$ with $\nu(m) < \nu(n)$ such that there is a path in $\mathcal{X}^0$ from n to m.*

PROOF. We consider two cases.

Case 1: for some ℓ dividing n, the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \to H^1(\mathbf{Q}_\ell,\bar{T})$ is nonzero. In the left-hand diagram of Lemma 4.1.6 applied to n/ℓ and ℓ, we have $d = 1$. Since $\lambda(n/\ell,\bar{T}) \geq \chi(\bar{T}) = \lambda(n,\bar{T})$, we conclude that n/ℓ is a vertex of $\mathcal{X}^0$. By Lemma 4.3.8 there is an edge of $\mathcal{X}^0$ joining n and n/ℓ.

Case 2: for every ℓ dividing n, the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \to H^1(\mathbf{Q}_\ell,\bar{T})$ is zero. Then

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}_n}(\mathbf{Q},\bar{T}) = \bigcap_{\ell|n} H^1_{\mathcal{F}_\ell}(\mathbf{Q},\bar{T}).$$

Since this intersection of at least $\dim_{\mathbb{k}} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T})$ subspaces of $H^1_{\mathcal{F}}(\mathbf{Q},\bar{T})$ is nonempty, there is a proper divisor g of n, say $g = n/q$ for some prime q, such that $H^1_{\mathcal{F}_n}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}_g}(\mathbf{Q},\bar{T})$.

If $\lambda(g,\bar{T}) = 1$ then by Lemma 4.3.9 there is a path from n to g, and again we are done. So we may assume that $\lambda(g,\bar{T}) > 1$. By Lemma 4.1.7(i), $\lambda(g,\bar{T}) = 2$, so by Corollary 4.1.14 we have $H^1_{\mathcal{F}(g)^*}(\mathbf{Q},\bar{T}^*) \neq 0$.

Choose nonzero elements $c \in H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \subset H^1_{\mathcal{F}(g)}(\mathbf{Q},\bar{T})$, $d \in H^1_{\mathcal{F}(g)^*}(\mathbf{Q},\bar{T}^*)$, and apply Proposition 3.6.1 to get a prime $\ell \in \mathcal{P}$, prime to n, such that $c_\ell \neq 0$ and $d_\ell \neq 0$.

By Lemma 4.1.7(iv) we have $\lambda(g\ell,\bar{T}) = 1$, so $g\ell$ is a vertex of $\mathcal{X}^0$. From the left-hand diagram of Lemma 4.1.6 it follows that $H^1_{\mathcal{F}(g\ell)}(\mathbf{Q},\bar{T}) \subset H^1_{\mathcal{F}(g)}(\mathbf{Q},\bar{T})$, and hence

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) = \ker[H^1_{\mathcal{F}(g)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_q,\bar{T})],$$
$$H^1_{\mathcal{F}(g\ell)}(\mathbf{Q},\bar{T}) = \ker[H^1_{\mathcal{F}(g)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T})].$$

Since the class c belongs to the first kernel but not the second, these two kernels are different; since both are one-dimensional, they are disjoint. It follows that the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,\bar{T}), \quad H^1_{\mathcal{F}(g\ell)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_q,\bar{T})$$

are both nonzero, so by Lemmas 4.1.7(ii) and 4.3.8, $n\ell$ is a vertex of $\mathcal{X}^0$ and there are edges joining n to $n\ell$ and $g\ell$ to $n\ell$.

Finally, we claim that there is a prime r dividing $g\ell$ such that the localization map $H^1_{\mathcal{F}(g\ell)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{s}}(\mathbf{Q}_r,\bar{T})$ is nonzero. If not, then

$$H^1_{\mathcal{F}(g\ell)}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}_{g\ell}}(\mathbf{Q},\bar{T}) \subset H^1_{\mathcal{F}_n}(\mathbf{Q},\bar{T}) = H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T})$$

which we have seen is not the case. Thus by Case 1 there is an edge connecting $g\ell$ and $g\ell/r$, and so the path $(n, n\ell, g\ell, g\ell/r)$ satisfies the proposition. □

Proposition 4.3.11. *Suppose that n and m are vertices of $\mathcal{X}^0$ and $\nu(n) = \nu(m) = \dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T}) - 1$. Then there is a path in $\mathcal{X}^0$ from n to m.*

Proof. We will prove this by induction on $\dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T}) - \nu(\gcd(n,m))$. This quantity is always at least one, and when it is equal to one we have $n = m$ and there is nothing to prove.

Suppose $n \neq m$, and fix distinct primes $q \mid n$ and $r \mid m$. Applying Lemma 4.1.7(i) repeatedly we conclude that $\lambda(n/q,\bar{T}) = \lambda(m/r,\bar{T}) = 2$. As in the proof of Proposition 4.3.10 it follows that

$$\begin{aligned} H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T}) &= \ker[H^1_{\mathcal{F}(n/q)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_q,\bar{T})], \\ H^1_{\mathcal{F}(m)}(\mathbf{Q},\bar{T}) &= \ker[H^1_{\mathcal{F}(m/r)}(\mathbf{Q},\bar{T}) \to H^1_{\mathrm{f}}(\mathbf{Q}_r,\bar{T})], \\ \dim_{\Bbbk} H^1_{\mathcal{F}(n/q)^*}(\mathbf{Q},\bar{T}^*) &= \dim_{\Bbbk} H^1_{\mathcal{F}(m/r)^*}(\mathbf{Q},\bar{T}^*) = 1. \end{aligned}$$

Choose nonzero elements $c \in H^1_{\mathcal{F}(n)}(\mathbf{Q},\bar{T})$, $c' \in H^1_{\mathcal{F}(m)}(\mathbf{Q},\bar{T})$, $d \in H^1_{\mathcal{F}(n/q)^*}(\mathbf{Q},\bar{T}^*)$, and $d' \in H^1_{\mathcal{F}(m/r)^*}(\mathbf{Q},\bar{T}^*)$. By Proposition 3.6.1 we can find a prime $\ell \in \mathcal{P}$, prime to nm, such that $c_\ell, c'_\ell, d_\ell, d'_\ell$ are all nonzero.

Exactly as in the proof of Proposition 4.3.10, it follows that

- $\lambda(n\ell/q,\bar{T}) = \lambda(n\ell,\bar{T}) = 1$ and there are edges in $\mathcal{X}^0$ connecting n to $n\ell$ and $n\ell/q$ to $n\ell$,
- $\lambda(m\ell/r,\bar{T}) = \lambda(m\ell,\bar{T}) = 1$ and there are edges in $\mathcal{X}^0$ connecting m to $m\ell$ and $m\ell/r$ to $m\ell$.

We have $\nu(\gcd(n\ell/q, m\ell/r)) = \nu(\gcd(n,m)) + 1$, so our induction hypothesis shows that there is a path in $\mathcal{X}^0$ connecting $n\ell/q$ and $m\ell/r$. Therefore there is a path $(n, n\ell, n\ell/q, \cdots, m\ell/r, m\ell, m)$ connecting n and m. □

Theorem 4.3.12. *The graph $\mathcal{X}^0$ is connected.*

Proof. Suppose n and m are vertices of $\mathcal{X}^0$. By Lemma 4.1.7(i), we must have $\nu(n), \nu(m) \geq \dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T}) - 1$. Applying Proposition 4.3.10 inductively we can find paths connecting n to a vertex n' and m to a vertex m' with $\nu(n') = \nu(m') = \dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q},\bar{T}) - 1$. By Proposition 4.3.11 there is a path from n' to m', and the proof is complete. □

Proof of Theorem 4.3.4. Since $\chi(T) = 1$, Lemma 4.3.2 shows that the stalks of $\mathcal{H}'$ are cyclic. If e is an edge joining vertices n and $n\ell$, then the vertex-to-edge map $\mathcal{H}'(n) \to \mathcal{H}'(e)$ is surjective by definition, and then $\mathcal{H}'(n\ell) \to \mathcal{H}'(e)$ is surjective by Lemma 4.1.7(iii).

It remains to show that if $n \in \mathcal{N}$ and $\lambda(n,T^*) = 0$, then n is a hub of $\mathcal{H}'$. Fix such a vertex n, and let m be any other vertex. We will show by induction on $\lambda(m,\bar{T}^*)$ that there is a surjective path from n to m.

Note that n is a vertex of $\mathcal{X}^0$. If $\lambda(m,\bar{T}^*)=0$ then m is also a vertex of $\mathcal{X}^0$, and so there is a path in $\mathcal{X}^0$ from n to m. Every path in $\mathcal{X}^0$ is a surjective path (because all vertex-to-edge maps in $\mathcal{X}^0$ are isomorphisms by Lemma 4.3.7), so there is an $\mathcal{H}'$-surjective path from n to m.

Now suppose $\lambda(m,\bar{T}^*)>0$. Using Proposition 3.6.1, choose a prime $\ell\in\mathcal{P}$ such that the localization maps

$$\mathfrak{m}^{k-1}H^1_{\mathcal{F}(m)}(\mathbf{Q},T)\to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T),\quad H^1_{\mathcal{F}(m)^*}(\mathbf{Q},T^*)[\mathfrak{m}]\to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T^*)$$

are both nonzero. (Note that $\mathfrak{m}^{k-1}H^1_{\mathcal{F}(n)}(\mathbf{Q},T)\neq 0$ by Theorem 4.1.13.) Then by Lemma 4.1.7(iv), $\lambda(m\ell,\bar{T}^*)<\lambda(m,\bar{T}^*)$, so by our induction hypothesis there is an $\mathcal{H}'$-surjective path from n to $m\ell$. Further we see that localization $H^1_{\mathcal{F}(m)}(\mathbf{Q},T)\to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T)$ is surjective, so $\mathfrak{m}^{\lambda(m,T^*)}H^1_{\mathcal{F}(m)}(\mathbf{Q},T)\to\mathfrak{m}^{\lambda(m,T^*)}H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T)$ is surjective as well. These two modules are both cyclic of length $\max\{0,k-\lambda(m,T^*)\}$, so if e is the edge joining m and $m\ell$, we conclude that the map $\mathcal{H}'(m)\to\mathcal{H}'(e)$ is an isomorphism. Therefore the path from $m\ell$ to m is a surjective path, so by composition we obtain a surjective path from n to m. This concludes the proof. □

4.4. Kolyvagin systems and the stub Selmer sheaf

In this section we show that under fairly general hypotheses, a Kolyvagin system, a priori a global section of the Selmer sheaf $\mathcal{H}$, is actually a global section of the subsheaf $\mathcal{H}'$. This is the content of Theorems 4.4.1 and 4.4.3. These results play a central role in the rest of the paper. As an immediate consequence we obtain (Corollary 4.4.5) the Kolyvagin upper bound for the Selmer group $H^1_{\mathcal{F}^*}(\mathbf{Q},T^*)$ in terms of a Kolyvagin system $\boldsymbol{\kappa}\in\mathbf{KS}(T)$ (compare with, for example, Theorem 2.2.2 of [**Ru6**]).

THEOREM 4.4.1. *Suppose that (at least) one of the following three conditions is satisfied.*

- $\chi(T)=1$,
- $k=1$, *i.e., R is a field, or*
- (H.4a) *holds, and the image of $R\to\mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]]\to\mathrm{End}(T)$.*

Then the inclusion $\Gamma(\mathcal{H}')\subset\Gamma(\mathcal{H})$ is an isomorphism. In other words, for every $\boldsymbol{\kappa}\in\mathbf{KS}(T)$ and $n\in\mathcal{N}$ we have $\kappa_n\in\mathcal{H}'(n)$.

PROOF. Fix a $\boldsymbol{\kappa}\in\mathbf{KS}(T)$. We treat the three hypotheses separately, but in each case we will show by induction on $\lambda(n,\bar{T}^*)$ that $\kappa_n\in\mathcal{H}'(n)$ for every $n\in\mathcal{N}$. If $\lambda(n,\bar{T}^*)=0$ we have $\lambda(n,T^*)=0$ (Proposition 4.1.3) so $\mathcal{H}'(n)=\mathcal{H}(n)$ and there is nothing to prove.

Case 1: $k=1$. Suppose $\lambda(n,\bar{T}^*)>0$. In this case $\mathcal{H}'(n)=\mathfrak{m}^{\lambda(n,T^*)}\mathcal{H}(n)=0$, so we need to show $\kappa_n=0$. If $\kappa_n\neq 0$, then using Proposition 3.6.1 we can fix a prime $\ell\in\mathcal{P}$ not dividing n such that

(a) $(\kappa_n)_\ell\neq 0$,
(b) the localization map $H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T^*)\to H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T^*)$ is nonzero.

It follows from (a), (b) and Lemma 4.1.7(iv) that $\lambda(n\ell,\bar{T}^*)<\lambda(n,\bar{T}^*)$, so our induction hypothesis shows that $\kappa_{n\ell}\in\mathcal{H}'(n\ell)$. Thus by Lemma 4.2.1 we conclude that $(\kappa_n)_\ell=0$. But this contradicts (a), so we must have $\kappa_n=0$.

Case 2: (H.4a) holds, and the image of $R \to \mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \mathrm{End}(T)$. By Theorem 4.2.2 we may assume that $\chi(T) > 0$. Suppose that $\lambda(n, \bar{T}^*) > 0$.

Since $\chi(T) > 0$, it follows from Theorem 4.1.13 that

$$\mathcal{H}(n)[\mathfrak{m}] \not\subset \mathcal{H}'(n).$$

If $\kappa_n \notin \mathcal{H}'(n)$ we can find a homomorphism $\phi : \mathcal{H}(n) \to R$ such that

$$\phi(\mathcal{H}'(n)) = 0, \quad \phi(\mathcal{H}(n)[\mathfrak{m}]) \neq 0, \quad \phi(\kappa_n) \neq 0.$$

Hence by Proposition 3.6.2(ii) we can fix a prime $\ell \in \mathcal{P}$, prime to n, such that

(a) the localization map $\mathfrak{m}^{\lambda(n,T^*)} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ is zero,
(b) $(\kappa_n)_\ell \neq 0$,
(c) the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T), \quad H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$$

are both nonzero.

By (c) and Lemma 4.1.7(iv), we have $\lambda(n\ell, \bar{T}^*) < \lambda(n, \bar{T}^*)$, so by our induction hypothesis we have $\kappa_{n\ell} \in \mathcal{H}'(n\ell)$. Therefore by Lemma 4.2.1, $(\kappa_n)_\ell = 0$, which contradicts condition (b). This contradiction shows that $\kappa_n \in \mathcal{H}'(n)$.

Case 3: $\chi(T) = 1$. Choose a core vertex m. By Howard's Theorem 4.3.3(i) there is a section $\boldsymbol{\kappa}' \in \Gamma(\mathcal{H}')$ such that $\kappa'(m) = \kappa(m)$. Let $\bar{\boldsymbol{\kappa}} = \boldsymbol{\kappa} - \boldsymbol{\kappa}' \in \mathbf{KS}(T)$, so $\bar{\kappa}_m = 0$. We will show that $\bar{\boldsymbol{\kappa}} = 0$.

Let $\mathcal{X}^0$ be the subgraph of $\mathcal{X}$ of Definition 4.3.6, whose vertices are the core vertices of $\mathcal{X}$, and $\mathcal{H}^0$ the restriction of $\mathcal{H}$ to $\mathcal{X}^0$. By Theorem 4.3.12 and Lemma 4.3.7, $\mathcal{X}^0$ is connected and $\mathcal{H}^0$ is locally free of rank one. Since $\bar{\kappa}_m = 0$ at the vertex m of $\mathcal{X}^0$, the restriction of $\bar{\kappa}$ to $\mathcal{X}^0$ must be identically zero (Proposition 3.4.4(i)). In other words, $\bar{\kappa}_n = 0$ for every core vertex n.

Now let $n \in \mathcal{N}$ be any vertex of $\mathcal{X}$. We will show by induction on $\lambda(n, \bar{T}^*)$ that $\bar{\kappa}_n = 0$. We have already dealt with the case of core vertices, $\lambda(n, \bar{T}^*) = 0$.

Suppose now that $\lambda(n, \bar{T}^*) > 0$, and suppose $\bar{\kappa}_n \neq 0$. Using Proposition 3.6.1, choose a prime $\ell \in \mathcal{P}$, prime to n, such that

(a) $(\bar{\kappa}_n)_\ell \neq 0$,
(b) the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T), \quad H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$$

are both nonzero.

By (b) and Lemma 4.1.7(iv), we have $\lambda(n\ell, \bar{T}^*) < \lambda(n, \bar{T}^*)$, so by our induction hypothesis we have $\bar{\kappa}_{n\ell} = 0$. But by (a) and the definition of a Kolyvagin system, we must have $(\bar{\kappa}_{n\ell})_{\ell,\mathrm{s}} \neq 0$. This contradiction shows that $\bar{\kappa}_n = 0$, and so $\kappa_n = \kappa'_n \in \mathcal{H}'(n)$. □

Definition 4.4.2. Suppose $\tilde{R}$ is a complete noetherian local ring such that R is a quotient of $\tilde{R}$. We say that $(\tilde{T}, \tilde{\mathcal{F}}, \mathcal{P})$ is a lifting of $(T, \mathcal{F}, \mathcal{P})$ to $\tilde{R}$ if $\tilde{T}$ is an $\tilde{R}[[G_{\mathbf{Q}}]]$-module, $(\tilde{T}, \tilde{\mathcal{F}}, \mathcal{P})$ is a Selmer triple over $\tilde{R}$, $T = \tilde{T} \otimes_{\tilde{R}} R$, and $\mathcal{F} = \tilde{\mathcal{F}} \otimes_{\tilde{R}} R$.

Theorem 4.4.3. *Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is* sufficiently liftable *in the sense that there is a local principal artinian ring $\tilde{R}$ of length $\tilde{k} \geq 2k-1$ and a lifting $(\tilde{T}, \tilde{\mathcal{F}}, \mathcal{P})$ of $(T, \mathcal{F}, \mathcal{P})$ to $\tilde{R}$ such that:*

- *$(\tilde{T}, \tilde{\mathcal{F}}, \mathcal{P})$ satisfies* (H.0) *through* (H.6) *and $\mathcal{P} \subset \mathcal{P}_{\tilde{k}}$.*

- $\boldsymbol{\kappa}$ *is in the image of the natural map* $\mathbf{KS}(\tilde{T}) \to \mathbf{KS}(T)$.

Then $\boldsymbol{\kappa}$ *is a global section of the subsheaf* $\mathcal{H}'$ *of stub Selmer modules (i.e., for all* $n \in \mathcal{N}$ *we have* $\kappa_n \in \mathcal{H}'(n)$*).*

PROOF. We will prove that $\kappa_n \in \mathcal{H}'(n)$ by induction on both k and $\lambda(n, \bar{T}^*)$. The case $k = 1$ is part of Theorem 4.4.1, and if $\lambda(n, \bar{T}^*) = 0$ then $\lambda(n, T^*) = 0$ (Proposition 4.1.3) so $\mathcal{H}'(n) = \mathcal{H}(n)$ and there is nothing to prove. If $\lambda(n, \bar{T}) = 0$ then $\mathcal{H}(n) = 0$ and there is again nothing to prove, so we may suppose that $\lambda(n, \bar{T}^*)$ and $\lambda(n, \bar{T}^*)$ are both positive.

Case 1: $\lambda(n, T^*) < k$.

Let $j = \lambda(n, T^*)$. By Lemma 4.1.1(ii) we have

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

so $\lambda(n, T^*[\mathfrak{m}^j]) = \lambda(n, T^*) = \lambda(n, \tilde{T}^*) = j$.

Consider the image $\boldsymbol{\kappa}^{(j)}$ of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/\mathfrak{m}^j T)$. By our induction hypothesis applied to the $R/\mathfrak{m}^j$-module $T/\mathfrak{m}^j T$, we have

$$\kappa_n^{(j)} \in \mathfrak{m}^j H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/\mathfrak{m}^j T) \otimes G_n = 0.$$

By Lemma 4.1.1(i) (with $i = k - j$) it follows that $\kappa_n \in \mathcal{H}(n)[\mathfrak{m}^{k-j}]$.

Since $\lambda(n, \tilde{T}^*) = j \le \tilde{k} - k$, Theorem 4.1.13 and Lemma 4.1.1(i) applied to $\tilde{T}$ show that the image of $H^1_{\tilde{\mathcal{F}}(n)}(\mathbf{Q}, \tilde{T}) \otimes G_n$ in $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \otimes G_n$ is free over R. Since κ_n belongs to this image, and is killed by $\mathfrak{m}^{k-j}$, we conclude that $\kappa_n \in \mathfrak{m}^j \mathcal{H}(n) = \mathcal{H}'(n)$ as desired.

Case 2: $\lambda(n, T^*) \ge k$. In this case $\mathcal{H}'(n) = 0$, so we need to prove that $\kappa_n = 0$.

Suppose $\kappa_n \ne 0$. Using Proposition 3.6.1 we can fix a prime ℓ such that

(a) $(\kappa_n)_\ell \ne 0$,

(b) the localization maps

$$H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T), \quad H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)[\mathfrak{m}] \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*)$$

are both nonzero.

It follows from (b) and Lemma 4.1.7(iv) that $\lambda(n\ell, \bar{T}^*) < \lambda(n, \bar{T}^*)$. Thus by our induction hypothesis $\kappa_{n\ell} \in \mathcal{H}'(n\ell)$, so Lemma 4.2.1 shows that $(\kappa_n)_\ell = 0$. But this contradicts (a), so we must have $\kappa_n = 0$. □

REMARK 4.4.4. Our typical examples of "sufficiently liftable" Kolyvagin systems will arise when R is a quotient of a discrete valuation ring D, $T = T_D \otimes R$ with a $D[[G_{\mathbf{Q}}]]$-module T_D, and $\boldsymbol{\kappa}$ belongs to the image of $\mathbf{KS}(T_D) \to \mathbf{KS}(T)$.

The following corollary is the standard application of a Kolyvagin system (or Euler system): an upper bound on the size of the dual Selmer group $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$, in terms of the divisibility of κ_1 (compare with, for example, Theorem 2.2.2 of [**Ru6**]). In Theorem 4.5.6 below, we will show that under some extra hypotheses this upper bound is sharp, so we get an exact formula for the size of $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$.

COROLLARY 4.4.5. *Suppose* $\boldsymbol{\kappa} \in \mathbf{KS}(T)$. *If one of the three hypotheses of Theorem 4.4.1 holds for* T*, or if the hypothesis of Theorem 4.4.3 holds for* T *and* $\boldsymbol{\kappa}$*, then*

$$\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) \le \max\{i : \kappa_1 \in \mathfrak{m}^i H^1_{\mathcal{F}}(\mathbf{Q}, T)\}.$$

PROOF. By Theorem 4.4.1 or 4.4.3,

$$\kappa_1 \in \mathcal{H}'(1) = \mathfrak{m}^{\lambda(1,T^*)} H^1_{\mathcal{F}}(\mathbf{Q}, T) = \mathfrak{m}^{\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},T^*))} H^1_{\mathcal{F}}(\mathbf{Q}, T). \qquad \square$$

4.5. Kolyvagin systems over principal artinian rings

This section contains the main results and applications of Kolyvagin systems over principal artinian rings.

COROLLARY 4.5.1. (i) *If $\chi(T) = 0$ then $\mathbf{KS}(T) = 0$.*

(ii) *If $\chi(T) \geq 2$ then for every $d \in \mathbf{Z}^+$, $\mathbf{KS}(T)$ contains a free R-module of rank d.*

PROOF. Assertion (i) is Theorem 4.2.2, and (ii) is Theorem 4.3.3(iii). $\square$

The rest of this section will deal with the case $\chi(T) = 1$. In particular this means we can apply Theorem 4.4.1.

COROLLARY 4.5.2. *Suppose $\chi(T) = 1$.*

(i) *$\mathbf{KS}(T)$ is a free R-module of rank one.*

(ii) *Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T)$, $m \in \mathcal{N}$, and $\kappa_m \neq 0$. Let $j \geq 0$ be such that κ_m generates $\mathfrak{m}^j \mathcal{H}'(m)$. Then κ_n generates $\mathfrak{m}^j \mathcal{H}'(n)$ for every $n \in \mathcal{N}$, so in particular $\kappa_n \in \mathfrak{m}^{j+\lambda(n,T^*)} \mathcal{H}(n)$ for every n.*

(iii) *Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T)$. If $n \in \mathcal{N}$ is a core vertex then the map $\mathbf{KS}(T) \to \mathcal{H}(n)$ which maps $\boldsymbol{\kappa} \mapsto \kappa_n$ is an isomorphism.*

(iv) *If $j \geq k$ then the natural restriction map $\mathbf{KS}(T, \mathcal{P}) \to \mathbf{KS}(T, \mathcal{P} \cap \mathcal{P}_j)$ is an isomorphism.*

(v) *If $j \leq k$ then the projection map $T \to T/\mathfrak{m}^j T$ induces a surjective map $\mathbf{KS}(T) \to \mathbf{KS}(T/\mathfrak{m}^j T)$.*

PROOF. Since $\mathbf{KS}(T) = \Gamma(\mathcal{H}')$ (Theorem 4.4.1), the first three assertions of the corollary are immediate from Corollary 4.3.5, Theorem 4.3.4, and Proposition 3.4.4.

By (iii) applied to $(T, \mathcal{P})$ and to $(T, \mathcal{P} \cap \mathcal{P}_j)$, if $n \in \mathcal{N} \cap \mathcal{N}_j$ is a core vertex (such n exist by Corollary 4.1.9) then we have isomorphisms

$$\mathbf{KS}(T, \mathcal{P}) \xrightarrow{\sim} \mathcal{H}(n) \xleftarrow{\sim} \mathbf{KS}(T, \mathcal{P}_j)$$

compatible with the restriction map $\mathbf{KS}(T, \mathcal{P}) \to \mathbf{KS}(T, \mathcal{P} \cap \mathcal{P}_j)$. By (iii) applied to T and $T/\mathfrak{m}^j T$, if $n \in \mathcal{N}$ is a core vertex we get a commutative diagram with vertical isomorphisms

$$\begin{array}{ccc} \mathbf{KS}(T) & \longrightarrow & \mathbf{KS}(T/\mathfrak{m}^j T) \\ \downarrow \cong & & \downarrow \cong \\ H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \otimes G_n & \twoheadrightarrow & H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/\mathfrak{m}^j) \otimes G_n. \end{array}$$

Since n is a core vertex, Lemma 4.1.1(i) shows that bottom map is surjective. This completes the proof of the corollary. $\square$

COROLLARY 4.5.3. *If $\chi(T) = 1$ then the natural map $\mathbf{KS}(T) \to \overline{\mathbf{KS}}(T)$ (see Definition 3.1.6) is an isomorphism.*

PROOF. This is immediate from the definition of $\overline{\mathbf{KS}}(T)$ and Corollary 4.5.2. $\square$

If $\chi(T) > 2$ then the map $\mathbf{KS}(T) \to \overline{\mathbf{KS}}(T)$ need not be an isomorphism. See Example 4.5.11.

COROLLARY 4.5.4. *Suppose that $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$. Then the following are equivalent.*

(i) *There is an $n \in \mathcal{N}$ such that $\mathcal{H}'(n) \neq 0$ and κ_n generates $\mathcal{H}'(n)$.*
(ii) *κ_n generates $\mathcal{H}'(n)$ for every $n \in \mathcal{N}$.*
(iii) *The global section of $\Gamma(\mathcal{H}')$ corresponding to $\boldsymbol{\kappa}$ is primitive in the sense of Definition 3.4.5.*
(iv) *The image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(\bar{T})$ is nonzero.*

PROOF. The equivalence (i) $\iff$ (ii) is Corollary 4.5.2(ii), and (ii) $\iff$ (iii) is Definition 3.4.5.

Suppose $n \in \mathcal{N}$. By Lemma 4.1.1(i), κ_n maps to zero in $H^1(\mathbf{Q}, \bar{T})$ if and only if $\mathfrak{m}^{k-1}\kappa_n = 0$. Thus if the image of κ_n in $H^1(\mathbf{Q}, \bar{T})$ is nonzero, then κ_n must generate the free, rank-one R-module $\mathcal{H}'(n)$, so (iv) $\Rightarrow$ (i). Conversely, suppose (ii) holds and n is a core vertex of $\mathcal{X}$ (these exist by Corollary 4.1.9). Then $\mathcal{H}'(n)$ is free of rank one over R, so $\mathfrak{m}^{k-1}\kappa_n \neq 0$, and therefore the image of κ_n in $H^1(\mathbf{Q}, \bar{T})$ is nonzero. Thus (ii) $\Rightarrow$ (iv). □

DEFINITION 4.5.5. We say that $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is *primitive* if the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(\bar{T})$ is nonzero.

The following theorem is a sharpening of the more general Corollary 4.4.5.

THEOREM 4.5.6. *Suppose $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is primitive. If $\kappa_1 \neq 0$ then*

$$\operatorname{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) = k - \operatorname{length}(R\kappa_1) = \max\{i : \kappa_1 \in \mathfrak{m}^i H^1_{\mathcal{F}}(\mathbf{Q}, T)\}.$$

If $\kappa_1 = 0$ then $\operatorname{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) \geq k$.

PROOF. By Corollary 4.5.4, κ_1 generates $\mathcal{H}'(1) \subset \mathfrak{m}^{\operatorname{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))} H^1_{\mathcal{F}}(\mathbf{Q}, T)$, and by Lemma 4.3.2, $\operatorname{length}(\mathcal{H}'(1)) = k - \max\{\operatorname{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)), k\}$. □

We can formulate a more precise version of Theorem 4.5.6, which at least partially determines the R-module structure of $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$.

DEFINITION 4.5.7. If $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ and $r \geq 0$, define

$$\partial^{(r)}(\boldsymbol{\kappa}) = \min\{k - \operatorname{length}(R\kappa_n) : n \in \mathcal{N}, \nu(n) = r\}.$$

The *elementary divisors* of κ are defined by

$$e_i(\boldsymbol{\kappa}) = \partial^{(i)}(\boldsymbol{\kappa}) - \partial^{(i+1)}(\boldsymbol{\kappa}), \quad i \geq 0.$$

PROPOSITION 4.5.8. *Suppose $\chi(T) = 1$, $\boldsymbol{\kappa} \in \mathbf{KS}(T)$, $m \in \mathcal{N}$, and $\kappa_m \neq 0$. Write $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \cong \oplus_i R/\mathfrak{m}^{d_i}$ with nonnegative integers $d_1 \geq d_2 \geq \cdots$, and fix $j \geq 0$ such that κ_m generates $\mathfrak{m}^j \mathcal{H}'(m)$.*

Then for every $r \geq 0$,

$$\partial^{(r)}(\boldsymbol{\kappa}) = \min\{k, j + \sum_{i>r} d_i\}.$$

PROOF. Note that since κ_m generates a nonzero submodule of the cyclic R-module $\mathcal{H}'(m)$, there is a unique $j \geq 0$ such that κ_m generates $\mathfrak{m}^j\mathcal{H}'(m)$. By Corollary 4.5.2(ii), κ_n generates $\mathfrak{m}^j\mathcal{H}'(n)$ for every n. Therefore by Lemma 4.3.2 we have

$$\partial^{(r)}(\boldsymbol{\kappa}) = \min\{k, j + \lambda(n, T^*) : n \in \mathcal{N}, \nu(n) = r\}.$$

In particular when $r = 0$ we get the desired equality since $\lambda(1, T^*) = \sum_i d_i$.

Suppose $n \in \mathcal{N}$ and $\nu(n) = r$. Consider the map

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \longrightarrow \bigoplus_{\ell|n} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*).$$

The right-hand side is free of rank r over R, so the image is a quotient of $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$ generated by (at most) r elements. Hence the image has length at most $\sum_{i\leq r} d_i$. Therefore the kernel has length at least $\sum_{i>r} d_i$. But by definition this kernel is contained in $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*)$, so we conclude that $\lambda(n, T^*) \geq \sum_{i>r} d_i$. Hence $\partial^{(r)}(\boldsymbol{\kappa}) \geq \min\{k, j + \sum_{i>r} d_i\}$.

We will prove the opposite inequality by induction on r. The case $r = 0$ was proved above.

Since $\chi(T) = 1$, Theorem 4.1.13(i) shows that $\mathfrak{m}^{k-1}H^1_{\mathcal{F}}(\mathbf{Q}, T) \neq 0$. Fix a nonzero element $c \in \mathfrak{m}^{k-1}H^1_{\mathcal{F}}(\mathbf{Q}, T) \subset H^1_{\mathcal{F}}(\mathbf{Q}, T)[\mathfrak{m}]$. If $d_1 > 0$ then choose a nonzero element $c' \in \mathfrak{m}^{d_1-1}H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \subset H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[\mathfrak{m}]$. Using Proposition 3.6.1, choose a prime $\ell \in \mathcal{P}$ such that the localization c_ℓ is nonzero and, if $d_1 > 0$, such that c'_ℓ is nonzero as well.

It follows that

- the localization map $H^1_{\mathcal{F}}(\mathbf{Q}, T) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ is surjective, and
- $H^1_{(\mathcal{F}^\ell)^*}(\mathbf{Q}, T^*) \cong \oplus_{i\geq 1} R/\mathfrak{m}^{d_{i+1}}$.

By Theorem 4.1.7(ii) we have $H^1_{\mathcal{F}(\ell)^*}(\mathbf{Q}, T^*) = H^1_{(\mathcal{F}^\ell)^*}(\mathbf{Q}, T^*)$.

Let $\boldsymbol{\kappa}^{(\ell)} \in \mathbf{KS}(T, \mathcal{F}(\ell), \mathcal{P} - \{\ell\})$ be the Kolyvagin system defined in Example 3.1.12, which is obtained by setting $\kappa^{(\ell)}_n = \kappa_{n\ell} \otimes \xi$ for some generator ξ of $\mathrm{Hom}(G_\ell, R)$. We have

$$\partial^{(r)}(\boldsymbol{\kappa}) \geq \partial^{(r-1)}(\boldsymbol{\kappa}^{(\ell)}) = \min\{k, j + \sum_{i>r-1} d_{i+1}\}.$$

where the inequality is clear from the definition and the equality follows from our induction hypothesis applied to $\boldsymbol{\kappa}^{(\ell)}$. This completes the proof. □

THEOREM 4.5.9. *Suppose $\chi(T) = 1$, $\boldsymbol{\kappa} \in \mathbf{KS}(T)$, and $\kappa_1 \neq 0$. Then*

$$\begin{aligned} \partial^{(0)}(\boldsymbol{\kappa}) &\geq \partial^{(1)}(\boldsymbol{\kappa}) \geq \partial^{(2)}(\boldsymbol{\kappa}) \geq \cdots, \\ e_0(\boldsymbol{\kappa}) &\geq e_1(\boldsymbol{\kappa}) \geq e_2(\boldsymbol{\kappa}) \geq \cdots \geq 0, \end{aligned}$$

and

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \cong \bigoplus_{i\geq 0} R/\mathfrak{m}^{e_i(\boldsymbol{\kappa})}.$$

PROOF. If $\kappa_1 \neq 0$ then $\partial^{(0)}(\boldsymbol{\kappa}) < k$, so in Proposition 4.5.8 we have $\partial^{(r)}(\boldsymbol{\kappa}) = j + \sum_{i>r} d_i$ for every r. The theorem follows immediately. □

REMARK 4.5.10. Theorem 4.5.9 shows that the elementary divisors of $\boldsymbol{\kappa}$ are independent of $\boldsymbol{\kappa}$ as long as $\kappa_1 \neq 0$.

We conclude this section with a mildly pathological example in which the map $\mathbf{KS}(T) \to \overline{\mathbf{KS}}(T)$ is not injective.

EXAMPLE 4.5.11. Let $R = \mathbf{Z}/p^k\mathbf{Z}$, and take T to be a free, rank-one R-module with $G_{\mathbf{Q}}$ acting via an odd character ρ of conductor p, not the Teichmuller character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$. Define a Selmer structure $\mathcal{F}$ by $\Sigma(\mathcal{F}) = \{p, \infty\}$ and $H^1_{\mathcal{F}}(\mathbf{Q}_p, T) = H^1(\mathbf{Q}_p, T)$ (our assumptions force $p > 2$, so $H^1(\mathbf{R}, T) = 0$).

Fix primes q, ℓ congruent to one modulo p, with q not congruent to one modulo p^2. It follows without difficulty from Proposition 2.3.5 that

$$\chi(T, \mathcal{F}) = 1, \quad \chi(T, \mathcal{F}^\ell) = 2, \quad \chi(T/pT, \mathcal{F}^\ell_q) = 1.$$

Let $\mathcal{P} = \{\text{rational primes } r : r \equiv 1 \pmod{p}, r \neq q, \ell\}$. Both of the Selmer triples $(T, \mathcal{F}^\ell, \mathcal{P} \cup \{q\})$ and $(T/pT, \mathcal{F}^\ell_q, \mathcal{P})$ satisfy hypotheses (H.0) through (H.6)

By Corollary 4.5.2(i) we can fix $\boldsymbol{\kappa}' \in \mathbf{KS}(T/pT, \mathcal{F}^\ell_q, \mathcal{P}) \subset \mathbf{KS}(T/pT, \mathcal{F}^\ell, \mathcal{P})$, $\boldsymbol{\kappa}' \neq 0$. Define $\boldsymbol{\kappa}$ by

$$\kappa_n = \begin{cases} 0 & \text{if } n \in \mathcal{N}, \\ \kappa'_{n/q} & \text{if } n \in \mathcal{N}(\mathcal{P} \cup \{q\}), q \mid n. \end{cases}$$

Note that if $n \in \mathcal{N}(\mathcal{P} \cup \{q\})$ and $q \mid n$, then $I_n = pR$. It follows that $\boldsymbol{\kappa}$ is a nonzero Kolyvagin system in $\mathbf{KS}(T, \mathcal{F}^\ell, \mathcal{P} \cup \{q\})$, but the restriction of $\boldsymbol{\kappa}$ to $\mathbf{KS}(T, \mathcal{F}^\ell, (\mathcal{P} \cup \{q\}) \cap \mathcal{P}_2)$ is zero. Thus $\boldsymbol{\kappa}$ is a nonzero element of the kernel of the map $\mathbf{KS}(T, \mathcal{F}^\ell, \mathcal{P} \cup \{q\}) \to \overline{\mathbf{KS}}(T, \mathcal{F}^\ell, \mathcal{P} \cup \{q\})$.

We now return to the dual Selmer group $\mathrm{Sel}^*(\boldsymbol{\kappa})$ of Definition 3.3.1 and Example 3.3.2 attached to a Kolyvagin system $\boldsymbol{\kappa}$.

THEOREM 4.5.12. *Suppose that $\chi(T) = 1$, that the image of $R \to \mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \mathrm{End}(T)$, and that hypothesis (H.4a) holds. If $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is primitive then the canonical map*

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \longrightarrow \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}), \mathbf{Q}_p/\mathbf{Z}_p)$$

of Proposition 3.3.3 is an isomorphism.

The proof of Theorem 4.5.12 will be given after the following lemmas and proposition. Let $\mathcal{X}^0$ be the core subgraph of $\mathcal{X}$ of Definition 4.3.6.

LEMMA 4.5.13. *Suppose n is a core vertex and $\ell \in \mathcal{P}$, $\ell \nmid n$. Then either $n\ell$ is a core vertex and $n, n\ell$ are connected by an edge in $\mathcal{X}^0$, or there is a prime $q \in \mathcal{P}$ such that nq and $nq\ell$ are core vertices and there are edges of $\mathcal{X}^0$ connecting n to nq and nq to $nq\ell$.*

PROOF. Let $\bar{T} = T/\mathfrak{m}T$. If the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, \bar{T})$ is nonzero then n is a core vertex by Lemma 4.1.7(ii), and there is an edge of $\mathcal{X}^0$ joining n and $n\ell$ by Lemma 4.3.8.

Suppose now that the map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, \bar{T})$ is zero. Then the proof of Lemma 4.3.9 shows (among other things) that there is a prime $q \in \mathcal{P}$ such that nq and $nq\ell$ are core vertices and there are edges of $\mathcal{X}^0$ connecting n to nq and nq to $nq\ell$. □

Recall that if $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ and $n \in \mathcal{N}$ then

$$\mathrm{Sel}^*(\boldsymbol{\kappa}; n) = \Big(\bigoplus_{\ell \mid n} H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)\Big) \Big/ \Big(\sum_{d \mid n} \mathrm{image}(R\kappa_d)\Big)$$

after choosing generators of G_ℓ for every ℓ to view $\kappa_d \in H^1_{\mathcal{F}(d)}(\mathbf{Q}, T)$.

LEMMA 4.5.14. *If n and $n\ell$ are vertices of $\mathcal{X}^0$, connected by an edge, and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is primitive, then the natural map $\mathrm{Sel}^*(\boldsymbol{\kappa}; n) \to \mathrm{Sel}^*(\boldsymbol{\kappa}; n\ell)$ is surjective.*

PROOF. Since $n\ell$ is a core vertex and $\boldsymbol{\kappa}$ is primitive, $\kappa_{n\ell}$ generates the free, rank-one R-module $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T) \otimes G_{n\ell}$ by Corollary 4.5.4. By Lemma 4.3.8, the localization map $H^1_{\mathcal{F}(n\ell)}(\mathbf{Q}, T) \to H^1_{\mathrm{s}}(\mathbf{Q}_\ell, T)$ is surjective. It now follows directly from the definition that the map $\mathrm{Sel}^*(\boldsymbol{\kappa}; n) \to \mathrm{Sel}^*(\boldsymbol{\kappa}; n\ell)$ is surjective. □

Recall (Definition 4.1.15) that $n \in \mathcal{N}$ is a leading vertex if n is a core vertex and $\nu(n) = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}])$.

PROPOSITION 4.5.15. *Suppose $\chi(T) = 1$, the image of $R \to \mathrm{End}(T)$ is contained in the image of $\mathbf{Z}_p[[G_{\mathbf{Q}}]] \to \mathrm{End}(T)$, (H.4a) holds, and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is primitive. If n is a leading vertex then there is a prime q such that nq is a core vertex and the natural map $H^1_{\mathcal{F}}(\mathbf{Q}, T^*) \to \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}; nq), \mathbf{Q}_p/\mathbf{Z}_p)$ of Proposition 3.3.3 is an isomorphism.*

PROOF. Let $\bar{T} = T/\mathfrak{m}T$, and let $r = \dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q}, \bar{T}) = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) + 1 = \nu(n) + 1$. Then localization gives exact sequences

$$0 \longrightarrow H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, \bar{T}) \xrightarrow{\oplus \mathrm{loc}_{\ell,\mathrm{f}}} \bigoplus_{\ell | n} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T}) \longrightarrow 0,$$

$$0 \longrightarrow H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*) \xrightarrow{\oplus \mathrm{loc}_{\ell,\mathrm{f}}} \bigoplus_{\ell | n} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T}^*) \longrightarrow 0.$$

Using Proposition 3.6.2(ii), choose a prime $q \in \mathcal{P}$ so that the localization map $H^1_{\mathcal{F}(n)}(\mathbf{Q}, \bar{T}) \xrightarrow{\mathrm{loc}_{q,\mathrm{f}}} H^1_{\mathrm{f}}(\mathbf{Q}_q, \bar{T})$ is nonzero and such that for every prime r dividing nq,

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*) \xrightarrow{\oplus \mathrm{loc}_{\ell,\mathrm{f}}} \bigoplus_{\ell | nq/r} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T}^*)$$

is an isomorphism. (For the latter, we can choose q so that the kernel of $\mathrm{loc}_{q,\mathrm{f}}$ on $H^1_{\mathcal{F}^*}(\mathbf{Q}, \bar{T}^*)$ is equal to the kernel of $\sum_{\ell | n} \psi_\ell \circ \mathrm{loc}_{\ell,\mathrm{f}}$ where $\psi_\ell : H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T}^*) \xrightarrow{\sim} \Bbbk$ is a fixed isomorphism.) We conclude that

$$H^1_{\mathcal{F}}(\mathbf{Q}, \bar{T}) \xrightarrow{\oplus \mathrm{loc}_{\ell,\mathrm{f}}} \bigoplus_{\ell | nq} H^1_{\mathrm{f}}(\mathbf{Q}_\ell, \bar{T})$$

is an isomorphism.

By Lemma 4.1.7(ii), nq is a core vertex. Applying Lemma 4.1.7(iv) inductively we see that nq/ℓ is a core vertex for every prime ℓ dividing nq, and that $\mathrm{loc}_{\ell,\mathrm{f}} : H^1_{\mathcal{F}(nq/\ell)}(\mathbf{Q}, T) \to H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T)$ is an isomorphism.

Fix generators of G_ℓ for every ℓ, so that we can view $\kappa_m \in H^1_{\mathcal{F}(m)}(\mathbf{Q}, T)$ for every m. By Theorem B.2 from Howard's Appendix B, $H^1_{\mathcal{F}^{nq}}(\mathbf{Q}, T)$ is free of rank $r + 1$ over R. We claim that $\{\kappa_{nq}\} \cup \{\kappa_{nq/\ell} : \ell \mid nq\}$ is an R-basis of $H^1_{\mathcal{F}^{nq}}(\mathbf{Q}, T)$. For, suppose that

$$a\kappa_{nq} + \sum_{\ell | nq} a_\ell \kappa_{nq/\ell} = 0$$

with $a, a_\ell \in R$. Applying $\mathrm{loc}_{\ell,\mathrm{f}}$ shows that $a_\ell \kappa_{nq/\ell} = 0$ for each ℓ, and then that $a\kappa_{nq} = 0$ as well. Since $\boldsymbol{\kappa}$ is primitive, each $\kappa_{nq}, \kappa_{nq/\ell}$ generates a free, rank-one

R-module (Corollary 4.5.4), so we must have $a = a_\ell = 0$ for every ℓ and the claim follows.

Now the proposition follows from global duality (Theorem 2.3.4) applied with $\mathcal{G}_1 = \mathcal{F}$ and $\mathcal{G}_2 = \mathcal{F}^{nq}$ (using that $H^1_{(\mathcal{F}^{nq})^*}(\mathbf{Q}, T^*) \subset H^1_{\mathcal{F}(nq)^*}(\mathbf{Q}, T^*) = 0$). □

Proof of Theorem 4.5.12. Fix a leading vertex n and a prime q as in Proposition 4.5.15. for any $m \in \mathcal{N}$ we can choose, using Lemma 4.5.13, a sequence of primes $\ell_1, \dots, \ell_t$ such that every $m_j = nq\prod_{i=1}^{j}\ell_j$ is a core vertex, there is a sequence of edges in $\mathcal{X}^0$ forming a path n—nq—m_1—m_2—$\cdots$—m_t, and m_t is divisible by m. By Lemma 4.5.14 the map $\mathrm{Sel}^*(\boldsymbol{\kappa}; nq) \to \mathrm{Sel}^*(\boldsymbol{\kappa}; m_t)$ is surjective. On the other hand, Proposition 4.5.15 shows that the composition

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \longrightarrow \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}; m_t), \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}; nq), \mathbf{Q}_p/\mathbf{Z}_p)$$

is an isomorphism. Hence $\mathrm{Sel}^*(\boldsymbol{\kappa}; nq) \to \mathrm{Sel}^*(\boldsymbol{\kappa}; m_t)$ is an isomorphism, and so passing to the direct limit over m we conclude that $H^1_{\mathcal{F}}(\mathbf{Q}, T^*) \to \mathrm{Hom}(\mathrm{Sel}^*(\boldsymbol{\kappa}), \mathbf{Q}_p/\mathbf{Z}_p)$ is an isomorphism. □

Remark 4.5.16. The proof of Theorem 4.5.12 (specifically Lemma 4.5.14 and Proposition 4.5.15) shows that, under the hypotheses of that theorem, if we fix generators of G_ℓ for every ℓ to view $\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$ for every n, then the collection $\{\kappa_n : n \in \mathcal{N}\}$ generates $\cup_n H^1_{\mathcal{F}^n}(\mathbf{Q}, T)$. More precisely, we can find an $m \in \mathcal{N}$ and order the set $\{\ell \in \mathcal{P} : \ell \nmid m\} = \{\ell_1, \ell_2, \ell_3 \dots\}$ so that

$$\{\kappa_{m/\ell} : \ell \mid m\} \cup \{\kappa_{m\prod_{i=1}^{j}\ell_i} : j \geq 0\}$$

generates $\cup_n H^1_{\mathcal{F}^n}(\mathbf{Q}, T)$.

CHAPTER 5

Kolyvagin Systems over Integral Domains

5.1. Kolyvagin systems over a field

Suppose for this section that $R = \Bbbk$ is a field, and that the Selmer triple $(T, \mathcal{F}, \mathcal{P})$ satisfies hypotheses (H.0) through (H.5) (hypothesis (H.6) is vacuous when R is a field).

In particular R is principal and artinian, so we can apply the results of Chapter 4 with $k = 1$. The following theorem summarizes our results in this case. Recall that the order of vanishing of $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is $\mathrm{ord}(\boldsymbol{\kappa}) = \min\{\nu(n) : n \in \mathcal{N}, \kappa_n \neq 0\}$.

THEOREM 5.1.1. *Suppose $R = \Bbbk$ is a field.*

(i) *If $\chi(T) \leq 1$ then $\dim_{\Bbbk} \mathbf{KS}(T) = \chi(T)$.*
(ii) *If $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is nonzero, then $\kappa_n \neq 0$ if and only if n is a core vertex.*
(iii) *If $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is nonzero, then $\dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) = \mathrm{ord}(\boldsymbol{\kappa})$.*

PROOF. Assertion (i) is Theorem 4.2.2 (when $\chi(T) = 0$) and Corollary 4.5.2(i) (when $\chi(T) = 1$). If $\chi(T) = 1$ we have

$$\mathcal{H}'(n) \neq 0 \iff \lambda(n, T^*) = 0 \iff n \text{ is a core vertex},$$

so (ii) is Corollary 4.5.2(ii) in this setting.

Assertion (iii) is immediate from (ii) and Corollary 4.1.9. □

REMARK 5.1.2. Howard's Theorem 4.3.3(iii) shows that if $\chi(T) > 1$, then $\mathbf{KS}(T)$ is infinite dimensional over $\Bbbk$.

Recall (Definition 4.1.15) that a leading vertex is an $n \in \mathcal{N}$ such that $\nu(n) = \dim_{\Bbbk} H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$ and $H^1_{\mathcal{F}(n)^*}(\mathbf{Q}, T^*) = 0$.

THEOREM 5.1.3. *Suppose $\chi(T) = 1$, hypothesis* (H.4a) *is satisfied, and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is nonzero. If $\mathcal{L}$ is a line in $H^1_{\mathcal{F}}(\mathbf{Q}, T)$, then there is a leading vertex $n \in \mathcal{N}$ such that κ_n generates $\mathcal{L} \otimes G_n$. If $\dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q}, T) > 1$ then there are infinitely many such n.*

PROOF. If $\dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q}, T) > 1$ then by Theorem 4.1.16 there are infinitely many leading vertices n such that $\mathcal{L} \subset H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$, and since a leading vertex has $\dim_{\Bbbk} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) = 1$, we must have $\mathcal{L} = H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$. If $\dim_{\Bbbk} H^1_{\mathcal{F}}(\mathbf{Q}, T) = 1$ then $\mathcal{L} = H^1_{\mathcal{F}}(\mathbf{Q}, T)$ and $n = 1$ is a leading vertex.

In either case, Theorem 5.1.1(ii) shows that $\kappa_n \neq 0$, so κ_n is a generator of $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \otimes G_n = \mathcal{L} \otimes G_n$. □

5.2. Kolyvagin systems over a discrete valuation ring

For this section we assume that R is a discrete valuation ring. We assume that the triple $(T, \mathcal{F}, \mathcal{P})$ satisfies Hypotheses (H.0) through (H.5). We assume also that the Selmer structure $\mathcal{F}$ is such that $H^1(\mathbf{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ is torsion free for every $\ell \in \Sigma(\mathcal{F})$. Then for every k, $T/\mathfrak{m}^k T$ (with the induced Selmer structure) satisfies (H.0) through (H.6) (this clear for (H.0) through (H.5), and for (H.6) it follows from Lemma 3.7.1(i)). Thus we can apply the results of Chapter 4 to study the image of $\mathbf{KS}(T)$ in $\mathbf{KS}(T/\mathfrak{m}^k T)$ for every k, and use this information to study $\mathbf{KS}(T)$.

Again we write $\bar{T} = T/\mathfrak{m}T$. For simplicity we suppose that $\mathcal{P} = \mathcal{P}_1$.

Writing $\mathrm{Frac}(R)$ for the field of fractions of R, we define the rank of an R-module M to be $\mathrm{rank}_R M = \dim_{\mathrm{Frac}(R)} M \otimes \mathrm{Frac}(R)$ and the corank of M to be $\mathrm{corank}_R M = \mathrm{rank}_R \mathrm{Hom}(M, \mathbf{Q}_p/\mathbf{Z}_p)$.

Definition 5.2.1. If $\boldsymbol{\kappa} \in \mathbf{KS}(T)$, define

$$\partial^{(0)}(\boldsymbol{\kappa}) = \max\{j : \kappa_1 \in \mathfrak{m}^j H^1_{\mathcal{F}}(\mathbf{Q}, T)\}$$

(we allow $\partial^{(0)}(\boldsymbol{\kappa}) = \infty$). This is a special case of Definition 5.2.11 below.

Theorem 5.2.2. *If $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ then*

$$\mathrm{length}_R H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \le \partial^{(0)}(\boldsymbol{\kappa}).$$

In particular if $\kappa_1 \neq 0$ then $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$ is finite.

Proof. We may assume that $\kappa_1 \neq 0$ or else there is nothing to prove. Then $\partial^{(0)}(\boldsymbol{\kappa})$ is finite, because $H^1(\mathbf{Q}, T)$ has no nonzero divisible submodules.

For every $k \in \mathbf{Z}^+$, let $\boldsymbol{\kappa}^{(k)}$ be the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/\mathfrak{m}^k T)$. Then $\kappa_1^{(k)}$ is the image of κ_1 under the natural map $H^1(\mathbf{Q}, T) \to H^1(\mathbf{Q}, T/\mathfrak{m}^k T)$, so $\kappa_1^{(k)} \in \mathfrak{m}^{\partial^{(0)}(\boldsymbol{\kappa})} H^1_{\mathcal{F}}(\mathbf{Q}, T/\mathfrak{m}^k T)$. By Corollary 4.4.5, it follows that

$$\mathrm{length}_R H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[\mathfrak{m}^k] = \mathrm{length}_R H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}^k]) \le \partial^{(0)}(\boldsymbol{\kappa}).$$

Since $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) = \cup H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[\mathfrak{m}^k]$, this proves the theorem. □

Remark 5.2.3. The definition of $\partial^{(0)}(\boldsymbol{\kappa})$ also makes sense for $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(T)$ (see Definition 3.1.6). Then Theorem 5.2.2 remains true, with the same proof, if we replace $\mathbf{KS}(T)$ by $\overline{\mathbf{KS}}(T)$ in the statement.

Definition 5.2.4. For every $k \in \mathbf{Z}^+$ we have the Selmer triple $(T/\mathfrak{m}^k T, \mathcal{F}, \mathcal{P}_k)$ over $R/\mathfrak{m}^k$, with the induced Selmer structure $\mathcal{F}$. By Theorem 4.1.13, the core ranks $\chi(T/\mathfrak{m}^k T)$ and $\chi(T^*[\mathfrak{m}^k])$ are independent of k. We define $\chi(T)$, the core rank of T, to be this common value $\chi(T/\mathfrak{m}^k T)$, and similarly $\chi(T^*) = \chi(T^*[\mathfrak{m}^k])$.

In particular either $\chi(T) = 0$ or $\chi(T^*) = 0$.

Theorem 5.2.5. *For every $k \in \mathbf{Z}^+$ and every $n \in \mathcal{N}_k$ there is a noncanonical isomorphism*

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

Proof. Since $\chi(T) = \chi(T/\mathfrak{m}^k T)$ and $\chi(T^*) = \chi(T^*[\mathfrak{m}^k])$, this is just a restatement of Theorem 4.1.13. □

Corollary 5.2.6. $\mathrm{rank}_R(H^1_{\mathcal{F}}(\mathbf{Q}, T)) - \mathrm{corank}_R(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) = \chi(T) - \chi(T^*)$.

PROOF. We have

$$H^1_{\mathcal{F}}(\mathbf{Q},T) = \varprojlim H^1_{\mathcal{F}}(\mathbf{Q},T/\mathfrak{m}^kT), \qquad H^1_{\mathcal{F}^*}(\mathbf{Q},T^*) = \varinjlim H^1_{\mathcal{F}^*}(\mathbf{Q},T^*[\mathfrak{m}^k]),$$

so (using Lemma 4.1.1) this follows from Theorem 5.2.5. □

LEMMA 5.2.7. *The natural map* $\mathbf{KS}(T,\mathcal{P}) \to \varprojlim \mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_k)$ *is injective*

PROOF. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is nonzero. Then we can find an n such that $\kappa_n \neq 0$ in $H^1_{\mathcal{F}(n)}(\mathbf{Q},T/I_nT)$. If $I_n \neq 0$ then let k be such that $\mathfrak{m}^k = I_n$. If $I_n = 0$ (for example, if $n=1$) choose k so that $\kappa_n \neq 0$ in $H^1_{\mathcal{F}(n)}(\mathbf{Q},T/\mathfrak{m}^kT)\otimes G_n$. In either case $I_n \subset \mathfrak{m}^k$, so $n \in \mathcal{N}_k$ and the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_k)$ is nonzero. □

LEMMA 5.2.8. *Suppose* $\chi(T) = 1$ *and* $j \leq k$. *The projection map* $T/\mathfrak{m}^kT \to T/\mathfrak{m}^jT$ *and restriction to* $\mathcal{P}_k$ *induce a surjection and an isomorphism, respectively*

$$\mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_k) \twoheadrightarrow \mathbf{KS}(T/\mathfrak{m}^jT,\mathcal{P}_k) \xleftarrow{\sim} \mathbf{KS}(T/\mathfrak{m}^jT,\mathcal{P}_j).$$

PROOF. This is Corollary 4.5.2(iv) and (v). □

PROPOSITION 5.2.9. *If* $\chi(T) = 1$ *then the natural maps give isomorphisms*

$$\mathbf{KS}(T) \xrightarrow{\sim} \varprojlim \mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_k) \xrightarrow{\sim} \overline{\mathbf{KS}}(T).$$

PROOF. Lemma 5.2.8 shows that for every k we have

$$\mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_k) \xrightarrow{\sim} \varinjlim_j \mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_j)$$

which gives the second isomorphism of the proposition. The injectivity of the first map is Lemma 5.2.7, so we need only show surjectivity.

Suppose $\{\boldsymbol{\kappa}^{(k)}\} \in \varprojlim \mathbf{KS}(T/\mathfrak{m}^k,\mathcal{P}_k)$. If $n \in \mathcal{N}$, let j be maximal such that $n \in \mathcal{N}_j$. If $j < \infty$ then $I_n = \mathfrak{m}^j$, and we define $\kappa_n = \kappa_n^{(j)} \in H^1_{\mathcal{F}(n)}(\mathbf{Q},T/I_nT)\otimes G_n$. If $j = \infty$ (for example, when $n=1$) then we set $\kappa_n = \lim_k \kappa_n^{(k)} \in H^1_{\mathcal{F}(n)}(\mathbf{Q},T)\otimes G_n$. It is straightforward to verify that this defines an element $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ which maps to $\boldsymbol{\kappa}^{(k)} \in \mathbf{KS}(T/\mathfrak{m}^kT)$ for every k. □

THEOREM 5.2.10. (i) *If* $\chi(T) = 0$ *then* $\mathbf{KS}(T) = 0$.

(ii) *If* $\chi(T) = 1$ *then* $\mathbf{KS}(T)$ *is a free* R*-module of rank one, generated by a* $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ *whose image in* $\mathbf{KS}(\bar{T})$ *is nonzero.*

PROOF. If $\chi(T) = 0$ then $\mathbf{KS}(T/\mathfrak{m}^kT,\mathcal{P}_k) = 0$ for every k by Theorem 4.2.2, and (i) follows by Lemma 5.2.7.

Suppose now that $\chi(T) = 1$. By Corollary 4.5.2(i), $\mathbf{KS}(T/\mathfrak{m}^k,\mathcal{P}_k)$ is free of rank one over $R/\mathfrak{m}^k$ for every k. The maps $\mathbf{KS}(T/\mathfrak{m}^{k+1},\mathcal{P}_{k+1}) \to \mathbf{KS}(T/\mathfrak{m}^k,\mathcal{P}_k)$ are surjective by Lemma 5.2.8, so (ii) follows by Proposition 5.2.9. □

DEFINITION 5.2.11. Recall that the order of vanishing of a nonzero $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is $\mathrm{ord}(\boldsymbol{\kappa}) = \min\{\nu(n) : n \in \mathcal{N}, \kappa_n \neq 0\}$.

For $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ and $r \in \mathbf{Z}^+$ define (compare Definition 4.5.7)

$$\partial^{(r)}(\boldsymbol{\kappa}) = \max\{j : \kappa_n \in \mathfrak{m}^j H^1_{\mathcal{F}(n)}(\mathbf{Q},T/I_nT)\otimes G_n \text{ for every } n \in \mathcal{N} \text{ with } \nu(n) = r\}$$

(we allow $\partial^{(r)}(\boldsymbol{\kappa}) = \infty$), and the sequence of *elementary divisors*

$$e_i(\boldsymbol{\kappa}) = \partial^{(i)}(\boldsymbol{\kappa}) - \partial^{(i+1)}(\boldsymbol{\kappa}), \quad i \geq \mathrm{ord}(\boldsymbol{\kappa}).$$

Then $\partial^{(0)}(\boldsymbol{\kappa}) = \max\{j : \kappa_1 \in \mathfrak{m}^j H^1_{\mathcal{F}}(\mathbf{Q}, T)\}$ as in Definition 5.2.1, and if $r < \mathrm{ord}(\boldsymbol{\kappa})$ then $\partial^{(r)}(\boldsymbol{\kappa}) = \infty$. Theorem 5.2.12(ii) below shows that $\partial^{(r)}(\boldsymbol{\kappa})$ is finite if $\chi(T) = 1$ and $r \geq \mathrm{ord}(\boldsymbol{\kappa})$, so the $e_i(\boldsymbol{\kappa})$ are well-defined. Define

$$\partial^{(\infty)}(\boldsymbol{\kappa}) = \min\{\partial^{(r)}(\boldsymbol{\kappa}) : r \geq 0\}.$$

As in Definition 4.5.5 we say $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is primitive if its image in $\mathbf{KS}(\bar{T})$ is nonzero.

THEOREM 5.2.12. *Suppose $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$, $\boldsymbol{\kappa} \neq 0$. Then*

(i) *for every s, $\partial^{(s)}(\boldsymbol{\kappa}) = \lim_{k\to\infty} \partial^{(s)}(\boldsymbol{\kappa}^{(k)})$ where $\boldsymbol{\kappa}^{(k)}$ is the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T/\mathfrak{m}^k T, \mathcal{P}_k)$ and $\partial^{(s)}(\boldsymbol{\kappa}^{(k)})$ is given by Definition 4.5.7,*
(ii) *the sequence $\partial^{(s)}(\boldsymbol{\kappa})$ is nonincreasing, and finite for $s \geq \mathrm{ord}(\boldsymbol{\kappa})$,*
(iii) *the sequence $e_i(\boldsymbol{\kappa})$ is nonincreasing, nonnegative, and finite for $i \geq \mathrm{ord}(\boldsymbol{\kappa})$,*
(iv) *$\mathrm{ord}(\boldsymbol{\kappa})$ and the $e_i(\boldsymbol{\kappa})$ are independent of the choice of nonzero $\boldsymbol{\kappa} \in \mathbf{KS}(T)$,*
(v) *$\mathrm{corank}_R(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) = \mathrm{ord}(\boldsymbol{\kappa})$,*
(vi) *$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)/(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))_{\mathrm{div}} \cong \oplus_{i\geq \mathrm{ord}(\boldsymbol{\kappa})} R/\mathfrak{m}^{e_i(\boldsymbol{\kappa})}$,*
(vii) *$\mathrm{length}_R(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)/(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))_{\mathrm{div}}) = \partial^{(\mathrm{ord}(\boldsymbol{\kappa}))}(\boldsymbol{\kappa}) - \partial^{(\infty)}(\boldsymbol{\kappa})$,*
(viii) *$\boldsymbol{\kappa}$ is primitive if and only if $\partial^{(\infty)}(\boldsymbol{\kappa}) = 0$.*

PROOF. Write $r = \mathrm{corank}_R(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))$ and

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)/(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))_{\mathrm{div}} \cong \bigoplus_{i>r} R/\mathfrak{m}^{d_i}$$

with $d_{r+1} \geq d_{r+2} \geq \cdots$. Let $d_1 = \cdots d_r = \infty$. If $k \in \mathbf{Z}^+$ then

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}^k]) = H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)[\mathfrak{m}^k] \cong \bigoplus_{i\geq 1} R/\mathfrak{m}^{\min\{k,d_i\}}.$$

Fix a generator π of $\mathfrak{m}$. By Theorem 5.2.10 we can choose a primitive $\boldsymbol{\kappa}_0 \in \mathbf{KS}(T)$ and a $j \geq 0$ such that $\boldsymbol{\kappa} = \pi^j \boldsymbol{\kappa}_0$. Then Proposition 4.5.8 shows that for every s and k

$$\partial^{(s)}(\boldsymbol{\kappa}^{(k)}) = \min\{k, j + \sum_{i>s} \min\{k, d_i\}\}. \tag{11}$$

Fix $s \geq 0$, and let $h = \partial^{(s)}(\boldsymbol{\kappa})$. Then we can find $n \in \mathcal{N}$ (necessarily in $\mathcal{N}_{h+1}$), with $\nu(n) = s$, such that $\kappa_n \notin \mathfrak{m}^{h+1} H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_n T) \otimes G_n$. Therefore by Theorem 4.4.3 and Lemma 4.3.2, $\partial^{(s)}(\kappa^{(h+1)}) \leq h$. By (11) it follows that $\partial^{(s)}(\kappa^{(k)}) \leq h = \partial^{(s)}(\boldsymbol{\kappa})$ for all k.

On the other hand, since $\kappa_n \in \mathfrak{m}^h H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_n T) \otimes G_n$ for every n with $\nu(n) = s$, by definition we have $\partial^{(s)}(\boldsymbol{\kappa}^{(k)}) \geq h$ for every $k \geq h$. Thus $\partial^{(s)}(\boldsymbol{\kappa}) = \sup\{\partial^{(s)}(\boldsymbol{\kappa}^{(k)}) : k \in \mathbf{Z}^+\}$. Since $\partial^{(s)}(\boldsymbol{\kappa}^{(k)})$ is a nondecreasing function of k by (11), this proves (i).

The rest of the theorem follows from (i) and (11). □

COROLLARY 5.2.13. *Suppose $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$ is nonzero.*

(i) *$\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))$ is finite if and only if $\kappa_1 \neq 0$.*
(ii) *$\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) \leq \partial^{(0)}(\boldsymbol{\kappa}) = \max\{j : \kappa_1 \in \mathfrak{m}^j H^1_{\mathcal{F}}(\mathbf{Q}, T)\}$, with equality if and only if $\boldsymbol{\kappa}$ is primitive.*

PROOF. If $\kappa_1 = 0$ then $\mathrm{ord}(\boldsymbol{\kappa}) \geq 1$, so $\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*))$ is infinite by Theorem 5.2.12(v). The other direction of (i) is Theorem 5.2.2.

Assertion (ii) is immediate from Theorem 5.2.12(vii) and (viii). □

Let $\mathcal{L} = \{\kappa_1 : \boldsymbol{\kappa} \in \mathbf{KS}(T)\} \subset H^1_{\mathcal{F}}(\mathbf{Q}, T)$ denote the module of L-values given by Definition 3.1.5.

THEOREM 5.2.14. *If $\chi(T) = 1$ then*

$$\mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) = \mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}, T)/\mathcal{L}).$$

PROOF. By Lemma 3.5.2, $H^0(\mathbf{Q}, \bar{T}) = 0$. It follows that $H^1(\mathbf{Q}, T)$ has no R-torsion, and then Corollary 5.2.6 shows that $H^1_{\mathcal{F}}(\mathbf{Q}, T)$ is a free R-module of rank equal to $\mathrm{corank}_R(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)) + 1$.

By Theorem 5.2.10(ii), $\mathbf{KS}(T)$ is generated by a primitive Kolyvagin system $\boldsymbol{\kappa}$, and then $\mathcal{L} = R\kappa_1$. If $\kappa_1 = 0$ then both $H^1_{\mathcal{F}}(\mathbf{Q}, T)/\mathcal{L}$ and (by Corollary 5.2.13(i)) $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$ have infinite length. If $\kappa_1 \neq 0$ then (again using Corollary 5.2.13(i)) $H^1_{\mathcal{F}}(\mathbf{Q}, T)$ is free of rank one over R, so $\mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}, T)/\mathcal{L}) = \partial^{(0)}(\boldsymbol{\kappa})$ which by Corollary 5.2.13(ii) is the length of $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$. □

Let $d^- = \mathrm{rank}_R(T^-)$, where T^- is the minus part of T for the action of some complex conjugation.

THEOREM 5.2.15. *Suppose $\mathcal{F} = \mathcal{F}_{\mathrm{can}}$, the canonical Selmer structure on T given by Definition 3.2.1. Then $\chi(T^*) = 0$ and*

$$\chi(T) = d^- + \mathrm{corank}_R(H^0(\mathbf{Q}_p, T^*)).$$

PROOF. If f, g are functions of $k \in \mathbf{Z}^+$, we will write $f(k) \sim g(k)$ to mean that $|f(k) - g(k)|$ is bounded independently of k.

By Proposition 2.3.5 (with T replaced by $T^*[\mathfrak{m}^k]$) and Lemma 3.5.2, for every $k \in \mathbf{Z}^+$

$$\begin{aligned}\mathrm{length}(H^1_{\mathcal{F}}(\mathbf{Q}, T/\mathfrak{m}^k T)) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*[\mathfrak{m}^k])) \\ = \sum_{\ell \in \Sigma(\mathcal{F})} (\mathrm{length}(H^0(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k])) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k]))). \quad (12)\end{aligned}$$

By Theorem 5.2.5, the left-hand side of (12) is $k(\chi(T) - \chi(T^*))$. When $\ell = \infty$, we have $\mathrm{length}(H^1_{\mathcal{F}}(\mathbf{R}, T^*[\mathfrak{m}^k])) \sim 0$ and $\mathrm{length}(H^0(\mathbf{R}, T^*[\mathfrak{m}^k])) \sim kd^-$.

Suppose $\ell \in \Sigma(\mathcal{F})$, $\ell \neq p$. Recalling (Definition 1.1.6(iii))

$$H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k]) = H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, T^*[\mathfrak{m}^k]^{\mathcal{I}_\ell}) = T^*[\mathfrak{m}^k]^{\mathcal{I}_\ell}/(\mathrm{Fr}_\ell - 1)T^*[\mathfrak{m}^k]^{\mathcal{I}_\ell}$$

we have an exact sequence

$$0 \to H^0(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k]) \to T^*[\mathfrak{m}^k]^{\mathcal{I}_\ell} \xrightarrow{\mathrm{Fr}_\ell - 1} T^*[\mathfrak{m}^k]^{\mathcal{I}_\ell} \to H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k]) \to 0$$

and so $\mathrm{length}(H^0(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k])) = \mathrm{length}(H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k]))$. It now follows from Lemma 1.3.5 of [**Ru6**] that

$$\mathrm{length}(H^0(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k])) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*[\mathfrak{m}^k])) \sim 0.$$

When $\ell = p$, we have $H^1_{\mathcal{F}^*}(\mathbf{Q}_p, T^*) = 0$ by definition of the canonical Selmer structure, so $H^1_{\mathcal{F}^*}(\mathbf{Q}_p, T^*[\mathfrak{m}^k]) = \ker[H^1(\mathbf{Q}_p, T^*[\mathfrak{m}^k]) \to H^1(\mathbf{Q}_p, T^*)]$, which is a quotient of $H^0(\mathbf{Q}_p, T^*)/H^0(\mathbf{Q}_p, T^*)_{\mathrm{div}}$, which has finite length independent of k. Thus

$$\mathrm{length}(H^0(\mathbf{Q}_p, T^*[\mathfrak{m}^k])) - \mathrm{length}(H^1_{\mathcal{F}^*}(\mathbf{Q}_p, T^*[\mathfrak{m}^k])) \sim k\,\mathrm{corank}(H^0(\mathbf{Q}_p, T^*)).$$

Combining these observations we conclude that

$$k(\chi(T) - \chi(T^*)) \sim k(d^- + \mathrm{corank}_R(H^0(\mathbf{Q}_p, T^*))$$

and the theorem follows. □

For applications of these results see §6.1 and §6.2.

5.3. Kolyvagin systems over Λ

Let $\mathbf{Q}_\infty$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$, and $\mathbf{Q}_n \subset \mathbf{Q}_\infty$ the (unique, cyclic) extension of degree p^n over $\mathbf{Q}$. Let Λ denote the Iwasawa algebra

$$\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]] = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})].$$

For this section suppose that T is a free $\mathbf{Z}_p$-module of finite rank with a continuous action of $G_\mathbf{Q}$, unramified outside a finite set of primes. We set $\mathbf{T} = T \otimes \Lambda$ with $G_\mathbf{Q}$ acting on both factors, and we take $R = \Lambda$. Let $\mathcal{A}$ denote the augmentation ideal of Λ, so that $\mathbf{T}/\mathcal{A}\mathbf{T} = T$, and let $\bar{T} = T/pT = \mathbf{T}/\mathfrak{m}\mathbf{T}$.

We assume throughout this section that T satisfies hypotheses (H.0) through (H.4), and then it follows immediately that $\mathbf{T}$ satisfies (H.0) through (H.4) as well. For simplicity we fix $\mathcal{P} = \mathcal{P}_1$. Fix a finite set of primes Σ containing p, ∞, and the primes where T is ramified, and let $\mathbf{Q}_\Sigma$ denote the maximal extension of $\mathbf{Q}$ unramified outside of Σ.

Lemma 5.3.1. (i) $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T}) \cong \varprojlim H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, T)$.
(ii) *If $\ell \neq p$ then* $H^1(\mathbf{Q}_\ell, \mathbf{T}) = H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, \mathbf{T})$.
(iii) $H^1(\mathbf{Q}, \mathbf{T}) = H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T})$.

Proof. (See [**Co**] Proposition II.1.1.) By Shapiro's Lemma,

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, T \otimes \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]) = H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, T),$$

and so we have

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T}) = H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \varprojlim T \otimes \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]) \cong \varprojlim H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_n, T).$$

Similarly, if ℓ is a prime we have an isomorphism

$$H^1(\mathbf{Q}_\ell, \mathbf{T}) \cong \varprojlim \oplus_{\lambda|\ell} H^1(\mathbf{Q}_{n,\lambda}, T).$$

By a standard argument (see [**Ru6**] Proposition B.3.4 for details),

$$\varprojlim \oplus_{\lambda|\ell} H^1(\mathbf{Q}_{n,\lambda}, T) = \varprojlim \oplus_{\lambda|\ell} H^1_{\mathrm{unr}}(\mathbf{Q}_{n,\lambda}, T).$$

This proves (ii), and then (iii) follows from (i) and (ii). □

Definition 5.3.2. We define a Selmer structure $\mathcal{F}_\Lambda$ on $\mathbf{T}$ by setting $\Sigma(\mathcal{F}_\Lambda) = \Sigma$ and $H^1_\mathcal{F}(\mathbf{Q}_v, \mathbf{T}) = H^1(\mathbf{Q}_v, \mathbf{T})$ for $v \in \Sigma$. By Lemma 5.3.1(ii) we also have $H^1_{\mathrm{f}}(\mathbf{Q}_v, \mathbf{T}) = H^1(\mathbf{Q}_v, \mathbf{T})$ for $v \notin \Sigma$. Thus this Selmer structure is independent of the choice of Σ, and we have $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}, \mathbf{T}) = H^1(\mathbf{Q}, \mathbf{T})$.

Note that the induced Selmer structure $\mathcal{F}_\Lambda$ on quotients $\mathbf{T}/I\mathbf{T}$ (such as T and $\bar{T}$) will not usually satisfy $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_v, \mathbf{T}/I\mathbf{T}) = H^1(\mathbf{Q}_v, \mathbf{T}/I\mathbf{T})$.

We have the following analogue of Theorem 3.2.4, which says that an Euler system for T gives rise to a Kolyvagin system for T. Let $\mathbf{ES}(T) = \mathbf{ES}(T, \mathcal{P}, \mathcal{K})$ be the Galois module of Euler systems for T as given in Definition 3.2.2, and recall the generalized module of Kolyvagin systems $\overline{\mathbf{KS}}(\mathbf{T})$ of Definition 3.1.6.

THEOREM 5.3.3. *Suppose that $\mathcal{K}$ contains the maximal abelian p-extension of $\mathbf{Q}$ which is unramified outside of p and $\mathcal{P}$, and*

(a) *$T/(\mathrm{Fr}_\ell - 1)T$ is a cyclic R-module for every $\ell \in \mathcal{P}$,*

(b) *$\mathrm{Fr}_\ell^{p^k} - 1$ is injective on T for every $\ell \in \mathcal{P}$ and every $k \geq 0$.*

Then there is a canonical homomorphism $\mathbf{ES}(T, \mathcal{K}, \mathcal{P}) \to \overline{\mathbf{KS}}(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{P})$ with the property that if $\mathbf{c}$ maps to $\boldsymbol{\kappa}$, then

$$\kappa_1 = \{c_{\mathbf{Q}_n}\} \in \varprojlim H^1(\mathbf{Q}_n, T) = H^1(\mathbf{Q}, \mathbf{T}).$$

This theorem will be proved in Appendix A, along with Theorem 3.2.4.

LEMMA 5.3.4. *For every $i \geq 0$, the Λ-modules $H^i(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T})$ and $H^i(\mathbf{Q}_p, \mathbf{T})$ are finitely generated, and $H^i(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T}^*)$ is co-finitely generated.*

Further, $H^2(\mathbf{Q}_p, \mathbf{T})$ is a torsion Λ-module.

PROOF. These are standard results. For the global cohomology groups see for example [**Gr2**] Proposition 3 or §3 of [**PR1**]. For the local cohomology groups see for example [**Gr2**] Proposition 1 or [**PR2**] Proposition 3.2.1. □

LEMMA 5.3.5. *The Λ-module $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}, \mathbf{T}) = H^1(\mathbf{Q}, \mathbf{T})$ is finitely generated and torsion-free, and $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*)$ is co-finitely generated.*

PROOF. The fact that these modules are (co-) finitely generated follows from Lemma 5.3.4. By Lemma 3.5.2, $T^{G_\mathbf{Q}} = 0$, so by the lemma of §1.3.3 of [**PR3**], $H^1(\mathbf{Q}, \mathbf{T})$ has no Λ-torsion. □

THEOREM 5.3.6. *Suppose $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbf{T})$, and $\kappa_1 \neq 0$. Then $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*)$ is a co-torsion Λ-module.*

Theorem 5.3.6 will be proved below. The assertion that $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*)$ is a co-torsion Λ-module is a form of the weak Leopoldt conjecture. See for example [**Gr2**] Conjecture 2 or [**PR3**] §1.3.

DEFINITION 5.3.7. If X is a finitely generated Λ-module, then there is a pseudo-isomorphism (Λ-module map with finite kernel and cokernel) $X \to \oplus_i \Lambda/f_i\Lambda$, where the f_i are elements of Λ (which can be zero). If further X is a torsion Λ-module then the *characteristic ideal* $\mathrm{char}(X)$ of X is the (nonzero) ideal $(\prod_i f_i)\Lambda$. If convenient we may assume that each nonzero f_i is a power of an irreducible element of Λ.

DEFINITION 5.3.8. If $c \in H^1(\mathbf{Q}, \mathbf{T})$, we let $\mathrm{Ind}(c)$ denote the principal ideal of Λ

$$\mathrm{Ind}(c) = \mathrm{char}((H^1(\mathbf{Q}, \mathbf{T})/\Lambda c)_{\mathrm{tors}}).$$

By Lemma 5.3.5, $H^1(\mathbf{Q}, \mathbf{T})$ is pseudo-isomorphic to a free Λ-module. If we fix a pseudo-isomorphism $\psi : H^1(\mathbf{Q}, \mathbf{T}) \to \Lambda^r$ and write $\psi(c) = (a_1, \ldots, a_r)$, then $\mathrm{Ind}(c)$ is the greatest common divisor of the a_i. It follows that there is an ideal $\mathcal{B}$ of finite index in Λ such that $\mathcal{B}c \in \mathrm{Ind}(c)H^1(\mathbf{Q}, \mathbf{T})$.

If $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbf{T})$ (or $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(\mathbf{T})$) we will write $\mathrm{Ind}(\boldsymbol{\kappa}) = \mathrm{Ind}(\kappa_1)$.

DEFINITION 5.3.9. If $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbf{T})$, we will say that $\boldsymbol{\kappa}$ is Λ-*primitive* if the blind spot of $\boldsymbol{\kappa}$ (see Definition 3.1.6) contains no height-one primes of Λ.

This is not in general the same as being primitive (Definition 4.5.5), which requires that the image of $\boldsymbol{\kappa}$ be nonzero in $\mathbf{KS}(\bar{T})$.

Let $X_\infty = \mathrm{Hom}(H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*), \mathbf{Q}_p/\mathbf{Z}_p)$.

THEOREM 5.3.10. *Suppose* $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbf{T})$.

(i) $\mathrm{char}(X_\infty)$ *divides* $\mathrm{Ind}(\boldsymbol{\kappa})$.
(ii) *If* $\chi(\mathbf{T}) = 1$, $\kappa_1 \neq 0$, *and* $\mathfrak{P}$ *is is a height-one prime of* Λ *not in the blind spot of* $\boldsymbol{\kappa}$, *then* $\mathrm{ord}_{\mathfrak{P}}(\mathrm{char}(X_\infty)) = \mathrm{ord}_{\mathfrak{P}}(\mathrm{Ind}(\boldsymbol{\kappa}))$.
(iii) *If* $\chi(\mathbf{T}) = 1$, $\kappa_1 \neq 0$, *and* $\boldsymbol{\kappa}$ *is* Λ*-primitive then* $\mathrm{char}(X_\infty) = \mathrm{Ind}(\boldsymbol{\kappa})$.

REMARK 5.3.11. Theorems 5.3.6 and 5.3.10 remain true (with the same proofs) if $\mathbf{KS}(\mathbf{T})$ is replaced by $\widetilde{\mathbf{KS}}(\mathbf{T})$. This is useful when starting with an Euler system and applying Theorem 5.3.3. For simplicity we will give the proof only for $\mathbf{KS}(\mathbf{T})$.

Theorem 5.3.10 can be used to prove "main conjectures". See the examples of §§6.1 and 6.2.

The rest of this section is devoted to the proofs of Theorems 5.3.6 and 5.3.10. We will apply the results of §5.2 to quotients $\mathbf{T}/\mathfrak{P}\mathbf{T}$ for appropriate primes $\mathfrak{P}$ of Λ, and deduce the desired results about $\mathbf{T}$.

Suppose $\mathfrak{P}$ is a height-one prime ideal of Λ. Let $S_{\mathfrak{P}}$ denote the integral closure of $\Lambda/\mathfrak{P}$. Then $S_{\mathfrak{P}}$ is a discrete valuation ring, $[S_{\mathfrak{P}} : \Lambda/\mathfrak{P}]$ is finite, and $\mathbf{T} \otimes_\Lambda S_{\mathfrak{P}} = T \otimes_{\mathbf{Z}_p} S_{\mathfrak{P}}$. We will study Kolyvagin systems on $\mathbf{T}$ by studying their images in $\mathbf{KS}(T \otimes S_{\mathfrak{P}})$, and applying the results of §5.2 to the latter. We will make frequent use of the exact sequence, obtained by fixing a generator ρ of $\mathfrak{P}$,

$$0 \longrightarrow \mathbf{T} \xrightarrow{\rho} \mathbf{T} \longrightarrow \mathbf{T}/\mathfrak{P}\mathbf{T} \longrightarrow 0. \tag{13}$$

As in Definition 3.2.1, we have a canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on $T \otimes S_{\mathfrak{P}}$ given by

- $\Sigma(\mathcal{F}_{\mathrm{can}}) = \{\ell : T \text{ is ramified at } \ell\} \cup \{p, \infty\}$,
- if $\ell \in \Sigma(\mathcal{F}_{\mathrm{can}})$ and $\ell \neq p, \infty$ then

$$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, T \otimes S_{\mathfrak{P}}) = \ker[H^1(\mathbf{Q}_\ell, T \otimes S_{\mathfrak{P}}) \to H^1(\mathbf{Q}_\ell^{\mathrm{unr}}, T \otimes \mathrm{Frac}(S_{\mathfrak{P}}))],$$

- $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_p, T \otimes S_{\mathfrak{P}}) = H^1(\mathbf{Q}_p, T \otimes S_{\mathfrak{P}})$,
- $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{R}, T \otimes S_{\mathfrak{P}}) = H^1(\mathbf{R}, T \otimes S_{\mathfrak{P}})$,

where $\mathrm{Frac}(S_{\mathfrak{P}})$ is the field of fractions of $S_{\mathfrak{P}}$.

DEFINITION 5.3.12. Define an exceptional set of height-one primes of Λ by

$$\Sigma_\Lambda = \{\mathfrak{P} : H^2(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T})[\mathfrak{P}] \text{ is infinite}\} \cup \{\mathfrak{P} : H^2(\mathbf{Q}_p, \mathbf{T})[\mathfrak{P}] \text{ is infinite}\} \cup \{p\Lambda\}.$$

It follows from Lemma 5.3.4 that Σ_Λ is finite.

LEMMA 5.3.13. *Suppose* $\mathfrak{P}$ *is a height-one prime ideal of* Λ. *The inclusion*

$$\mathbf{T}/\mathfrak{P}\mathbf{T} = T \otimes (\Lambda/\mathfrak{P}) \hookrightarrow T \otimes S_{\mathfrak{P}}$$

induces maps

$$H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_v, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_v, T \otimes S_{\mathfrak{P}}),$$
$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_v, (T \otimes S_{\mathfrak{P}})^*) \to H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}_v, (\mathbf{T}/\mathfrak{P}\mathbf{T})^*),$$

for every place v. *If* $\mathfrak{P} \notin \Sigma_\Lambda$, *then the kernels and cokernels of these maps are finite with order bounded by a constant depending only on* T *and* $[S_{\mathfrak{P}} : \Lambda/\mathfrak{P}]$.

PROOF. First suppose that v is a prime $\ell \neq p$, and let $\mathcal{I}$ be the inertia group of ℓ. By definition, $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T})$ is the image of $H^1(\mathbf{Q}_\ell, \mathbf{T})$ in $H^1(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T})$.

Using Lemma 5.3.1(ii) for the first equality, the map $H^1(\mathbf{Q}_\ell, \mathbf{T}) \to H^1(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T})$ factors through

$$H^1(\mathbf{Q}_\ell, \mathbf{T}) = H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, \mathbf{T}^{\mathcal{I}}) \to H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, \mathbf{T}^{\mathcal{I}}/\mathfrak{P}\mathbf{T}^{\mathcal{I}}) \\ \to H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, (\mathbf{T}/\mathfrak{P}\mathbf{T})^{\mathcal{I}}) = H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T}). \quad (14)$$

Hence $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T}) \subset H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T})$, and so the image of $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T})$ in $H^1(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P})$ is contained in $H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P})$. By definition this is a submodule of $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P})$, so we obtain the desired map

$$H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T}) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P}). \quad (15)$$

The kernel of $H^1(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P})$ is a quotient of $H^0(\mathbf{Q}_\ell, T \otimes (S_\mathfrak{P}/(\Lambda/\mathfrak{P})))$, which has order bounded by $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]^{\mathrm{rank}_{\mathbf{Z}_p} T}$. Hence the same bound holds for the kernel of (15).

We now consider the cokernel of (15). In (14), the map

$$H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, \mathbf{T}^{\mathcal{I}}) \to H^1(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell, \mathbf{T}^{\mathcal{I}}/\mathfrak{P}\mathbf{T}^{\mathcal{I}})$$

is surjective because $\mathrm{Gal}(\mathbf{Q}_\ell^{\mathrm{unr}}/\mathbf{Q}_\ell)$ has cohomological dimension one. Taking $\mathcal{I}$-cohomology of (13) yields

$$0 \longrightarrow \mathbf{T}^{\mathcal{I}}/\mathfrak{P}\mathbf{T}^{\mathcal{I}} \longrightarrow (\mathbf{T}/\mathfrak{P}\mathbf{T})^{\mathcal{I}} \longrightarrow H^1(\mathcal{I}, \mathbf{T})[\mathfrak{P}] \longrightarrow 0.$$

Since $\ell \neq p$ the action of $\mathcal{I}$ on Λ is trivial, and since Λ is free over $\mathbf{Z}_p$ we get

$$H^1(\mathcal{I}, \mathbf{T})[\mathfrak{P}] = (H^1(\mathcal{I}, T) \otimes \Lambda)[\mathfrak{P}].$$

But $\mathfrak{P} \neq p\Lambda \in \Sigma_\Lambda$, so (recall that $\mathfrak{P}$ acts only on the second factor of this tensor product) $H^1(\mathcal{I}, T) \otimes \Lambda$ has no $\mathfrak{P}$-torsion. Thus the composition (14) is surjective.

The cokernel of $H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P})$ has order bounded by $|T \otimes (S_\mathfrak{P}/(\Lambda/\mathfrak{P}))|$. A straightforward diagram chase (see the proof of Lemma 1.3.5 of [**Ru6**]) shows that

$$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P})/H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T \otimes S_\mathfrak{P}) \cong H^1(\mathcal{I}, T \otimes S_\mathfrak{P})^{\mathrm{Fr}_\ell = 1}_{\mathrm{tors}}.$$

Since $\mathcal{I}$ acts trivially on the free $\mathbf{Z}_p$-module $S_\mathfrak{P}$, $H^1(\mathcal{I}, T \otimes S_\mathfrak{P}) = H^1(\mathcal{I}, T) \otimes S_\mathfrak{P}$ and $H^1(\mathcal{I}, T \otimes S_\mathfrak{P})_{\mathrm{tors}} = H^1(\mathcal{I}, T)_{\mathrm{tors}} \otimes S_\mathfrak{P}$. But $H^1(\mathcal{I}, T)_{\mathrm{tors}}$ is finite for every ℓ, so

$$|H^1(\mathcal{I}, T \otimes S_\mathfrak{P})^{\mathrm{Fr}_\ell = 1}_{\mathrm{tors}}| = |H^1(\mathcal{I}, T)_{\mathrm{tors}} \otimes S_\mathfrak{P} \otimes \Lambda/(\mathrm{Fr}_\ell - 1)\Lambda|.$$

Since $\Lambda/(\mathrm{Fr}_\ell - 1)\Lambda$ has finite $\mathbf{Z}_p$-rank, the right-hand side has finite order with a bound depending only on T and ℓ. If T is unramified at ℓ then $H^1(\mathcal{I}, T)_{\mathrm{tors}} = \mathrm{Hom}(\mathcal{I}, T)_{\mathrm{tors}} = 0$, and we conclude that the cokernel of (15) is finite with a bound depending only on T and $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]$.

Now consider the case $v = p$. Taking $G_{\mathbf{Q}_p}$-cohomology of the sequence (13) shows that the cokernel of $H^1(\mathbf{Q}_p, \mathbf{T}) \to H^1(\mathbf{Q}_p, \mathbf{T}/\mathfrak{P}\mathbf{T})$ is $H^2(\mathbf{Q}_p, \mathbf{T})[\mathfrak{P}]$. Since $\mathfrak{P} \notin \Sigma_\Lambda$, we have that $H^2(\mathbf{Q}_p, \mathbf{T})[\mathfrak{P}]$ is finite. Hence this cokernel is no bigger than the maximal finite submodule of the finitely-generated Λ-module $H^2(\mathbf{Q}_p, \mathbf{T})$, so $[H^1(\mathbf{Q}_p, \mathbf{T}/\mathfrak{P}\mathbf{T}) : H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_p, \mathbf{T}/\mathfrak{P}\mathbf{T})]$ is finite and independent of $\mathfrak{P}$.

By definition $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_p, T \otimes S_\mathfrak{P}) = H^1(\mathbf{Q}_p, T \otimes S_\mathfrak{P})$, so the first map of the lemma is just the composition

$$H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_p, \mathbf{T}/\mathfrak{P}\mathbf{T}) \hookrightarrow H^1(\mathbf{Q}_p, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1(\mathbf{Q}_p, T \otimes S_\mathfrak{P}).$$

The kernel and cokernel of the map $H^1(\mathbf{Q}_p, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1(\mathbf{Q}_p, T \otimes S_\mathfrak{P})$ are controlled by $H^i(\mathbf{Q}_p, T \otimes (S_\mathfrak{P}/(\Lambda/\mathfrak{P})))$ with $i = 0$ and 1, respectively, and these groups have bounds of the desired sort.

When $v = \infty$, it is straightforward to check that $H^1(\mathbf{R}, \mathbf{T}) \to H^1(\mathbf{R}, \mathbf{T}/\mathfrak{P}\mathbf{T})$ is surjective, so $H^1_{\mathcal{F}_\Lambda}(\mathbf{R}, \mathbf{T}/\mathfrak{P}\mathbf{T}) = H^1(\mathbf{R}, \mathbf{T}/\mathfrak{P}\mathbf{T})$, and then the kernel and cokernel of $H^1(\mathbf{R}, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1(\mathbf{R}, T \otimes S_\mathfrak{P})$ are bounded exactly as for $v = p$.

This gives the desired properties of the first map of the lemma for every v. The proof for the second map is similar (the "dual" of the proof above). □

Proposition 5.3.14. *For every height-one prime ideal $\mathfrak{P}$ of Λ, the composition $\mathbf{T} \twoheadrightarrow T \otimes (\Lambda/\mathfrak{P}) \hookrightarrow T \otimes S_\mathfrak{P}$ induces maps*

$$\pi_\mathfrak{P} : H^1(\mathbf{Q}, \mathbf{T})/\mathfrak{P}H^1(\mathbf{Q}, \mathbf{T}) \hookrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, T \otimes S_\mathfrak{P}),$$
$$\pi^*_\mathfrak{P} : H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, (T \otimes S_\mathfrak{P})^*) \to H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*)[\mathfrak{P}].$$

For every $\mathfrak{P}$ the map $\pi_\mathfrak{P}$ is injective. If $\mathfrak{P} \notin \Sigma_\Lambda$ then $\mathrm{coker}(\pi_\mathfrak{P})$, $\ker(\pi^*_\mathfrak{P})$, *and* $\mathrm{coker}(\pi^*_\mathfrak{P})$ *are all finite with order bounded by a constant depending only on T and $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]$.*

Proof. By Lemma 5.3.1(iii), $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T}) = H^1(\mathbf{Q}, \mathbf{T})$. Thus $\mathrm{Gal}(\mathbf{Q}_\Sigma/\mathbf{Q})$-cohomology of (13) yields an injective map

$$H^1(\mathbf{Q}, \mathbf{T})/\mathfrak{P}H^1(\mathbf{Q}, \mathbf{T}) \hookrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T}/\mathfrak{P}\mathbf{T}) \tag{16}$$

with cokernel $H^2(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T})[\mathfrak{P}]$. If $\mathfrak{P} \notin \Sigma_\Lambda$, then $H^2(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T})[\mathfrak{P}]$ is contained in the maximal finite submodule of the finitely-generated Λ-module $H^2(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T})$, so the cokernel of (16) is finite and bounded by a constant depending only on T.

The map

$$H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, \mathbf{T}/\mathfrak{P}\mathbf{T}) \longrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, T \otimes S_\mathfrak{P}) \tag{17}$$

has kernel and cokernel controlled by $H^i(\mathbf{Q}_\Sigma/\mathbf{Q}, T \otimes (S_\mathfrak{P}/(\Lambda/\mathfrak{P})))$ with $i = 0$ and 1, respectively.

The Λ-module $S_\mathfrak{P}/(\Lambda/\mathfrak{P})$ has a Jordan-Holder filtration in which all quotients are $\mathbf{Z}/p\mathbf{Z}$ (with trivial Galois action). Hence by Lemma 3.5.2,

$$H^0(\mathbf{Q}_\Sigma/\mathbf{Q}, T \otimes (S_\mathfrak{P}/(\Lambda/\mathfrak{P}))) = 0,$$

so (17) is injective. On the other hand, $H^1(\mathbf{Q}_\Sigma/\mathbf{Q}, T \otimes (S_\mathfrak{P}/(\Lambda/\mathfrak{P})))$ is finite with order bounded by a function of $\mathrm{rank}_{\mathbf{Z}_p} T$, $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]$, and Σ. Thus the cokernel of (17) is bounded in terms of T and $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]$.

Lemma 5.3.13 shows that (17) restricts to a (still injective) map

$$H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}, \mathbf{T}/\mathfrak{P}\mathbf{T}) \hookrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, T \otimes S_\mathfrak{P}). \tag{18}$$

It follows from the bounds on the kernels and cokernels in Lemma 5.3.13 that the cokernel of (18) is finite with order bounded by a constant depending only on T and $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]$. The map $\pi_\mathfrak{P}$ is the composition of (16) and (18), so combining the observations above we get the desired properties of $\ker(\pi_\mathfrak{P})$ and $\mathrm{coker}(\pi_\mathfrak{P})$.

The map $\pi^*_\mathfrak{P}$ and the bounds on its kernel and cokernel follow from Lemma 5.3.13 in the same way, using Lemma 3.5.3 as well to identify $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*[\mathfrak{P}])$ with $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*)[\mathfrak{P}]$. □

Corollary 5.3.15. *For every height-one prime $\mathfrak{P}$ of Λ, there is a natural map*

$$\mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda) \to \mathbf{KS}(T \otimes S_\mathfrak{P}, \mathcal{F}_{\mathrm{can}}).$$

PROOF. We have maps $\mathbf{KS}(\mathbf{T},\mathcal{F}_\Lambda) \to \mathbf{KS}(\mathbf{T}/\mathfrak{P}\mathbf{T},\mathcal{F}_\Lambda) \to \mathbf{KS}(T\otimes S_\mathfrak{P},\mathcal{F}_{\mathrm{can}})$, the first by functoriality (Remark 3.1.4) and the second by Lemma 5.3.13. □

LEMMA 5.3.16. *If $\mathfrak{P}$ is a height-one prime of Λ, and $\mathfrak{P}\notin\Sigma_\Lambda$, then*

$$\chi(T\otimes S_\mathfrak{P},\mathcal{F}_{\mathrm{can}}) = \mathrm{rank}_{\mathbf{Z}_p} T^-$$

where T^- is the minus part of T for complex conjugation.

PROOF. By Theorem 5.2.15,

$$\chi(T\otimes S_\mathfrak{P}) = \mathrm{rank}_{S_\mathfrak{P}}(T\otimes S_\mathfrak{P})^- + \mathrm{corank}_{S_\mathfrak{P}} H^0(\mathbf{Q}_p,(T\otimes S_\mathfrak{P})^*)$$

where $(T\otimes S_\mathfrak{P})^-$ is the minus part of $T\otimes S_\mathfrak{P}$ for complex conjugation. But $(T\otimes S_\mathfrak{P})^- = T^-\otimes S_\mathfrak{P}$, so $\mathrm{rank}_{S_\mathfrak{P}}(T\otimes S_\mathfrak{P})^- = \mathrm{rank}_{\mathbf{Z}_p}T^-$. Further, $H^0(\mathbf{Q}_p,(\mathbf{T}/\mathfrak{P}\mathbf{T})^*)$ is dual to $H^2(\mathbf{Q}_p,\mathbf{T}/\mathfrak{P}\mathbf{T})$, and $H^2(\mathbf{Q}_p,\mathbf{T}/\mathfrak{P}\mathbf{T}) \cong H^2(\mathbf{Q}_p,\mathbf{T})/\mathfrak{P}H^2(\mathbf{Q}_p,\mathbf{T})$ because $G_{\mathbf{Q}_p}$ has cohomological dimension 2. Since $H^2(\mathbf{Q}_p,\mathbf{T})$ is a finitely-generated torsion Λ-module (Lemma 5.3.4) and $\mathfrak{P}\notin\Sigma_\Lambda$, we see that $H^2(\mathbf{Q}_p,\mathbf{T})/\mathfrak{P}H^2(\mathbf{Q}_p,\mathbf{T})$ is finite. Hence $H^0(\mathbf{Q}_p,(T\otimes S_\mathfrak{P})^*)$ is finite as well, and this proves the lemma. □

DEFINITION 5.3.17. We define $\chi(\mathbf{T})$ to be the common value (by Lemma 5.3.16) of $\chi(T\otimes S_\mathfrak{P},\mathcal{F}_{\mathrm{can}})$ for $\mathfrak{P}\notin\Sigma_\Lambda$. Equivalently, $\chi(\mathbf{T}) = \mathrm{rank}_{\mathbf{Z}_p}T^-$.

REMARK 5.3.18. By Proposition 1.3.2 of [**PR3**], if the weak Leopoldt conjecture holds for T then $\mathrm{rank}_\Lambda H^1(\mathbf{Q},\mathbf{T}) = \chi(\mathbf{T})$.

If $\boldsymbol{\kappa}\in\mathbf{KS}(\mathbf{T})$ and $\mathfrak{P}$ is a height-one prime of Λ, let $\boldsymbol{\kappa}^{(\mathfrak{P})}$ denote the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T\otimes S_\mathfrak{P},\mathcal{F}_{\mathrm{can}})$ under the map of Corollary 5.3.15.

COROLLARY 5.3.19. *Suppose $\boldsymbol{\kappa}\in\mathbf{KS}(\mathbf{T})$ and $\kappa_1\neq 0$. Then for all but finitely many height-one primes $\mathfrak{P}$ of Λ, the class $\kappa_1^{(\mathfrak{P})}\in H^1(\mathbf{Q},T\otimes S_\mathfrak{P})$ is nonzero.*

PROOF. Since κ_1 is a nonzero element of the finitely-generated torsion-free (Lemma 5.3.5) Λ-module $H^1(\mathbf{Q},\mathbf{T})$, there are only finitely many height-one primes $\mathfrak{P}$ such that $\kappa_1\in\mathfrak{P}H^1(\mathbf{Q},\mathbf{T})$. Thus the corollary follows from the injectivity of the map $\pi_\mathfrak{P}$ in Proposition 5.3.14. □

LEMMA 5.3.20. *Suppose $\boldsymbol{\kappa}\in\mathbf{KS}(\mathbf{T})$ and $\mathfrak{P}$ is a height-one prime of Λ, and $\mathfrak{P}$ is not in the blind spot of $\boldsymbol{\kappa}$. Then $\boldsymbol{\kappa}^{(\mathfrak{P})}\neq 0$.*

PROOF. Write $T_\mathfrak{P} = \mathbf{T}/\mathfrak{P}\mathbf{T}$. Fix nonzero elements $\alpha,\beta\in\Lambda/\mathfrak{P}$ such that $\alpha S_\mathfrak{P}\subset\Lambda/\mathfrak{P}$ and the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T_\mathfrak{P}/\beta T_\mathfrak{P},\mathcal{P}_j)$ is nonzero for every j. In particular (taking j such that $\mathfrak{m}^j(\Lambda/\mathfrak{P})\subset\alpha\beta(\Lambda/\mathfrak{P})$) we can find an $n\in\mathcal{N}_j$ such that $I_n(\Lambda/\mathfrak{P})\subset\alpha\beta(\Lambda/\mathfrak{P})$ and the image of κ_n in $H^1(\mathbf{Q},T_\mathfrak{P}/\beta T_\mathfrak{P})\otimes G_n$ is nonzero.

Since $\mathfrak{P}$ is prime, we have an injection $T_\mathfrak{P}/\beta T_\mathfrak{P} \xrightarrow{\alpha} T_\mathfrak{P}/\alpha\beta T_\mathfrak{P}$ and hence (by Lemma 3.5.2) an injection $H^1(\mathbf{Q},T_\mathfrak{P}/\beta T_\mathfrak{P}) \xrightarrow{\alpha} H^1(\mathbf{Q},T_\mathfrak{P}/\alpha\beta T_\mathfrak{P})$. Thus the image of $\alpha\kappa_n$ in $H^1(\mathbf{Q},T_\mathfrak{P}/\alpha\beta T_\mathfrak{P})\otimes G_n$ is nonzero. From the composition

$$H^1(\mathbf{Q},T_\mathfrak{P}/\alpha\beta T_\mathfrak{P}) \to H^1(\mathbf{Q},(T\otimes S_\mathfrak{P})/\alpha\beta(T\otimes S_\mathfrak{P})) \xrightarrow{\alpha} H^1(\mathbf{Q},T_\mathfrak{P}/\alpha\beta T_\mathfrak{P})$$

we conclude that the image of κ_n in $H^1(\mathbf{Q},(T\otimes S_\mathfrak{P})/\alpha\beta(T\otimes S_\mathfrak{P}))\otimes G_n$ is nonzero, and so $\boldsymbol{\kappa}^{(\mathfrak{P})}\neq 0$. □

PROOF OF THEOREM 5.3.6. By Corollary 5.3.19 we can choose a height-one prime $\mathfrak{P}$ of Λ such that $\mathfrak{P}\notin\Sigma_\Lambda$ and $\kappa_1^{(\mathfrak{P})}\neq 0$.

Applying Theorem 5.2.2 to $\boldsymbol{\kappa}^{(\mathfrak{P})}$ shows that $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q},(T\otimes S_{\mathfrak{P}})^*)$ is finite, and then Proposition 5.3.14 shows that $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q},\mathbf{T}^*)[\mathfrak{P}]$ is finite. But $\Lambda^*[\mathfrak{P}]=(\Lambda/\mathfrak{P})^*$ is infinite, and so $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q},\mathbf{T}^*)$ must be co-torsion. □

Proof of Theorem 5.3.10. If $\kappa_1=0$ then $\mathrm{Ind}(\boldsymbol{\kappa})=0$ and there is nothing to prove. So we assume from now on that $\kappa_1\neq 0$.

Fix a height-one prime $\mathfrak{P}$ of Λ, and suppose first that $\mathfrak{P}\neq p\Lambda$. For convenience we identify Λ with the power series ring $\mathbf{Z}_p[[U]]$, and we fix a generator $\rho(U)$ of $\mathfrak{P}$ which is a distinguished polynomial (a monic polynomial congruent to $U^{\deg(\rho)}$ modulo p). For every N let

$$\mathfrak{P}_N=(\rho(U)+p^N)\Lambda.$$

Since $\mathfrak{P}\neq p\Lambda$, the $\mathfrak{P}_N$ are distinct ideals of Λ, and different from $\mathfrak{P}$.

Fix a pseudo-isomorphism

$$X_\infty\longrightarrow\bigoplus_i(\Lambda/\mathfrak{P}^{m_i})\bigoplus_j(\Lambda/f_j\Lambda) \tag{19}$$

where each f_j is prime to $\mathfrak{P}$. In particular $\mathrm{ord}_{\mathfrak{P}}(\mathrm{char}(X_\infty))=\sum_i m_i$.

We first claim that if N is sufficiently large, then $\mathfrak{P}_N$ satisfies the following properties:

(i) $\mathfrak{P}_N$ is a prime ideal and $\Lambda/\mathfrak{P}\cong\Lambda/\mathfrak{P}_N$,
(ii) the image of κ_1 in $H^1(\mathbf{Q},T\otimes S_{\mathfrak{P}_N})$ is nonzero,
(iii) the cokernel of the injection

$$H^1(\mathbf{Q},\mathbf{T})/\mathfrak{P}_NH^1(\mathbf{Q},\mathbf{T})\hookrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q},T\otimes S_{\mathfrak{P}_N})$$

is finite with order bounded by a constant independent of N,
(iv) $\mathfrak{P}_N$ is prime to each f_j in (19), and $\mathfrak{P}_N\notin\Sigma_\Lambda$.

It follows without difficulty from Hensel's Lemma that the first property holds for N sufficiently large. The second property holds for all but finitely many N by Corollary 5.3.19, and the third holds for all but finitely many N by Proposition 5.3.14 (and using property (i)). The fourth property clearly holds for all but finitely many N.

Fix an N large enough so that these properties hold, write $\mathfrak{Q}=\mathfrak{P}_N$, and let $\boldsymbol{\kappa}^{(\mathfrak{Q})}$ denote the image of $\boldsymbol{\kappa}$ in $\mathbf{KS}(T\otimes S_{\mathfrak{Q}},\mathcal{F}_{\mathrm{can}})$. We will apply the results of §5.2 to $\boldsymbol{\kappa}^{(\mathfrak{Q})}$.

Let $d=\mathrm{ord}_{\mathfrak{P}}(\mathrm{Ind}(\boldsymbol{\kappa}))$, and let e be the ramification degree of $S_{\mathfrak{Q}}/\mathbf{Z}_p$. Since $\Lambda/(\mathfrak{P}^d,\mathfrak{Q})=\Lambda/(\mathfrak{Q},p^{Nd})$, it follows from (ii) and (iii) above that $|\partial^{(0)}(\boldsymbol{\kappa}^{(\mathfrak{Q})})-Nde|$ is bounded independently of N. Hence by Theorem 5.2.2 (writing $O(1)$ for an integer bounded independently of N)

$$\mathrm{length}_{S_{\mathfrak{Q}}}H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q},(T\otimes S_{\mathfrak{Q}})^*)\leq Ne\,\mathrm{ord}_{\mathfrak{P}}(\mathrm{Ind}(\boldsymbol{\kappa}))+O(1), \tag{20}$$

and so by Proposition 5.3.14, writing $r=\mathrm{rank}_{\mathbf{Z}_p}S_{\mathfrak{Q}}$,

$$\mathrm{length}_{\mathbf{Z}_p}H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q},\mathbf{T}^*)[\mathfrak{Q}]\leq Nr\,\mathrm{ord}_{\mathfrak{P}}(\mathrm{Ind}(\boldsymbol{\kappa}))+O(1).$$

On the other hand, using (19),

$$\begin{aligned}\operatorname{length}_{\mathbf{Z}_p} H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q},\mathbf{T}^*)[\mathfrak{Q}] &= \operatorname{length}_{\mathbf{Z}_p}(X_\infty/\mathfrak{Q}X_\infty)\\ &= \sum_i \operatorname{length}_{\mathbf{Z}_p}\Lambda/(\mathfrak{P}^{m_i},\mathfrak{Q}) + O(1)\\ &= \sum_i \operatorname{length}_{\mathbf{Z}_p}\Lambda/(\mathfrak{Q},p^{Nm_i}) + O(1)\\ &= Nr\sum_i m_i + O(1) = Nr\,\operatorname{ord}_{\mathfrak{P}}(\operatorname{char}(X_\infty)) + O(1),\end{aligned}$$

so taking N sufficiently large shows that $\operatorname{ord}_{\mathfrak{P}}(\operatorname{char}(X_\infty)) \le \operatorname{ord}_{\mathfrak{P}}(\operatorname{Ind}(\boldsymbol{\kappa}))$. Since $\mathfrak{P}$ was arbitrary, this proves (i).

Now suppose further that $\chi(\mathbf{T}) = 1$ and $\mathfrak{P}$ is not in the blind spot of $\boldsymbol{\kappa}$. Let $\mathfrak{m}_\mathfrak{P}$ and $\mathfrak{m}_\mathfrak{Q}$ denote the maximal ideals of $S_\mathfrak{P}$ and $S_\mathfrak{Q}$, respectively. By Lemma 5.3.20, there is an n such that the image of κ_n in $H^1(\mathbf{Q},(T\otimes S_\mathfrak{P})/I_n(T\otimes S_\mathfrak{P}))$ is nonzero. Fix k such that $I_nS_\mathfrak{P} \subset \mathfrak{m}_\mathfrak{P}^k S_\mathfrak{P}$ and such that the image of κ_n in $H^1(\mathbf{Q},(T\otimes S_\mathfrak{P})/\mathfrak{m}_\mathfrak{P}^k(T\otimes S_\mathfrak{P}))$ is nonzero (we can suppose $I_nS_\mathfrak{P} = \mathfrak{m}_\mathfrak{P}^k S_\mathfrak{P}$ unless $I_nS_\mathfrak{P} = 0$).

Suppose N is large enough so that properties (i) through (iv) above hold, and in addition $N > k$. Then $(T\otimes S_\mathfrak{Q})/\mathfrak{m}_\mathfrak{Q}^k(T\otimes S_\mathfrak{Q}) \cong (T\otimes S_\mathfrak{P})/\mathfrak{m}_\mathfrak{P}^k(T\otimes S_\mathfrak{P})$ so the image of κ_n in $H^1(\mathbf{Q},(T\otimes S_\mathfrak{Q})/\mathfrak{m}_\mathfrak{Q}^k(T\otimes S_\mathfrak{Q}))$ is nonzero. In particular $\partial^{(\infty)}(\boldsymbol{\kappa}^{(\mathfrak{Q})}) < k$. By Lemma 5.3.16 we have $\chi(T\otimes S_\mathfrak{P},\mathcal{F}_{\mathrm{can}}) = \chi(\mathbf{T}) = 1$, so Theorem 5.2.12(vii) shows that equality holds in (20). With this equality the argument above shows that $\operatorname{ord}_{\mathfrak{P}}(\operatorname{char}(X_\infty)) = \operatorname{ord}_{\mathfrak{P}}(\operatorname{Ind}(\boldsymbol{\kappa}))$.

This proves what we need for primes $\mathfrak{P} \ne p\Lambda$. When $\mathfrak{P} = p\Lambda$, we can repeat the argument above with $\mathfrak{P}_N = (U^N + p)\Lambda$, to obtain the same result. Combining all of this information proves the theorem. □

We end this section with some questions and speculation.

Recall the module of Euler systems $\mathbf{ES}(T) = \mathbf{ES}(T,\mathcal{P})$ given by Definition 3.2.2. The natural action of $G_\mathbf{Q}$ on $H^1(F,T)$ for finite abelian extensions F of $\mathbf{Q}$ gives an action of $G_\mathbf{Q}^{\mathrm{ab}}$ on $\mathbf{ES}(T)$. Further, $H^1(\mathbf{Q},\mathbf{T})$ and all of the $H^1(\mathbf{Q},\mathbf{T}/I_n\mathbf{T})$ have a natural Λ-module structure induced by the Λ-module structure on $\mathbf{T}$ (alternatively this action can be defined using Lemma 5.3.1(i)), so $\mathbf{KS}(\mathbf{T})$ also has a $G_\mathbf{Q}^{\mathrm{ab}}$ action which factors through $\operatorname{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$.

Let $\mathcal{A}$ be the kernel of the restriction map $\mathbf{Z}_p[[G_\mathbf{Q}^{\mathrm{ab}}]] \to \Lambda$. Since $\mathcal{A}$ annihilates $\overline{\mathbf{KS}}(\mathbf{T})$, $\mathcal{A}\mathbf{ES}(T)$ maps to zero under the Euler-system-to-Kolyvagin-system map of Theorem 5.3.3. Consider the composition

$$\psi : \mathbf{ES}(T)/\mathcal{A}\mathbf{ES}(T) \xrightarrow{\psi_{\mathrm{EK}}} \overline{\mathbf{KS}}(\mathbf{T}) \xrightarrow{\psi_1} H^1(\mathbf{Q},\mathbf{T})$$

where ψ_{EK} is the map induced by Theorem 5.3.3, and $\psi_1(\boldsymbol{\kappa}) = \kappa_1$. Then $\psi(\mathbf{c}) = \{c_{\mathbf{Q}_n}\}$, and all of these maps are Λ-module homomorphisms.

Question 5.3.21. *Is ψ injective?*

Even in the basic examples we do do not know the answer to this question. Assuming the weak Leopoldt conjecture for T, we have (Proposition 1.3.2 of [**PR3**]) that $\operatorname{rank}_\Lambda H^1(\mathbf{Q},\mathbf{T}) = \chi(\mathbf{T})$. In many examples (see §6.1 and §6.2) we have that $\chi(\mathbf{T}) = 1$, and in some of those examples we know that the image of ψ is free of rank one, and we know an Euler system $\mathbf{c}$ such that $\psi(\mathbf{c})$ generates the image of ψ.

If ψ were injective, it would follow that $\mathbf{ES}(T)/\mathcal{A}\mathbf{ES}(T)$ would be free of rank one over Λ, and therefore (Nakayama's Lemma) $\mathbf{ES}(T)$ would be cyclic over $\mathbf{Z}_p[[G_{\mathbf{Q}}^{\mathrm{ab}}]]$, generated by $\mathbf{c}$.

Assuming a conjecture of Greenberg [**Gr1**] and using a result of Seo (Theorem C of [**Seo**]), it is possible to show that ψ is injective for the cyclotomic unit Euler system discussed in §6.1 below.

QUESTION 5.3.22. *Is ψ_{EK} surjective?*

In other words, does every Kolyvagin system for $\mathbf{T}$ come from an Euler system? Again, this seems to be very difficult.

QUESTION 5.3.23. *Is ψ_1 injective?*

The analogous map $\mathbf{KS}(\bar{T}) \to H^1_{\mathcal{F}}(\mathbf{Q}, \bar{T})$ is not injective if $\chi(\bar{T}) > 1$ (see Remark 5.1.2). However, the construction that leads to Remark 5.1.2 does not work over Λ.

Note that if the answers to Questions 5.3.21 and 5.3.22 are "yes", then the answer to Question 5.3.23 is also "yes".

QUESTION 5.3.24. *What is the image of ψ?*

Let $\overline{H^1(\mathbf{Q}, \mathbf{T})}$ denote the double Λ-dual $\mathrm{Hom}(\mathrm{Hom}(H^1(\mathbf{Q}, \mathbf{T}), \Lambda), \Lambda)$. Then $\overline{H^1(\mathbf{Q}, \mathbf{T})}$ is a free Λ-module and there is a natural injection $H^1(\mathbf{Q}, \mathbf{T}) \hookrightarrow \overline{H^1(\mathbf{Q}, \mathbf{T})}$ (since $H^1(\mathbf{Q}, \mathbf{T})$ is torsion-free) with finite cokernel. Let $\overline{\psi}$ denote the composition of ψ with this inclusion.

It follows from Theorem 5.3.10 that $\mathrm{image}(\overline{\psi}) \subset \mathrm{char}(X_\infty)\overline{H^1(\mathbf{Q}, \mathbf{T})}$.

When $\chi(\mathbf{T}) = 1$, conjecturally we have $\mathrm{rank}_\Lambda H^1(\mathbf{Q}, \mathbf{T}) = 1$ and it seems reasonable to hope that $\mathrm{image}(\overline{\psi}) = \mathrm{char}(X_\infty)\overline{H^1(\mathbf{Q}, \mathbf{T})}$. If the weak Leopoldt conjecture holds for T and $\mathbf{KS}(\mathbf{T})$ contains a Λ-primitive Kolyvagin system, then this equality follows from Theorem 5.3.10. Both of these conditions do hold in many examples, see §6.1.

When $\chi(\mathbf{T}) > 1$, it is less clear what to expect. The simplest answer would be $\mathrm{image}(\overline{\psi}) = \mathrm{char}(X_\infty)\overline{H^1(\mathbf{Q}, \mathbf{T})}$; some evidence for this can be found in §6 of [**Ru4**]. But at present there are no well-understood examples with $\chi(\mathbf{T}) > 1$.

CHAPTER 6

Examples

6.1. The multiplicative group

For this section fix a character $\rho : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ of finite order. Assume that $p > 2$, so that the order of ρ is prime to p. Let L be the cyclic extension of $\mathbf{Q}$ which is the fixed field of ρ, and $\Delta = \mathrm{Gal}(L/\mathbf{Q})$. If M is a $\mathbf{Z}_p[\Delta]$-module, then M^ρ will denote the submodule of M on which Δ acts via ρ.

First, suppose $k \in \mathbf{Z}^+$, and let $R = \mathbf{Z}/p^k\mathbf{Z}$ and $T = \boldsymbol{\mu}_{p^k} \otimes \rho^{-1}$, a one-dimensional representation with $G_{\mathbf{Q}}$ acting via the product of ρ^{-1} and the cyclotomic character.

We have

$$H^1(\mathbf{Q}, T) = H^1(\mathbf{Q}, \boldsymbol{\mu}_{p^k} \otimes \rho^{-1}) \cong (H^1(L, \boldsymbol{\mu}_{p^k}) \otimes \rho^{-1})^\Delta \cong (L^\times/(L^\times)^{p^k})^\rho, \quad (21)$$

the last isomorphism depending on a choice of generator of the free rank-one R-module ρ^{-1}. Similarly for every prime ℓ we have

$$H^1(\mathbf{Q}_\ell, T) \cong (L_\ell^\times/(L_\ell^\times)^{p^k})^\rho, \quad (22)$$

where $L_\ell = L \otimes \mathbf{Q}_\ell$ is the sum of the completions of L at primes above ℓ.

The dual representation $T^* = \mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty})$ is a one-dimensional representation with $G_{\mathbf{Q}}$ acting via ρ. We have

$$H^1(\mathbf{Q}, T^*) \cong (H^1(L, \mathbf{Z}/p^k\mathbf{Z}) \otimes \rho)^\Delta = \mathrm{Hom}(G_L, \mathbf{Z}/p^k\mathbf{Z})^{\rho^{-1}}, \quad (23)$$

the subgroup of $\mathrm{Hom}(G_L, \mathbf{Z}/p^k\mathbf{Z})$ on which $G_{\mathbf{Q}}$ acts via ρ^{-1}. Similarly for every prime ℓ we have

$$H^1(\mathbf{Q}_\ell, T^*) \cong (\bigoplus_{\lambda|\ell} \mathrm{Hom}(G_{L_\lambda}, \mathbf{Z}/p^k\mathbf{Z}))^{\rho^{-1}}. \quad (24)$$

Definition 6.1.1. Define a Selmer structure $\mathcal{F}$ by taking $\Sigma(\mathcal{F})$ to be the set of primes where ρ is ramified, together with p and ∞. For every prime $\ell \notin \Sigma(\mathcal{F})$ one can check that

$$H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T) \cong (\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^k})^\rho$$

under the identification (22), where $\mathcal{O}_{L,\ell} = \mathcal{O}_L \otimes \mathbf{Z}_\ell$. For primes $\ell \in \Sigma(\mathcal{F})$ we define $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) = (\mathcal{O}_{L,\ell}^\times/(\mathcal{O}_{L,\ell}^\times)^{p^k})^\rho$ as well. (Since $p > 2$, we have $H^1(\mathbf{R}, T) = 0$ so we can safely ignore the infinite place.)

Let $\mathcal{F}_{\mathrm{can}}$ be the "canonical" Selmer structure on T induced from $\mathbf{Z}_p(1) \otimes \rho^{-1}$ as in Definition 3.2.1. One can check ([**Ru6**] §1.6.C) that $\mathcal{F}_{\mathrm{can}}$ is obtained from $\mathcal{F}$ by relaxing the condition at p, i.e., $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_p, T) = H^1(\mathbf{Q}_p, T)$ and $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, T) = H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ for $\ell \neq p$.

The dual Selmer structure $\mathcal{F}^*$ is given as follows ([**Ru6**] §1.6.B). For every prime $\ell \notin \Sigma(\mathcal{F}^*) = \Sigma(\mathcal{F})$ we have

$$H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T^*) \cong \oplus_{\lambda|\ell}(\mathrm{Hom}(G_{L_\lambda}/\mathcal{I}_\lambda, \mathbf{Z}/p^k\mathbf{Z}))^{\rho^{-1}}$$

under the identification (24), where $\mathcal{I}_\lambda$ is the inertia group in G_{L_λ}. For primes $\ell \in \Sigma(\mathcal{F})$ we have $H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*) = (\oplus_{\lambda|\ell}\mathrm{Hom}(G_{L_\lambda}/\mathcal{I}_\lambda, \mathbf{Z}/p^k\mathbf{Z}))^{\rho^{-1}}$ as well.

The Selmer structure $\mathcal{F}^*_{\mathrm{can}}$ is obtained from $\mathcal{F}^*$ by strengthening the condition at p, i.e., $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_p, T^*) = 0$ and $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_\ell, T^*) = H^1_{\mathcal{F}^*}(\mathbf{Q}_\ell, T^*)$ for $\ell \neq p$.

LEMMA 6.1.2. *If $\rho(p) \neq 1$ then $\mathcal{F} = \mathcal{F}_{\mathrm{can}}$.*

PROOF. If ρ is nontrivial on the decomposition group of p, then it follows from (22) and (24) that $H^1(\mathbf{Q}_p, T)$ and $H^1(\mathbf{Q}_p, T^*)$ are both zero. □

PROPOSITION 6.1.3. *We have natural exact sequences*

$$0 \longrightarrow (\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^{p^k}))^\rho \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, T) \longrightarrow \mathrm{Cl}(L)[p^k]^\rho \longrightarrow 0$$
$$0 \longrightarrow (\mathcal{O}_L[1/p]^\times/(\mathcal{O}_L[1/p]^\times)^{p^k}))^\rho \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, T) \longrightarrow \mathrm{Cl}'(L)[p^k]^\rho \longrightarrow 0$$

and isomorphisms

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \cong \mathrm{Hom}(\mathrm{Cl}(L)^\rho, \mathbf{Z}/p^k\mathbf{Z}), \quad H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, T^*) \cong \mathrm{Hom}(\mathrm{Cl}'(L)^\rho, \mathbf{Z}/p^k\mathbf{Z})$$

where $\mathrm{Cl}(L)$ is the ideal class group of L, and $\mathrm{Cl}'(L)$ is $\mathrm{Pic}(\mathcal{O}_L[1/p])$, the quotient of $\mathrm{Cl}(L)$ by the classes of primes above p.

PROOF. From the definition of $\mathcal{F}$, under the identification (21) we have

$$H^1_{\mathcal{F}}(\mathbf{Q}, T) = \{x \in (L^\times/(L^\times)^{p^k})^\rho : \mathrm{ord}_\lambda(x) \equiv 0 \pmod{p^k} \text{ for every } \lambda\}.$$

This gives the first exact sequence of the proposition, where the map $H^1_{\mathcal{F}}(\mathbf{Q}, T) \to \mathrm{Cl}(L)[p^k]^\rho$ sends x to the class of an ideal $\mathfrak{a}$ such that $\mathfrak{a}^{p^k}$ is the ideal generated by (any representative of) x.

The second exact sequence is similar.

Under the identification (23), $H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*)$ consists of the unramified homomorphisms in $H^1(\mathbf{Q}, T^*)$, and $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, T^*)$ consists of those unramified homomorphisms which are trivial on the decomposition group at p, i.e.,

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) = \mathrm{Hom}(\mathrm{Cl}(L), \mathbf{Z}/p^k\mathbf{Z})^{\rho^{-1}},$$
$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, T^*) = \mathrm{Hom}(\mathrm{Cl}'(L), \mathbf{Z}/p^k\mathbf{Z})^{\rho^{-1}}.$$

This gives the rest of the proposition. □

Similarly if we take $R = \mathbf{Z}_p$ and $T = \mathbf{Z}_p(1) \otimes \rho^{-1}$ we get isomorphisms

$$H^1_{\mathcal{F}}(\mathbf{Q}, T) \cong (\mathcal{O}_L^\times \otimes \mathbf{Z}_p)^\rho, \quad H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, T) \cong (\mathcal{O}_L[1/p]^\times \otimes \mathbf{Z}_p)^\rho \tag{25}$$

since $\varprojlim_k \mathrm{Cl}(L)[p^k] = 0$, and

$$H^1_{\mathcal{F}^*}(\mathbf{Q}, T^*) \cong \mathrm{Hom}(\mathrm{Cl}(L)^\rho, \mathbf{Q}_p/\mathbf{Z}_p), \quad H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, T^*) \cong \mathrm{Hom}(\mathrm{Cl}'(L)^\rho, \mathbf{Q}_p/\mathbf{Z}_p). \tag{26}$$

DEFINITION 6.1.4. Take $\mathcal{P}$ to be the set of all primes different from p. Fix a collection $\{\zeta_n : n \in \mathbf{Z}^+\}$ such that ζ_n is a primitive n-th root of unity and $\zeta_{mn}^m = \zeta_n$ for every m and n. If F is a finite abelian extension of $\mathbf{Q}$ of conductor f, we define c_F to be the image of $\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{fp})/F}(\zeta_{fp} - 1)$ under the Kummer map

$$F^\times \hookrightarrow H^1(F, \mathbf{Z}_p(1)).$$

One can check without difficulty that this defines an Euler system in the sense of [**Ru6**] Chapter 2, the Euler system of cyclotomic units. To obtain an Euler system $\mathbf{c} \in \mathbf{ES}(\mathbf{Z}_p(1), \mathcal{P}, \mathbf{Q}^{\mathrm{ab}})$ satisfying Definition 3.2.2 we need to modify these units slightly (see Remark 3.2.3) as in [**Ru6**] §9.6.

By Remark 3.2.5, the Euler system $\mathbf{c}$ gives an Euler system $\mathbf{c}^\rho \in \mathbf{ES}(T, \mathcal{P}_\rho, \mathbf{Q}^{\mathrm{ab}})$ where $\mathcal{P}_\rho$ is the set of primes not dividing pm_ρ and m_ρ is the conductor of ρ. For r prime to m_ρ, using the identification (21), we have

$$c^\rho_{\mathbf{Q}(\boldsymbol{\mu}_r)} = \prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{rpm_\rho})/\mathbf{Q}(\boldsymbol{\mu}_r))} (\zeta_{rpm_\rho} - 1)^{\rho^{-1}(\delta)\delta}. \tag{27}$$

Hypotheses (a) and (b) of Theorem 3.2.4 are satisfied, and $H^0(\mathbf{Q}_p, T^*)$ is either zero (if $\rho(p) \neq 1$) or all of T^* (if $\rho(p) = 1$). Thus by Theorem 3.2.4, $\mathbf{c}^\rho$ gives rise to a Kolyvagin system $\boldsymbol{\kappa}^\rho \in \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_\rho)$ with

$$\kappa_1^\rho = c^\rho_{\mathbf{Q}} = \Big(\prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{m_\rho})/\mathbf{Q})} (\zeta_{m_\rho} - 1)^{\rho^{-1}(\delta)\delta} \Big)^{1-\rho^{-1}(p)}. \tag{28}$$

This will be trivial unless ρ is an even character and $\rho(p) \neq 1$.

There is no way to get something nontrivial when ρ is odd, because cyclotomic units have no "odd components". However, we can eliminate the assumption that $\rho(p) \neq 1$. Namely, if $\mathbf{Q}^{\mathrm{ab},p}$ denotes the maximal abelian extension of $\mathbf{Q}$ which is unramified at p, then we can define an Euler system $\bar{\mathbf{c}}^\rho \in \mathbf{ES}(T, \mathcal{P}_\rho, \mathbf{Q}^{\mathrm{ab},p})$ satisfying

$$\bar{c}^\rho_{\mathbf{Q}(\boldsymbol{\mu}_r)} = \prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{rm_\rho})/\mathbf{Q}(\boldsymbol{\mu}_r))} (\zeta_{rm_\rho} - 1)^{\rho^{-1}(\delta)\delta}$$

in place of (27). As long as $\rho \neq 1$ we get a Kolyvagin system $\boldsymbol{\kappa}^\rho \in \mathbf{ES}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_\rho)$ by Theorem 3.2.7.

Thus for every even nontrivial ρ we get a Kolyvagin system $\boldsymbol{\kappa}^\rho$ satisfying

$$\kappa_1^\rho = \prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{m_\rho})/\mathbf{Q})} (\zeta_{m_\rho} - 1)^{\rho^{-1}(\delta)\delta}, \tag{29}$$

and using the fact that ζ_f is a unit when f is not a prime power one can show that in fact $\boldsymbol{\kappa}^\rho \in \mathbf{KS}(T, \mathcal{F}, \mathcal{P}_\rho)$.

Let $\omega : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ denote the Teichmuller character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$.

LEMMA 6.1.5. *Suppose $\rho \neq 1$ and $\rho \neq \omega$. Then T satisfies hypotheses* (H.0), (H.1), (H.2), (H.3), *and* (H.4a) *of §3.5, and $\mathcal{F}$ and $\mathcal{F}_{\mathrm{can}}$ both satisfy* (H.6).

PROOF. Hypotheses (H.0) and (H.1) are trivially satisfied, and (H.2) holds with $\tau = 1$. If $\rho \neq 1$ and $\rho \neq \omega$, then (H.3) holds as well (note that since ρ has order prime to p, it is not congruent to either 1 or ω modulo p). Since ρ takes values in $\mathbf{Z}_p^\times$, ρ^2 cannot equal ω and therefore (H.4a) holds. Lemma 3.7.1 shows that (H.6) holds for $\mathcal{F}$ and $\mathcal{F}_{\mathrm{can}}$. □

PROPOSITION 6.1.6.

$$\chi(T,\mathcal{F}) = \begin{cases} 1 & \text{if } \rho \text{ is even, } \rho \neq 1, \\ 0 & \text{if } \rho \text{ is odd, } \rho \neq \omega \end{cases}$$

PROOF. From Theorem 4.1.13 and Proposition 6.1.3 we have (when $R = \mathbf{Z}/p^k\mathbf{Z}$)

$$k\chi(T,\mathcal{F}) = \text{length}(H^1_{\mathcal{F}}(\mathbf{Q},T)) - \text{length}(H^1_{\mathcal{F}^*}(\mathbf{Q},T^*)) = \text{length}(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^{p^k})^\rho$$

and the proposition follows. □

For $\chi(T,\mathcal{F}_{\text{can}})$ see Theorem 5.2.15.

The following result is the main application of the cyclotomic unit Kolyvagin system $\boldsymbol{\kappa}^\rho$. Originally known as the Gras conjecture, it was proved by the first author and Wiles in [**MW**]. The proof sketched here is essentially due to Kolyvagin ([**Ko**], see also [**Ru1**]).

THEOREM 6.1.7. *If ρ is an even character, and $\mathcal{C}_L \subset \mathcal{O}_L^\times$ denotes the subgroup of cyclotomic units of L, then*

$$|\text{Cl}(L)^\rho| = |\mathcal{O}_L^\times/\mathcal{C}_L|^\rho.$$

PROOF. Apply Corollary 5.2.13(ii) to the Kolyvagin system $\boldsymbol{\kappa}^\rho \in \mathbf{KS}(T,\mathcal{F},\mathcal{P}_\rho)$ satisfying (29). Equations (25) and (29) show that $\partial^{(0)}(\boldsymbol{\kappa}^\rho) = \text{length}((\mathcal{O}_L^\times/\mathcal{C}_L)^\rho)$, and together with (26) this yields

$$|\text{Cl}(L)^\rho| \leq |\mathcal{O}_L^\times/\mathcal{C}_L|^\rho.$$

By a standard method using the analytic class number formula, (see for example [**Ru1**] Theorem 4.2) this inequality for all ρ implies that equality must hold for all ρ. □

REMARK 6.1.8. The proof of Theorem 6.1.7 shows, using Corollary 5.2.13(ii), that $\boldsymbol{\kappa}^\rho$ is primitive.

Now take $R = \Lambda$, $T = \mathbf{Z}_p(1) \otimes \rho^{-1}$, and $\mathbf{T} = T \otimes \Lambda$ as in §5.3. By Theorem 5.3.3 the cyclotomic unit Euler system defined by (27) gives rise to a Kolyvagin system $\boldsymbol{\kappa}^{\rho,\infty} \in \overline{\mathbf{KS}}(\mathbf{T},\mathcal{F}_\Lambda)$ where $\mathcal{F}_\Lambda$ is the Selmer structure of Definition 5.3.2. We have

$$\kappa_1^{\rho,\infty} = \{c^\rho_{\mathbf{Q}_n}\} \in \varprojlim_n (L_n^\times)^\rho \subset H^1(\mathbf{Q},\mathbf{T})$$

where $L_n = L\mathbf{Q}_n$ and $c^\rho_{\mathbf{Q}_n} \in (L_n^\times)^\rho$ is given by

$$c^\rho_{\mathbf{Q}_n} = \prod_{\delta \in \text{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}m_\rho})/\mathbf{Q}_n)} (\zeta_{p^{n+1}m_\rho} - 1)^{\rho^{-1}(\delta)\delta}.$$

Applying the results of §5.3 to $\boldsymbol{\kappa}^{\rho,\infty}$ leads to the following theorem, equivalent to Iwasawa's "main conjecture" which was proved by the first author and Wiles in [**MW**]. Let $\mathcal{C}_n \subset \mathcal{O}_{L_n}^\times$ denote the group of cyclotomic units in L_n, and let $\mathcal{C}_\infty$ and $\mathcal{E}_\infty$ denote the inverse limits (with respect to norm maps) of the p-adic completions of the $\mathcal{C}_n$ and $\mathcal{O}_{L_n}^\times$, respectively.

THEOREM 6.1.9. *If ρ is an even character then*

$$\text{char}(\varprojlim_n (\text{Cl}(L_n)[p^\infty])^\rho) = \text{char}(\mathcal{E}_\infty^\rho/\mathcal{C}_\infty^\rho).$$

PROOF. Suppose first that $\rho(p) \neq 1$. Then $H^1(\mathbf{Q}, \mathbf{T}) = \mathcal{E}^\rho_\infty$ and $\kappa_1^{\rho,\infty}$ is a generator of $\mathcal{C}^\rho_\infty$, so

$$\mathrm{Ind}(\boldsymbol{\kappa}^{\rho,\infty}) = \mathrm{char}(\mathcal{E}^\rho_\infty/\mathcal{C}^\rho_\infty).$$

As in Proposition 6.1.3 (and using Lemma 6.1.2) we have

$$\mathrm{Hom}(H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*), \mathbf{Q}_p/\mathbf{Z}_p) = \varprojlim_n (\mathrm{Cl}(L_n)[p^\infty])^\rho.$$

It follows from Remark 6.1.8 that $\boldsymbol{\kappa}^{\rho,\infty}$ is Λ-primitive, so in this case the theorem follows directly from Theorem 5.3.10 (and Remark 5.3.11).

When $\rho(p) = 1$, the statements above still hold "up to" powers of the augmentation ideal $\mathcal{A}$ of Λ. But one can show that $\mathrm{char}(\varprojlim(\mathrm{Cl}(L_n)[p^\infty])^\rho)$ is not divisible by $\mathcal{A}$. See [**Ru6**] §3.2 for details.

Taking these facts into account, Theorem 5.3.10 (together with Remark 5.3.11) shows in this case that

$$\mathrm{char}(\varprojlim_n (\mathrm{Cl}(L_n)[p^\infty])^\rho) \text{ divides } \mathrm{char}(\mathcal{E}^\rho_\infty/\mathcal{C}^\rho_\infty).$$

Once again a standard argument using the analytic class number formula (see for example [**MW**] §1.6 or [**Ru1**] p. 414) allows us to turn this divisibility (for all ρ) into an equality. □

REMARK 6.1.10. When $\rho(p) \neq 1$, it follows from Remark 6.1.8 that the blind spot of $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is empty.

Suppose now that $\rho(p) = 1$. Let $\mathcal{A}$ denote the augmentation ideal of Λ, and $\boldsymbol{\kappa}^{\rho,\infty,\mathcal{A}}$ denote the image of $\boldsymbol{\kappa}^{\rho,\infty}$ in $\mathbf{KS}(\mathbf{T}/\mathcal{A}\mathbf{T}) = \mathbf{KS}(\mathbf{Z}_p(1) \otimes \rho^{-1})$. Then (28) shows that $\kappa_1^{\rho,\infty,\mathcal{A}}$ vanishes. But $\mathbf{KS}(\mathbf{Z}_p(1) \otimes \rho^{-1})$ is free of rank one over $\mathbf{Z}_p$ (Theorem 5.2.10(ii) and Proposition 6.1.6), and the Kolyvagin system $\boldsymbol{\kappa} \in \mathbf{KS}(\mathbf{Z}_p(1) \otimes \rho^{-1})$ of Definition 6.1.4 has nonvanishing κ_1 (given by (29)). Since $H^1(\mathbf{Q}, \mathbf{Z}_p(1) \otimes \rho^{-1})$ is torsion-free, we conclude that $\boldsymbol{\kappa}^{\rho,\infty,\mathcal{A}} = 0$. Thus (using Proposition 5.2.9) $\mathcal{A}$ is in the blind spot of $\boldsymbol{\kappa}^{\rho,\infty}$.

6.2. Elliptic curves

For this section fix an elliptic curve E defined over $\mathbf{Q}$. We will assume that

$$p > 3, \tag{30}$$

$$\text{the } p\text{-adic representation } G_{\mathbf{Q}} \to \mathrm{Aut}(E[p^\infty]) \cong \mathrm{GL}_2(\mathbf{Z}_p) \text{ is surjective.} \tag{31}$$

Suppose first that $k \in \mathbf{Z}^+$, and let $R = \mathbf{Z}/p^k\mathbf{Z}$ and $T = E[p^k]$, the p^k-torsion in $E(\bar{\mathbf{Q}})$.

DEFINITION 6.2.1. Define a Selmer structure $\mathcal{F}$ by taking $\Sigma(\mathcal{F})$ to be the set of primes where E has bad reduction, together with p and ∞. For every prime $\ell \notin \Sigma(\mathcal{F})$ one can check that $H^1_{\mathrm{f}}(\mathbf{Q}_\ell, E[p^k])$ is the image of the Kummer map

$$E(\mathbf{Q}_\ell)/p^k E(\mathbf{Q}_\ell) \hookrightarrow H^1(\mathbf{Q}_\ell, E[p^k]).$$

For primes $\ell \in \Sigma(\mathcal{F})$ we define $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ to be the image of the Kummer map as well.

With this Selmer structure $H^1_{\mathcal{F}}(\mathbf{Q}, E[p^k])$ is the classical p^k-Selmer group of E, which sits in an exact sequence

$$0 \to E(\mathbf{Q})/p^k E(\mathbf{Q}) \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, E[p^k]) \longrightarrow Ш_E[p^k] \longrightarrow 0 \tag{32}$$

where $Ш_E$ is the Tate-Shafarevich group of E.

The Weil pairing identifies $E[p^k]^* = E[p^k]$, and one can show that $\mathcal{F}^* = \mathcal{F}$.

Similarly if $R = \mathbf{Z}_p$ and T is the p-adic Tate module $T_p(E)$, we define $\mathcal{F}$ analogously and get

$$0 \to E(\mathbf{Q}) \otimes \mathbf{Z}_p \longrightarrow H^1_{\mathcal{F}}(\mathbf{Q}, T_p(E)) \longrightarrow \varprojlim_k Ш_E[p^k] \longrightarrow 0.$$

If $Ш_E$ is finite then this becomes an isomorphism $H^1_{\mathcal{F}}(\mathbf{Q}, T_p(E)) \cong E(\mathbf{Q}) \otimes \mathbf{Z}_p$.

Now let $\mathcal{F}_{\mathrm{can}}$ be the "canonical" Selmer structure on T as in Definition 3.2.1. Then $\mathcal{F}_{\mathrm{can}}$ is obtained from $\mathcal{F}$ by relaxing the condition at p, i.e.,

$$H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, E[p^k]) = \begin{cases} \mathrm{image}[H^1(\mathbf{Q}_p, T_p(E)) \to H^1(\mathbf{Q}_p, E[p^k])] & \text{if } \ell = p, \\ H^1_{\mathcal{F}}(\mathbf{Q}_\ell, E[p^k]) & \text{if } \ell \neq p. \end{cases}$$

Similarly $\mathcal{F}^*_{\mathrm{can}}$ is obtained from $\mathcal{F}$ by setting

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}_p, E[p^k]) = \ker[H^1(\mathbf{Q}_p, E[p^k]) \to H^1(\mathbf{Q}_p, E[p^\infty])].$$

Then $\mathcal{F}^*_{\mathrm{can}} \leq \mathcal{F} \leq \mathcal{F}_{\mathrm{can}}$ and so

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, E[p^k]) \subset H^1_{\mathcal{F}}(\mathbf{Q}, E[p^k]) \subset H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, E[p^k]).$$

PROPOSITION 6.2.2. *$\chi(T, \mathcal{F}) = 0$ and $\chi(T, \mathcal{F}_{\mathrm{can}}) = 1$.*

PROOF. Since $H^1_{\mathcal{F}}(\mathbf{Q}, E[p]) = H^1_{\mathcal{F}^*}(\mathbf{Q}, E[p]^*)$, we have $\chi(T, \mathcal{F}) = 0$ by Theorem 4.1.13. Also

$$\chi(T, \mathcal{F}_{\mathrm{can}}) = \chi(T_p(E), \mathcal{F}_{\mathrm{can}}) = \mathrm{rank}_{\mathbf{Z}_p} T_p(E)^- = 1$$

by Theorem 5.2.15. □

LEMMA 6.2.3. *With assumptions as above, T satisfies hypotheses* (H.0), (H.1), (H.2), (H.3), *and* (H.4) *of §3.5, and $\mathcal{F}$ and $\mathcal{F}_{\mathrm{can}}$ both satisfy* (H.6).

PROOF. Hypothesis (H.0) is trivially satisfied, (H.1), (H.2), and (H.3) hold thanks to (31), and (H.4b) holds because of (30). Lemma 3.7.1 shows that (H.6) holds for $\mathcal{F}$ and $\mathcal{F}_{\mathrm{can}}$. □

Let N be the conductor of E. Kato [**Ka2**] (see also [**Sch**] and §3.5 of [**Ru6**]) has constructed an Euler system for $(T_p(E), \mathcal{P}')$, where $\mathcal{P}'$ is the set of primes not dividing $NpDD'$ with two auxiliary positive integers D, D' used in Kato's construction. Every $\ell \in \mathcal{P}'$ satisfies hypothesis (b) of Theorem 3.2.4, let $\mathcal{P}$ be the subset of $\ell \in \mathcal{P}'$ which also satisfy (a) of Theorem 3.2.4. Then $\mathcal{P}$ satisfies hypothesis (H.5).

Using Theorem 3.2.4 (along with Propositions 5.2.9 and 6.2.2 if $E(\mathbf{Q}_p)[p] \neq 0$), Kato's Euler system gives a Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Kato}} \in \mathbf{KS}(T_p(E), \mathcal{F}_{\mathrm{can}}, \mathcal{P})$. Reducing $\boldsymbol{\kappa}^{\mathrm{Kato}}$ modulo p^k gives a Kolyvagin system for $E[p^k]$ for every k.

The following is an application of Kato's Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Kato}}$. Let $L(E, s)$ denote the Hasse-Weil L-function attached to E, and $L_N(E, s)$ the L-function with the Euler factors at primes dividing the conductor N of E removed. Let Ω be the fundamental real period of E. We continue to suppose that p satisfies (30) and (31).

THEOREM 6.2.4 (Kato [**Ka2**]).

(i) *If $L(E, 1) \neq 0$ then $E(\mathbf{Q})$ and $Ш_E[p^\infty]$ are finite. If $L(E, 1) = 0$ and $\boldsymbol{\kappa}^{\mathrm{Kato}} \neq 0$, then either $E(\mathbf{Q})$ is infinite or $Ш_E[p^\infty]$ is infinite (or both).*

(ii) *Suppose further that p satisfies*

(a) *E has good reduction at p,*
(b) *$p \nmid |E(\mathbf{F}_p)|$,*
(c) *p does not divide the integer r_E of Theorem 7.1 of* [**Ru5**].
If $L(E,1) \neq 0$ then

$$\operatorname{length}(Ш_E[p^\infty]) \leq \operatorname{ord}_p\Big(\frac{L_N(E,1)}{\Omega}\Big).$$

with equality if and only if $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is primitive.

Proof. Applying Corollary 5.2.13(ii) to $\boldsymbol{\kappa}^{\mathrm{Kato}}$ shows that

$$\operatorname{length}(H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, E[p^\infty])) \leq \partial^{(0)}(\boldsymbol{\kappa}^{\mathrm{Kato}})$$

with equality if and only if $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is primitive. Combining this with Kato's computation of κ_1^{Kato}, the exact sequence (32), and using global duality to compare the true Selmer group $H^1_{\mathcal{F}}(\mathbf{Q}, E[p^\infty])$ with $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, E[p^\infty])$, will prove the theorem. For the details see [**Ru5**] or Theorem 2.2.10 of [**Ru6**]. □

Remark 6.2.5. In general one does not expect the inequality in Theorem 6.2.4(ii) to be sharp. Besides the missing Euler factors in the L-value, the Birch and Swinnerton-Dyer conjecture for the order of $Ш_E$ involves other terms as well, namely $|E(\mathbf{Q})_{\mathrm{tors}}|$ and $c_\ell = [E(\mathbf{Q}_\ell) : E_0(\mathbf{Q}_\ell)]$ for primes ℓ of bad reduction. A stronger inequality than Theorem 6.2.4(ii), which includes those factors, follows from Theorem 6.2.7 below (see [**PR5**] Proposition 3.3.1). One consequence of this is that $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is not always primitive. The following proposition gives a direct proof of this.

Proposition 6.2.6. *Suppose $L(E,1) \neq 0$ and p satisfies the hypotheses of Theorem 6.2.4(ii). If $p \mid c_\ell$ for some $\ell \neq p$, then $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is not primitive.*

Proof. Define a Selmer structure $\mathcal{F}_{\mathrm{u}}$ on $T_p(E)$ by taking

$$H^1_{\mathcal{F}_{\mathrm{u}}}(\mathbf{Q}_\ell, T_p(E)) = \begin{cases} H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T_p(E)) & \text{if } \ell \neq p, \\ H^1(\mathbf{Q}_p, T_p(E)) & \text{if } \ell = p. \end{cases}$$

We also write $\mathcal{F}_{\mathrm{u}}$ for the Selmer structure on $E[p]$ induced by this. Then $\mathcal{F}_{\mathrm{u}} \leq \mathcal{F}_{\mathrm{can}}$ (see for example [**Ru6**] Lemma 1.3.5), and we will take advantage of the fact that under the hypotheses of the lemma, $\mathcal{F}_{\mathrm{u}} < \mathcal{F}_{\mathrm{can}}$.

Suppose $\ell \neq p$ and $p \mid c_\ell$. Then (for example [**Si**], Corollary 15.2.1 of Appendix C) E has split multiplicative reduction at ℓ, so $E(\mathbf{Q}_\ell) \cong \mathbf{Q}_\ell^\times / q^{\mathbf{Z}}$ with $q \in \mathbf{Q}_\ell^\times$, and $p \mid \operatorname{ord}_\ell(q)$. It follows that the image of ℓ under

$$\mathbf{Q}_\ell^\times / q^{\mathbf{Z}} \twoheadrightarrow E(\mathbf{Q}_\ell)/pE(\mathbf{Q}_\ell) \hookrightarrow H^1(\mathbf{Q}_\ell, E[p])$$

does not lie in $H^1_{\mathcal{F}_{\mathrm{u}}}(\mathbf{Q}_\ell, E[p])$. The image of this map is precisely $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, E[p])$, so we conclude that $H^1_{\mathcal{F}_{\mathrm{u}}}(\mathbf{Q}_\ell, E[p])$ is strictly smaller than $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}_\ell, E[p])$.

It now follows from Propositions 2.3.5 and 6.2.2 that

$$\begin{aligned} \dim_{\mathbf{F}_p} H^1_{\mathcal{F}_{\mathrm{u}}}(\mathbf{Q}, E[p]) - \dim_{\mathbf{F}_p} H^1_{\mathcal{F}^*_{\mathrm{u}}}(\mathbf{Q}, E[p]) \\ < \dim_{\mathbf{F}_p} H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbf{Q}, E[p]) - \dim_{\mathbf{F}_p} H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbf{Q}, E[p]) = 1, \end{aligned}$$

and therefore $\chi(E[p], \mathcal{F}_{\mathrm{u}}) = 0$.

Thus by Theorem 5.1.1(i), $\mathbf{KS}(E[p], \mathcal{F}_{\mathrm{u}}) = 0$. But (see Remark A.5) the proof of Theorem 3.2.4 actually shows that the image of $\boldsymbol{\kappa}^{\mathrm{Kato}}$ in $\mathbf{KS}(E[p], \mathcal{F}_{\mathrm{can}})$ lies in $\mathbf{KS}(E[p], \mathcal{F}_{\mathrm{u}})$. Hence this image must be zero, and $\boldsymbol{\kappa}^{\mathrm{Kato}}$ is not primitive. □

Now take $R = \Lambda$ and $\mathbf{T} = T_p(E) \otimes \Lambda$ as in §5.3. By Theorem 5.3.3, Kato's Euler system gives rise to a Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{Kato},\infty} \in \overline{\mathbf{KS}}(\mathbf{T}, \mathcal{F}_\Lambda)$ where $\mathcal{F}_\Lambda$ is the Selmer structure of Definition 5.3.2. Applying the results of §5.3 to $\boldsymbol{\kappa}^{\mathrm{Kato},\infty}$ leads to the following theorem.

THEOREM 6.2.7 (Kato [**Ka2**]). *Suppose E has good ordinary reduction or non-split multiplicative reduction at p, and p does not divide the integer r_E of Theorem 7.1 of* [**Ru5**]. *Then*

$$\mathrm{char}(\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}_\infty), \mathbf{Q}_p/\mathbf{Z}_p)) \text{ divides } \mathcal{L}_{E,N}$$

where $\mathcal{L}_{E,N} \in \Lambda$ is the p-adic L-function attached to E with the Euler factors at primes dividing N removed, and $\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}_\infty)$ is the classical p-power Selmer group attached to E over $\mathbf{Q}_\infty$.

If E has split multiplicative reduction at p then the augmentation ideal $\mathcal{A}$ of Λ divides $\mathcal{L}_{E,N}$ and

$$\mathrm{char}(\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}_\infty), \mathbf{Q}_p/\mathbf{Z}_p)) \text{ divides } \mathcal{A}^{-1}\mathcal{L}_{E,N}.$$

If $\boldsymbol{\kappa}^{\mathrm{Kato},\infty}$ is Λ-primitive then both divisibilities are equalities.

PROOF. We can relate $\mathrm{Sel}_{p^\infty}(E/\mathbf{Q}_\infty)$ with $H^1_{\mathcal{F}^*_\Lambda}(\mathbf{Q}, \mathbf{T}^*)$ and $\mathrm{Ind}(\boldsymbol{\kappa}^{\mathrm{Kato},\infty})$ with $\mathcal{L}_{E,N}$, and then the theorem follows from Theorem 5.3.10 (and Remark 5.3.11). See [**Ru5**] for the details. □

6.3. The multiplicative group, revisited

Return to the setting of §6.1: $p > 2$, $\rho : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ is a character of finite order, L is the cyclic extension of $\mathbf{Q}$ which is the fixed field of ρ, $\Delta = \mathrm{Gal}(L/\mathbf{Q})$, $R = \mathbf{Z}_p$, and $T = \mathbf{Z}_p(1) \otimes \rho^{-1}$. Let $\mathcal{F}$ be the Selmer structure on T given by Definition 6.1.1.

For this section we suppose that ρ is an *odd* character, different from the Teichmuller character ω. By Proposition 6.1.6 we have $\chi(T, \mathcal{F}) = 0$, so by Theorem 5.2.10(i), $\mathbf{KS}(T, \mathcal{F}) = 0$. However, we can modify $\mathcal{F}$ to obtain Kolyvagin systems as follows.

Recall (Example 2.1.8) that $\mathcal{F}^\ell$ denotes the Selmer structure obtained from $\mathcal{F}$ by relaxing the local condition at ℓ, i.e., we set $H^1_{\mathcal{F}^\ell}(\mathbf{Q}_\ell, T) = H^1(\mathbf{Q}_\ell, T)$.

PROPOSITION 6.3.1. *Suppose $\ell \neq p$ is prime and $\rho(\ell) = 1$. Then $\chi(T, \mathcal{F}^\ell) = 1$.*

PROOF. By Proposition 2.3.5 we have

$$\chi(T, \mathcal{F}^\ell) - \chi(T, \mathcal{F}) = \dim_{\mathbf{F}_p} H^1_{\mathcal{F}^\ell}(\mathbf{Q}_\ell, \bar{T}) - \dim_{\mathbf{F}_p} H^1_{\mathcal{F}}(\mathbf{Q}_\ell, \bar{T}).$$

But $\chi(T, \mathcal{F}) = 0$ by Proposition 6.1.6, and under the identification (22)

$$H^1_{\mathcal{F}}(\mathbf{Q}_\ell, \bar{T}) \cong \mathbf{Z}_\ell^\times/(\mathbf{Z}_\ell^\times)^p, \quad H^1_{\mathcal{F}^\ell}(\mathbf{Q}_\ell, \bar{T}) \cong \mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^p.$$

Thus $\chi(T, \mathcal{F}^\ell) = 1$. □

THEOREM 6.3.2. *Suppose $\rho : G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ is an odd character, $\rho \neq \omega$. For every prime $\ell \neq p$ with $\rho(\ell) = 1$, the $\mathbf{Z}_p$-module $\mathbf{KS}(T, \mathcal{F}^\ell)$ is free of rank one and is generated by a primitive Kolyvagin system.*

PROOF. This follows from Theorem 5.2.10(ii) and Proposition 6.3.1 (using Lemma 6.1.5). □

REMARK 6.3.3. Kolyvagin's "Gauss sum Euler system" (see [**Ko**] or [**Ru2**]) gives an Euler system $\mathbf{c}^{(\ell)} \in \mathbf{ES}(T, \mathcal{F}^\ell, \mathcal{P}^{(\ell)})$ for each ℓ with $\rho(\ell) = 1$, where $\mathcal{P}^{(\ell)}$ is the *finite* set of primes dividing $\ell - 1$. These "finite" Euler systems give rise to Kolyvagin systems $\boldsymbol{\kappa}^{(\ell)} \in \mathbf{KS}(T, \mathcal{F}^\ell, \mathcal{P}^{(\ell)})$. Theorem 6.3.2 says that $\boldsymbol{\kappa}^{(\ell)}$ can be extended to $\mathbf{KS}(T, \mathcal{F}^\ell, \mathcal{P})$ where $\mathcal{P}$ is the set of all primes not dividing $p\ell m_\rho$ where m_ρ is the conductor of ρ. It is not clear whether the Euler systems themselves can be extended.

The family of Kolyvagin systems $\{\boldsymbol{\kappa}^{(\ell)}\}$ satisfies a "compatibility in ℓ", in that the classes $\{\kappa_1^{(\ell)} \in (L^\times \otimes \mathbf{Z}_p)^\rho\}$, which are given by Gauss sums, are the values $\psi(\ell)$ of a Hecke character ψ.

REMARK 6.3.4. A similar phenomenon occurs in the work of Flach [**Fl**]. Let E be an elliptic curve defined over $\mathbf{Q}$, $R = \mathbf{Z}_p$, and $T = \mathrm{Sym}^2(T_p(E))$, the symmetric square of the p-adic Tate module of E. Assume that the p-adic representation $G_{\mathbf{Q}} \to \mathrm{Aut}(T_p(E))$ is surjective, so that the hypotheses of §3.5 will be satisfied.

Theorem 5.2.15 shows that $\chi(T, \mathcal{F}_{\mathrm{can}}) = 1$. If $\mathcal{F}_{\mathrm{BK}}$ denotes the Bloch-Kato Selmer structure on T used in [**Fl**], then $\mathcal{F}_{\mathrm{BK}}$ differs from $\mathcal{F}_{\mathrm{can}}$ only at p, $\mathcal{F}_{\mathrm{BK}} \leq \mathcal{F}_{\mathrm{can}}$, and one can show that $\chi(\mathcal{F}_{\mathrm{BK}}, T) = 0$. For every rational prime $\ell \neq p$ where E has good reduction, the automorphism Fr_ℓ of T has the eigenvalue ℓ with multiplicity one, and it follows that with the relaxed-at-ℓ Selmer structure $\mathcal{F}^\ell_{\mathrm{BK}}$ we have

$$\chi(T, \mathcal{F}^\ell_{\mathrm{BK}}) = \chi(T, \mathcal{F}_{\mathrm{BK}}) + 1 = 1.$$

Therefore by Theorem 5.2.10(ii) the $\mathbf{Z}_p$-module $\mathbf{KS}(T, \mathcal{F}^\ell_{\mathrm{BK}})$ is free of rank one, generated by a primitive Kolyvagin system, for every prime $\ell \neq p$ where E has good reduction.

In [**Fl**], Flach constructs what can be viewed as the classes $\kappa_1^{(\ell)} \in H^1_{\mathcal{F}^\ell_{\mathrm{BK}}}(\mathbf{Q}, T)$ for these Kolyvagin systems. So far no further classes $\kappa_n^{(\ell)}$ have been constructed, but the classes $\kappa_1^{(\ell)}$ are compatible in an important way. See [**Ma2**] or [**We**] for details.

APPENDIX A

Proof of Theorem 3.2.4

In this appendix we prove Theorems 3.2.4 and 5.3.3. The proof requires the setting, notation, and results from Chapter 4 of [**Ru6**]. We recall most of the essential information here and refer to [**Ru6**] for the details.

Let T, R, $\mathcal{F} = \mathcal{F}_{\text{can}}$, and $\mathcal{P}$ be as in Theorem 3.2.4. Thus R is the ring of integers of a finite extension of $\mathbf{Q}_p$, $\mathcal{P}$ is a set of primes different from p where T is unramified, and such that for every $\ell \in \mathcal{P}$,

- $T/(\mathrm{Fr}_\ell - 1)T$ is a cyclic R-module,
- $\mathrm{Fr}_\ell^{p^k} - 1$ is injective on T for every $k \geq 0$.

As usual let $\mathcal{N}$ be the set of all squarefree products of primes in $\mathcal{P}$.

LEMMA A.1. *If $H^0(\mathbf{Q}_p, T^*)$ is a divisible R-module then for every ideal I of R, we have $H^1_{\mathcal{F}}(\mathbf{Q}_p, T/IT) = H^1(\mathbf{Q}_p, T/IT)$.*

PROOF. When $I = 0$ this is the definition of the Selmer structure $\mathcal{F}$ at p. For general I the Selmer structure on T/IT is the one induced from T, i.e., $H^1_{\mathcal{F}}(\mathbf{Q}_p, T/IT)$ is the image of $H^1_{\mathcal{F}}(\mathbf{Q}_p, T) = H^1(\mathbf{Q}_p, T)$ in $H^1(\mathbf{Q}_p, T/IT)$. Fixing a generator α of I, cohomology of the exact sequence $0 \to T \xrightarrow{\alpha} T \to T/IT \to 0$ shows that

$$\mathrm{coker}[H^1(\mathbf{Q}_p, T) \to H^1(\mathbf{Q}_p, T/IT)] \cong H^2(\mathbf{Q}_p, T)[I],$$

the kernel of I in $H^2(\mathbf{Q}_p, T)$. By local duality

$$H^2(\mathbf{Q}_p, T)[I] \cong \mathrm{Hom}(H^0(\mathbf{Q}_p, T^*)/IH^0(\mathbf{Q}_p, T^*), \mathbf{Q}_p/\mathbf{Z}_p)$$

which is zero if $H^0(\mathbf{Q}_p, T^*)$ is divisible. □

Fix an Euler System $\mathbf{c} \in \mathbf{ES}(T) = \mathbf{ES}(T, \mathcal{P}, \mathcal{K})$ with $\mathcal{K}$ as in Theorem 3.2.4. Definition 4.4.10 of [**Ru6**] associates to $\mathbf{c}$ a collection

$$\{\kappa_n \in H^1(\mathbf{Q}, T/I_nT) \otimes G_n : n \in \mathcal{N}\}$$

such that $\kappa_1 = c_{\mathbf{Q}}$. Here we write simply κ_n for the class denoted $\kappa_{[\mathbf{Q},n,I_n]}$ of [**Ru6**]. (The arguments of [**Ru6**] use a fixed generator of each G_ℓ, and hence of each G_n, and produced $\kappa_{[\mathbf{Q},n,I_n]} \in H^1(\mathbf{Q}, T/I_nT)$. Without these choices the same construction gives $\kappa_{[\mathbf{Q},n,I_n]} \in H^1(\mathbf{Q}, T/I_nT) \otimes G_n$.)

PROPOSITION A.2. *If $H^0(\mathbf{Q}_p, T^*)$ is a divisible R-module then the collection $\{\kappa_n\}$ is a weak Kolyvagin system for $(T, \mathcal{F}, \mathcal{P})$ in the sense of Definition 3.1.8.*

In general, if $k \in \mathbf{Z}^+$ then for all sufficiently large j the collection $\{\kappa_n^{(k)} : n \in \mathcal{N}_j\}$ is a weak Kolyvagin system for $(T/\mathfrak{m}^kT, \mathcal{F}, \mathcal{P}_j)$, where $\kappa_n^{(k)}$ denotes the image of κ_n in $H^1(\mathbf{Q}, T/(I_n, \mathfrak{m}^k)T) \otimes G_n$.

PROOF. By [**Ru6**] Theorem 4.5.1, $\kappa_n \in H^1_{\mathcal{F}^{np}}(\mathbf{Q}, T/I_nT) \otimes G_n$. If $H^0(\mathbf{Q}_p, T^*)$ is divisible then Lemma A.1 shows that $H^1_{\mathcal{F}^{np}}(\mathbf{Q}, T/I_nT) = H^1_{\mathcal{F}^n}(\mathbf{Q}, T/I_nT)$.

In general $H^1_{\mathcal{F}}(\mathbf{Q}_p, T/\mathfrak{m}^kT)$ is the image of $H^1(\mathbf{Q}_p, T)$ in $H^1(\mathbf{Q}_p, T/\mathfrak{m}^kT)$, which is finite, so $H^1_{\mathcal{F}}(\mathbf{Q}_p, T/\mathfrak{m}^kT)$ is the image of $H^1(\mathbf{Q}_p, T/\mathfrak{m}^jT)$ for all sufficiently large j. For such j, if $n \in \mathcal{N}_j$ then $I_n \subset \mathfrak{m}^j$ so $\kappa_n^{(k)}$ is in the image of $H^1(\mathbf{Q}, T/\mathfrak{m}^jT) \otimes G_n$, and hence $\kappa_n^{(k)} \in H^1_{\mathcal{F}^n}(\mathbf{Q}, T/\mathfrak{m}^kT) \otimes G_n$.

Theorem 4.5.4 of [**Ru6**] shows that the κ_n satisfy (5) of §3.1. Thus in either case the definition of a weak Kolyvagin system is satisfied. □

The collection $\{\kappa_n\}$ (or $\{\kappa_n^{(k)}\}$) is not in general a Kolyvagin system, because we will not have $\kappa_n \in H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n$. However, by computing the finite projections $(\kappa_n)_{\ell,\mathrm{f}}$ at primes ℓ dividing n, we will show that a slight modification of the κ_n (or $\{\kappa_n^{(k)}\}$) gives a Kolyvagin system. Thus it remains to compute the $(\kappa_n)_{\ell,\mathrm{f}}$.

DEFINITION A.3. If I is an ideal of R and $\ell \in \mathcal{P}$, let $\mathcal{A}_{\ell,I}$ denote the augmentation ideal of $(R/I)[G_\ell \otimes R/I]$. Then there is a canonical isomorphism

$$\rho_\ell = \rho_{\ell,I} : \mathcal{A}_{\ell,I}/\mathcal{A}_{\ell,I}^2 \longrightarrow G_\ell \otimes R/I$$

which sends $\sigma - 1$ to $\sigma \otimes 1$.

If $n \in \mathcal{N}$ let $\mathfrak{S}(n)$ denote the set of permutations of the primes dividing n, and let $\mathfrak{S}_1(n) \subset \mathfrak{S}(n)$ be the subset

$$\{\pi \in \mathfrak{S}(n) : \text{the } \ell \text{ not fixed by } \pi \text{ form a single } \pi\text{-orbit}\}.$$

If $\pi \in \mathfrak{S}(n)$ let $d_\pi = \prod_{\pi(\ell)=\ell} \ell$.

THEOREM A.4. *If $n \in \mathcal{N}$ and $\ell \mid n$ then*

$$(\kappa_n)_{\ell,\mathrm{f}} = \sum_{\substack{\pi \in \mathfrak{S}_1(n) \\ \pi(\ell) \neq \ell}} (-1)^{\nu(n/d_\pi)} (\kappa_{d_\pi})_{\ell,\mathrm{f}} \bigotimes_{q \mid (n/d_\pi)} \rho_q(P_q(\mathrm{Fr}_{\pi(q)}^{-1}))$$

where as usual $\nu(d)$ is the number of prime factors of d.

We will prove Theorem A.4 below, after using it to prove Theorems 3.2.4 and 5.3.3.

PROOF OF THEOREM 3.2.4. Fix an Euler system $\mathbf{c}$ and keep the rest of the notation above.

First suppose that $H^0(\mathbf{Q}_p, T^*)$ is a divisible R-module. For every $n \in \mathcal{N}$ define

$$\kappa'_n = \sum_{\pi \in \mathfrak{S}(n)} \mathrm{sign}(\pi) \kappa_{d_\pi} \bigotimes_{\ell \mid (n/d_\pi)} \rho_\ell(P_\ell(\mathrm{Fr}_{\pi(\ell)}^{-1})) \in H^1(\mathbf{Q}, T/I_nT) \otimes G_n \tag{33}$$

where $\mathrm{sign}(\pi)$ is the sign of the permutation π. By inspection we see that since the κ_n satisfy (5) of §3.1, so do the κ'_n. On further inspection we see that if $\ell \mid n$ then

we can group the terms in the definition of κ'_n as

$$\begin{aligned}\kappa'_n &= \sum_{\substack{\pi\in\mathfrak{S}(n)\\ \pi(\ell)=\ell}} \operatorname{sign}(\pi)\kappa_{d_\pi} \bigotimes_{q|(n/d_\pi)} \rho_q(P_q(\mathrm{Fr}_{\pi(q)}^{-1})) \\ &\qquad + \sum_{\substack{\pi\in\mathfrak{S}(n)\\ \pi(\ell)=\ell}} \sum_{\substack{\pi'\in\mathfrak{S}_1(d_\pi)\\ \pi'(\ell)\neq\ell}} \operatorname{sign}(\pi\pi')\kappa_{d_{\pi'}} \bigotimes_{q|(n/d_{\pi'})} \rho_q(P_q(\mathrm{Fr}_{\pi\pi'(q)}^{-1})) \\ &= \sum_{\substack{\pi\in\mathfrak{S}(n)\\ \pi(\ell)=\ell}} \operatorname{sign}(\pi)s_\pi \bigotimes_{q|(n/d_\pi)} \rho_q(P_q(\mathrm{Fr}_{\pi(q)}^{-1}))\end{aligned}$$

where

$$s_\pi = \kappa_{d_\pi} - \sum_{\substack{\pi'\in\mathfrak{S}_1(d_\pi)\\ \pi'(\ell)\neq\ell}} (-1)^{\nu(d_\pi/d_{\pi'})}\kappa_{d_{\pi'}} \bigotimes_{q|(d_\pi/d_{\pi'})} \rho_q(P_q(\mathrm{Fr}_{\pi'(q)}^{-1})).$$

Theorem A.4 shows that $(s_\pi)_{\ell,\mathrm{f}} = 0$ for every π, so $(\kappa'_n)_{\ell,\mathrm{f}} = 0$. Combining this with Proposition A.2 we see that $\kappa'_n \in H^1_{\mathcal{F}(n)}(\mathbf{Q}, T/I_nT) \otimes G_n$, and the collection $\{\kappa'_n\}$ is a Kolyvagin system $\boldsymbol{\kappa}' \in \mathbf{KS}(T)$. We have $\kappa'_1 = \kappa_1 = c_{\mathbf{Q}}$, so the association $\mathbf{c} \to \boldsymbol{\kappa}'$ gives the desired map $\mathbf{ES}(T) \to \mathbf{KS}(T)$ in Theorem 3.2.4.

Now we no longer suppose that $H^0(\mathbf{Q}_p, T^*)$ is divisible. Let $k \in \mathbf{Z}^+$, let j be sufficiently large as in Proposition A.2, and let $\kappa_n^{(k)}$ be as in Proposition A.2. For $n \in \mathcal{N}_j$ define $\kappa'_n \in H^1(\mathbf{Q}, T/\mathfrak{m}^kT) \otimes G_n$ exactly as in (33), but with κ_n replaced by $\kappa_n^{(k)}$. Then the identical computation shows that $\boldsymbol{\kappa}^{(k,j)} = \{\kappa'_n : n \in \mathcal{N}_j\} \in \mathbf{KS}(T/\mathfrak{m}^kT, \mathcal{P}_j)$. The collection $\{\boldsymbol{\kappa}^{(k,j)}\}$ is an element of $\overline{\mathbf{KS}}(T)$, and this gives the desired map $\mathbf{ES}(T) \to \overline{\mathbf{KS}}(T)$. □

Remark A.5. The proof of Theorem 3.2.4 actually produces a Kolyvagin system for a possibly finer Selmer structure. Define $\mathcal{F}_{\mathrm{u}}$ by

$$H^1_{\mathcal{F}_{\mathrm{u}}}(\mathbf{Q}_\ell, T) = \begin{cases} H^1(\mathbf{Q}_p, T) & \text{if } \ell = p \\ H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T) & \text{if } \ell \neq p. \end{cases}$$

Then $\mathcal{F}_{\mathrm{u}} \leq \mathcal{F}$, and it can happen that $\mathcal{F}_{\mathrm{u}} < \mathcal{F}$. More precisely, if T is unramified at ℓ then $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) = H^1_{\mathcal{F}_{\mathrm{u}}}(\mathbf{Q}_\ell, T)$, but if T is ramified at ℓ they may be different (see [**Ru6**] Lemma 1.3.5(iv)).

The proof of Theorem 4.5.1 of [**Ru6**] shows that in fact the classes κ_n used in the proof of Theorem 3.2.4 lie in $H^1_{(\mathcal{F}_{\mathrm{u}})^n}(\mathbf{Q}, T/I_nT)$. Therefore the map of Theorem 3.2.4 factors through

$$\mathbf{ES}(T) \longrightarrow \mathbf{KS}(T, \mathcal{F}_{\mathrm{u}}) \longrightarrow \mathbf{KS}(T, \mathcal{F}).$$

See Proposition 6.2.6 for an application of this observation.

Proof of Theorem 5.3.3. The proof of Theorem 5.3.3 is essentially the same as that of Theorem 3.2.4. We sketch the argument again here. Fix an Euler system $\mathbf{c}$.

In $n \in \mathcal{N}$ let $I'_n \subset \Lambda$ be the ideal generated by $\ell - 1$, $P_\ell(1)$, and $\mathrm{Fr}_\ell - 1$ for ℓ dividing n. Then $I_n \subset I'_n$, and both ideals have finite index in Λ when $n > 1$. If F_n denotes the fixed field in $\mathbf{Q}_\infty$ of the automorphisms Fr_ℓ for ℓ dividing n, and M_n is the smallest power of p in I'_n, then $\Lambda/I'_n \cong (\mathbf{Z}/M_n\mathbf{Z})[\mathrm{Gal}(F_n/\mathbf{Q})]$ and the class

$\kappa_{[F_n,n,M_n]}$ associated to $\mathbf{c}$ by Definition 4.4.10 of [**Ru6**] lies in $H^1(F_n, T/M_nT) = H^1(\mathbf{Q}, \mathbf{T}/I_n'\mathbf{T})$. We will denote this class simply by κ_n.

We need to construct an element of $\overline{\mathbf{KS}}(\mathbf{T})$. In other words, for every $k \in \mathbf{Z}^+$ we need to construct, for some j, a Kolyvagin system in $\mathbf{KS}(\mathbf{T}/\mathfrak{m}^k, \mathcal{P}_j)$, and these need to be compatible in the obvious sense.

Fix $k \in \mathbf{Z}^+$. Let $\mathcal{A}_k \subset \mathfrak{m}^k$ be the ideal of Λ generated by $\gamma^{p^k} - 1$ and p^k, where γ is a topological generator of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Since $\mathfrak{m}^k$ has finite index in Λ, we can choose $j \geq k$ so that the image of

$$H^1(\mathbf{Q}_p, \mathbf{T}/\mathcal{A}_j\mathbf{T}) \longrightarrow H^1(\mathbf{Q}_p, \mathbf{T}/\mathfrak{m}^k\mathbf{T})$$

is equal to the image of $H^1(\mathbf{Q}_p, \mathbf{T})$ in $H^1(\mathbf{Q}_p, \mathbf{T}/\mathfrak{m}^k\mathbf{T})$, i.e., is $H^1_{\mathcal{F}_\Lambda}(\mathbf{Q}_p, \mathbf{T}/\mathfrak{m}^k\mathbf{T})$.

Now suppose $n \in \mathcal{N}_j$. It is not hard to check that $I_n' \subset \mathcal{A}_j$. Let $\kappa_n^{(k)}$ denote the image of κ_n in $H^1(\mathbf{Q}, \mathbf{T}/\mathfrak{m}^k\mathbf{T}) \otimes G_n$. Just as in the proof of Proposition A.2 we have (using Theorems 4.5.1 and 4.5.4 of [**Ru6**]) that the collection $\{\kappa_n^{(k)} : n \in \mathcal{N}_j\}$ is a weak Euler system for $(\mathbf{T}/\mathfrak{m}^k\mathbf{T}, \mathcal{P}_j)$.

Theorem A.4 remains true in this setting. The only difference in the proof is that instead of working over $R = \mathbf{Z}_p$ and its quotient $\mathbf{Z}_p/I_n\mathbf{Z}_p$, we need to work over $R = \mathbf{Z}_p[\mathrm{Gal}(F_n/\mathbf{Q})]$ and its quotient $\Lambda/I_n' = (\mathbf{Z}/M_n\mathbf{Z})[\mathrm{Gal}(F_n/\mathbf{Q})]$. The key points are that R is a free $\mathbf{Z}_p$-module, and that $\mathrm{Fr}_\ell = 1$ in R for every ℓ dividing n.

Now using Theorem A.4 exactly as in the proof of Theorem 3.2.4 we can modify the collection $\{\kappa_n^{(k)}\}$ to produce a collection $\{\kappa_n' : n \in \mathcal{N}_j\} \in \mathbf{KS}(\mathbf{T}/\mathfrak{m}^k\mathbf{T}, \mathcal{P}_j)$. The compatibility in j and k is evident, so putting these together gives the desired element of $\overline{\mathbf{KS}}(\mathbf{T})$. □

The rest of this appendix is devoted to the proof of Theorem A.4.

Fix $n \in \mathcal{N}$ and a prime $\ell \mid n$. If F is a number field then we will write $F_\ell = F \otimes \mathbf{Q}_\ell = \oplus_{\lambda|\ell} F_\lambda$ and $H^i(F_\ell, T) = \oplus_{\lambda|\ell} H^i(F_\lambda, T)$, $H^1_{\mathrm{f}}(F_\ell, T) = \oplus_{\lambda|\ell} H^1_{\mathrm{f}}(F_\lambda, T)$, etc. If $F/\mathbf{Q}$ is Galois then $H^i(F_\ell, T)$ and $H^1_{\mathrm{f}}(F_\ell, T)$ have natural actions of $\mathrm{Gal}(F/\mathbf{Q})$.

For simplicity we will assume from now on that $R = \mathbf{Z}_p$. The general case presents no additional difficulties. Let I be the power of p generating I_n. For every m dividing n let $\mathbf{Q}(m)$ denote the maximal extension of $\mathbf{Q}$ of exponent I inside $\mathbf{Q}(\boldsymbol{\mu}_m)$, and write $G(m) = \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$. We have a natural identification $G(m) = \mathrm{Gal}(\mathbf{Q}(n)/\mathbf{Q}(n/m))$, and we will view $G(m)$ either as a subgroup or as a quotient of $G(n)$, as convenient.

Although in general I_m can be a multiple of I, we will modify our previous notation and replace I_m by I for every m dividing n. With this change we have identifications $G(q) \cong G_q/IG_q$ for every $q \in \mathcal{P}$ and $G(m) \cong \prod_{q|m} G(q)$.

LEMMA A.6. (i) *If $L \subset \mathbf{Q}(n)$ and $H = \mathrm{Gal}(\mathbf{Q}(n)/L)$ then the natural restriction map $H^1(L_\ell, T) \xrightarrow{\sim} H^1(\mathbf{Q}(n)_\ell, T)^H$ is an isomorphism, and it induces an isomorphism $H^1_{\mathrm{f}}(L_\ell, T) \xrightarrow{\sim} H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)^H$.*

(ii) $H^1(G(n/\ell), H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)) = 0$.

PROOF. The first assertion follows from the inflation-restriction exact sequence, since we have assumed that $T^{\mathrm{Fr}_\ell^{p^k}=1} = 0$.

Let H be the decomposition group of ℓ in $\mathrm{Gal}(\mathbf{Q}(n)/\mathbf{Q}(\ell))$, and $L = \mathbf{Q}(n)^H$. Then

$$H^1(L/\mathbf{Q}(\ell), H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)^H) = H^1(L/\mathbf{Q}(\ell), H^1_{\mathrm{f}}(L_\ell, T)) = 0$$

since ℓ splits completely in $L/\mathbf{Q}_\ell(\ell)$.

On the other hand, $H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T) = \oplus_{\lambda|\ell} T/(\mathrm{Fr}_\lambda - 1)T$ (Lemma 1.2.1(i)), where Fr_λ is the Frobenius in $G_{\mathbf{Q}(n)_\lambda}$.

Write $|H| = k$. Since H is generated by Fr_ℓ, we can lift Fr_ℓ to G_{L_λ} so that $\mathrm{Fr}_\ell^k = \mathrm{Fr}_\lambda$, and then

$$\begin{aligned} H^1(H, H^1_{\mathrm{f}}(\mathbf{Q}(n)_\lambda, T)) &= H^1(\langle \mathrm{Fr}_\ell \rangle, T/(\mathrm{Fr}_\ell^k - 1)T) \\ &= \{t \in T : (\sum_{i=0}^{k-1} \mathrm{Fr}_\ell^i)t \in (\mathrm{Fr}_\ell^k - 1)T\}/(\mathrm{Fr}_\ell - 1)T. \end{aligned}$$

By our assumptions on ℓ, multiplication by $\mathrm{Fr}_\ell^k - 1$ is injective on T, and so this final quotient is zero. Hence $H^1(\mathbf{Q}(n)/L, H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)) = 0$, and (ii) follows from the inflation-restriction sequence. □

Let X_n be the "Universal Euler system" defined in §4.2 of [**Ru6**]. Then X_n is the free $\mathbf{Z}[G(n)]$-module generated by symbols x_m for m dividing n, modulo the relations

- $G(n/m)$ acts trivially on x_m,
- $N_q x_{qm} = P_q(\mathrm{Fr}_q^{-1})x_m$ for every prime q dividing n/m, where $N_q = \sum_{\sigma \in G(q)} \sigma \in \mathbf{Z}[G(n)]$, and $P_q(x) = \det(1 - \mathrm{Fr}_\ell\ x \mid T)$ as in Definition 2.2.1.

Thus $\{x_m\}$ "looks like" a piece of an Euler system. In particular our Euler system $\mathbf{c}$ induces a map $c : X_n \to H^1(\mathbf{Q}(n), T)$ by taking $c(x_m)$ to the restriction of $c_{\mathbf{Q}(m)}$. Since $(c_{\mathbf{Q}(m)})_\ell \in H^1_{\mathrm{f}}(\mathbf{Q}(m)_\ell, T)$ ([**Ru6**] Proposition 4.6.1), we also get a map $c_{\mathrm{f}} : X_n \to H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$ by taking $c_{\mathrm{f}}(x_m)$ to be the restriction of $(c_{\mathbf{Q}(m)})_\ell$.

For each q dividing n fix a generator σ_q of $G(q)$, so that we can identify $G(q)$ with $\mathbf{Z}/I\mathbf{Z}$. Following Kolyvagin we define

$$D_q = \sum_{i=0}^{I-1} i\sigma_q^i \in \mathbf{Z}[G(q)] \subset \mathbf{Z}[G(n)]$$

and $D_m = \prod_{q|m} D_q$. We have the telescoping identity in $\mathbf{Z}[G(n)]$

$$(\sigma_q - 1)D_q = I - N_q, \tag{34}$$

which leads to the fundamental property ([**Ru6**] Lemma 4.4.2)

$$(\sigma - 1)D_m x_m \in IX_n \quad \text{for every } \sigma \in G(n) \text{ and } m \text{ dividing } n. \tag{35}$$

Since X_n has no $\mathbf{Z}$-torsion ([**Ru6**] Proposition 4.3.1), it follows from (35) that $I^{-1}(\sigma - 1)D_m x_m$ is well-defined in X_n for every σ and m.

Definition A.7. Suppose $m \mid n$. The assignment $\sigma \mapsto c_{\mathrm{f}}(I^{-1}(\sigma - 1)D_m x_m)$ defines a 1-cocycle from $G(n/\ell)$ to $H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$. By Lemma A.6(ii) we conclude that there is a $\beta_m \in H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$ satisfying

$$(\sigma - 1)\beta_m = c_{\mathrm{f}}(I^{-1}(\sigma - 1)D_m x_m) \quad \text{for every } \sigma \in G(n/\ell). \tag{36}$$

In particular

$$(D_m c_{\mathbf{Q}(m)})_\ell - I\beta_m \in H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)^{G(n/\ell)},$$

so by Lemma A.6(i) there is a (unique) $\eta_m \in H^1_{\mathrm{f}}(\mathbf{Q}(\ell)_\ell, T)$ whose restriction to $\mathbf{Q}(n)_\ell$ is $(D_m c_{\mathbf{Q}(m)})_\ell - I\beta_m$.

Proposition A.8. *The restriction of κ_m to $H^1(\mathbf{Q}(\ell)_\ell, T/IT)$ is the image of η_m.*

PROOF. We mimic the arguments of [**Ru6**] §4.6. Fix a prime λ of $\bar{\mathbf{Q}}$ above ℓ, and let $\mathcal{D}$ denote the decomposition group of λ in $G_{\mathbf{Q}}$. Let

$$\mathbb{T} = \mathrm{Maps}(G_{\mathbf{Q}}, T),$$

the group of continuous maps (not necessarily homomorphisms) from $G_{\mathbf{Q}}$ to T, with $G_{\mathbf{Q}}$ acting by

$$(\gamma f)(g) = f(g\gamma) \quad \text{for } f \in \mathbb{T} \text{ and } \gamma, g \in G_{\mathbf{Q}}.$$

Define $\mathbb{T}_\ell \subset \mathbb{T}$ by

$$\mathbb{T}_\ell = \{f \in \mathbb{T} : f(hg) = h(f(g)) \text{ for all } h \in \mathcal{D}\}.$$

Cohomology of the exact sequence $0 \to \mathbb{T}_\ell \to \mathbb{T} \to \mathbb{T}/\mathbb{T}_\ell \to 0$ yields, for every subfield F of $\mathbf{Q}(n)$ (since $H^0(F_\ell, T) = 0$ by our assumption on ℓ), a short exact sequence

$$0 \longrightarrow \mathbb{T}^{G_F} \longrightarrow (\mathbb{T}/\mathbb{T}_\ell)^{G_F} \xrightarrow{\delta_F} H^1(F_\ell, T) \longrightarrow 0 \tag{37}$$

and a map

$$(\mathbb{T}/(I\mathbb{T} + \mathbb{T}_\ell))^{G_F} \xrightarrow{\bar{\delta}_{\mathbf{Q}}} H^1(F_\ell, T/IT)$$

(see [**Ru6**] Corollaries B.4.4 and B.5.2). The map $c_{\mathrm{f}} : X_n \to H^1(\mathbf{Q}(n)_\ell, T)$ factors through a map $d : X_n \to (\mathbb{T}/\mathbb{T}_\ell)^{G_{\mathbf{Q}(n)}}$ in (37) ([**Ru6**] Proposition 4.6.8). For every m dividing n we have $d(D_m x_m) \in (\mathbb{T}/(I\mathbb{T} + \mathbb{T}_\ell))^{G_{\mathbf{Q}}}$, and then

$$\kappa_m = \bar{\delta}_{\mathbf{Q}}(d(D_m x_m))$$

([**Ru6**] Lemma 4.6.7 and Definition 4.4.10).

The assignment $\sigma \mapsto d(I^{-1}(\sigma - 1)D_m x_m)$ defines a 1-cocycle from $G(n/\ell)$ to $(\mathbb{T}/\mathbb{T}_\ell)^{G_{\mathbf{Q}(n)}}$. The connecting map $\delta_{\mathbf{Q}(n)}$ sends this cocycle to the coboundary $\sigma \mapsto (\sigma - 1)\beta_m$, and hence to zero in $H^1(G(n/\ell), H^1(\mathbf{Q}(n)_\ell, T))$. But $\mathbb{T}^{G_{\mathbf{Q}(n)}}$ is a free $\mathbf{Z}_p[G(n)]$-module (see [**Ru6**] Lemma 4.4.6), so $H^1(G(n/\ell), \mathbb{T}^{G_{\mathbf{Q}(n)}}) = 0$ and hence there is a $\hat{\beta}_m \in (\mathbb{T}/\mathbb{T}_\ell)^{G_{\mathbf{Q}(n)}}$ such that

$$(\sigma - 1)\hat{\beta}_m = d(I^{-1}(\sigma - 1)D_m x_m)$$

for every $\sigma \in G(n/\ell)$.

It follows that

$$\delta_{\mathbf{Q}(n)}(\hat{\beta}_m) - \beta_m \in H^1(\mathbf{Q}(n)_\ell, T)^{G(n/\ell)} = H^1(\mathbf{Q}(\ell)_\ell, T)$$

the equality by Lemma A.6(i). Since $\delta_{\mathbf{Q}(\ell)}$ is surjective, after adjusting $\hat{\beta}_m$ by an element of $(\mathbb{T}/\mathbb{T}_\ell)^{G_{\mathbf{Q}(\ell)}}$ we may assume that $\delta_{\mathbf{Q}(n)}(\hat{\beta}_m) = \beta_m$.

Let $\hat{\eta}_m = d(D_m x_m) - I\hat{\beta}_m \in (\mathbb{T}/\mathbb{T}_\ell)^{G_{\mathbf{Q}(\ell)}}$. Then the restriction of κ_m to $\mathbf{Q}(\ell)$ is

$$\bar{\delta}_{\mathbf{Q}(\ell)}(d(D_m x_m)) = \bar{\delta}_{\mathbf{Q}(\ell)}(\hat{\eta}_m)$$

which is the image of $\delta_{\mathbf{Q}(\ell)}(\hat{\eta}_m) = \eta_m$ in $H^1(\mathbf{Q}(\ell)_\ell, T/IT)$. This proves the lemma. □

Proposition A.8 will enable us to prove Theorem A.4, because for each m, the finite projection $(\kappa_m)_{\ell,\mathrm{f}}$ is determined by the restriction of κ_m to $\mathbf{Q}(\ell)_\ell$.

DEFINITION A.9. Define the *ℓ-finite quotient* $\overline{X_n}$ of X_n to be the quotient of X_n by the elements $\{x_m : \ell \mid m, m \mid n\}$. For $x \in X_n$ let $\overline{x}$ denote the image of x in $\overline{X_n}$.

LEMMA A.10. (i) *The map* $c_{\mathrm{f}} : X_n \to H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$ *factors through a map* $X_n \to \overline{X_n} \xrightarrow{\bar{c}_{\mathrm{f}}} H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$.
(ii) $P_\ell(\mathrm{Fr}_\ell^{-1})\overline{X_n} = 0$.

PROOF. The "Euler system congruence relation", Corollary 4.8.1 of [**Ru6**] adapted to account for the different choice of Euler factors in our definition of Euler system, says that $(c_{\mathbf{Q}(m)})_{\ell,\mathrm{f}} = 0$ if $\ell \mid m$. This proves (i).

For (ii), we need only observe that $\overline{X_n}$ is generated by the $\overline{x_m}$ for m dividing n/ℓ, and for these m, $P_\ell(\mathrm{Fr}_\ell^{-1})\overline{x_m} = N_\ell \overline{x_{m\ell}} = 0$. □

DEFINITION A.11. Let $\mathcal{A}$ denote the augmentation ideal of $\mathbf{Z}[G(n)]$, and for each prime q dividing n define $\tilde{\rho}_q : \mathcal{A} \to \mathbf{Z}/I\mathbf{Z}$ to be the composition

$$\tilde{\rho}_q : \mathcal{A} \longrightarrow \mathcal{A}_{q,I} \xrightarrow{\rho_{q,I}} G_q \otimes \mathbf{Z}/I\mathbf{Z} \longrightarrow \mathbf{Z}/I\mathbf{Z}$$

where $\mathcal{A}_{q,I}$ and $\rho_{q,I}$ are as in Definition A.3, the map $\mathcal{A} \to \mathcal{A}_{I,q}$ is induced by $\mathbf{Z}[G(n)] \to \mathbf{Z}[G(q)] = \mathbf{Z}[G_q \otimes \mathbf{Z}/I\mathbf{Z}]$, and the final map sends our chosen generator σ_q to 1. Concretely, $\mathcal{A}$ is generated by the $\sigma_q - 1$ for q dividing n, and

$$\tilde{\rho}_q(\sigma_{q'} - 1) = \begin{cases} 1 & \text{if } q = q', \\ 0 & \text{if } q \neq q'. \end{cases}$$

LEMMA A.12. *Suppose* $m\ell \mid n$.
(i) *If* $f \in \mathcal{A}^2 + I\mathbf{Z}[G(n)]$ *then* $\overline{I^{-1} f D_{m\ell} x_{m\ell}} = 0$ *in* $\overline{X_n}$.
(ii) *If* $f \in \mathcal{A} + I\mathbf{Z}[G(n)]$, *then*

$$\overline{I^{-1} f D_{m\ell} x_{m\ell}} = -\sum_{q \mid m} \tilde{\rho}_q(f) \overline{I^{-1} P_q(\mathrm{Fr}_q^{-1}) D_{m\ell/q} x_{m\ell/q}} - \tilde{\rho}_\ell(f) \overline{I^{-1} P_\ell(\mathrm{Fr}_\ell^{-1}) D_m x_m}.$$

PROOF. Note that by (35), $I^{-1} f D_{m\ell} x_{m\ell}$ is a well-defined element of X_n. If $f \in I\mathbf{Z}[G(n)]$ then $\overline{I^{-1} f D_{m\ell} x_{m\ell}} = (I^{-1} f) D_{m\ell} \overline{x_{m\ell}} = 0$.

Using (34) we see that

$$(\sigma_q - 1) D_{m\ell} x_{m\ell} = ((q-1) - N_q) D_{m\ell/q} x_{m\ell} = (q-1) D_{m\ell/q} x_{m\ell} - P_q(\mathrm{Fr}_q^{-1}) D_{m\ell/q} x_{m\ell/q}$$

in X_n. Dividing by I and projecting into $\overline{X_n}$ proves (ii) when $f = \sigma_q - 1$.

Note that each $P_q(\mathrm{Fr}_q^{-1})$ belongs to $\mathcal{A} + I\mathbf{Z}[G(n)]$ by our assumption that I divides $P_q(1)$. Proceeding inductively we can continue to expand those terms in the sum with index divisible by ℓ, and we conclude that if $f \in \mathcal{A} + I\mathbf{Z}[G(n)]$ then $\overline{I^{-1} f D_{m\ell} x_{m\ell}}$ is a linear combination of the elements $\{\overline{I^{-1} P_\ell(\mathrm{Fr}_\ell^{-1}) D_r x_r} : r \mid (n/\ell)\}$.

Now if $f, g \in \mathcal{A}$ then $\overline{I^{-1} f g D_{m\ell} x_{m\ell}}$ can be expressed as a linear combination of $\{\overline{I^{-1} P_\ell(\mathrm{Fr}_\ell^{-1}) g D_r x_r} : r \mid (n/\ell)\}$. But since $g D_r x_r \in I X_n$,

$$\overline{I^{-1} P_\ell(\mathrm{Fr}_\ell^{-1}) g D_r x_r} = P_\ell(\mathrm{Fr}_\ell^{-1}) \overline{I^{-1} g D_r x_r} = 0$$

by Lemma A.10(ii). This proves (i).

The right-hand side of (ii) is a linear function of

$$f \in (\mathcal{A} + I\mathbf{Z}[G(n)])/(\mathcal{A}^2 + I\mathbf{Z}[G(n)]),$$

and thanks to (i) the left-hand side is as well. We have shown that (ii) holds for the generators $\sigma_q - 1$ of $(\mathcal{A} + I\mathbf{Z}[G(n)])/(\mathcal{A}^2 + I\mathbf{Z}[G(n)])$, so (ii) holds for all f. □

Fix a representative $\mathrm{Fr}_\ell \in G(n)$ so that $\mathrm{Fr}_\ell = 1$ on $\mathbf{Q}(\ell)$.

PROPOSITION A.13.

$$\overline{I^{-1}P_\ell(\mathrm{Fr}_\ell^{-1})D_n x_n} = \sum_{\substack{\pi\in\mathfrak{S}_1(n)\\ \pi(\ell)\neq\ell}} (-1)^{\nu(n/d_\pi)} \prod_{q|(n/d_\pi)} \tilde{\rho}_q(P_q(\mathrm{Fr}_{\pi(q)}^{-1}))\overline{I^{-1}P_\ell(\mathrm{Fr}_\ell^{-1})D_{d_\pi}x_{d_\pi}}$$

PROOF. Apply Lemma A.12 repeatedly, beginning with $m = n$ and $f = P_\ell(\mathrm{Fr}_\ell^{-1})$. Expand all terms of the form $\overline{I^{-1}gD_m x_m}$ with m divisible by ℓ, but not those with m prime to ℓ. (Note that at the first step we have $\tilde{\rho}_\ell(P_\ell(\mathrm{Fr}_\ell^{-1})) = 0$, since by convention Fr_ℓ restricts to 1 in $G(\ell)$.) The summand corresponding to π occurs as follows:

- expand $\overline{I^{-1}P_\ell(\mathrm{Fr}_\ell^{-1})D_n x_n}$,
- take the resulting term $\overline{I^{-1}P_{\pi(\ell)}(\mathrm{Fr}_{\pi(\ell)}^{-1})D_{n/\pi(\ell)}x_{n/\pi(\ell)}}$ and expand that,
- take the resulting term $\overline{I^{-1}P_{\pi^2(\ell)}(\mathrm{Fr}_{\pi^2(\ell)}^{-1})D_{n/(\pi(\ell)\pi^2(\ell))}x_{n/(\pi(\ell)\pi(\ell))}}$ and expand that,

and so forth until $\pi^i(\ell) = \ell$, which leaves us with the desired multiple of the term $\overline{I^{-1}P_\ell(\mathrm{Fr}_\ell^{-1})D_{d_\pi}x_{d_\pi}}$. □

DEFINITION A.14. By Lemma 1.2.1(i),

$$H^1_{\mathrm{f}}(\mathbf{Q}(\ell), T/IT) \cong T/(I, \mathrm{Fr}_\ell - 1)T, \quad H^1_{\mathrm{f}}(\mathbf{Q}(\ell), T) \cong T/(\mathrm{Fr}_\ell - 1)T.$$

By our assumptions on ℓ, both of these groups are cyclic and the latter is free of rank one over $\mathbf{Z}_p/P_\ell(1)$. Hence we have a composition

$$H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/IT) \xrightarrow{\mathrm{res}} H^1_{\mathrm{f}}(\mathbf{Q}(\ell)_\ell, T/IT) \xrightarrow{P_\ell(1)/I} H^1_{\mathrm{f}}(\mathbf{Q}(\ell)_\ell, T) \xrightarrow{\mathrm{res}} H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T) \tag{38}$$

in which all three maps are injective: the first by Lemma 1.2.4, the second by the observation above, and the third by Lemma A.6.

We denote the composition (38) by $\mathrm{res}_I : H^1_{\mathrm{f}}(\mathbf{Q}_\ell, T/IT) \to H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$. We will test the identity of Theorem A.4 in $H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$, by applying res_I. Note that we could not simply test this identity in $H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T/IT)$ because the natural restriction map is not injective.

PROPOSITION A.15. *If m divides n then*

$$\mathrm{res}_I((\kappa_m)_{\ell,\mathrm{f}}) = \bar{c}_{\mathrm{f}}(\overline{I^{-1}P_\ell(\mathrm{Fr}_\ell^{-1})D_m x_m})$$

where $\bar{c}_{\mathrm{f}} : \overline{X_n} \to H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T)$ is the map $\overline{x_m} \mapsto (c_{\mathbf{Q}(m)})_\ell$ of Lemma A.10(i).

PROOF. The Cayley-Hamilton theorem shows that $P_\ell(\mathrm{Fr}_\ell^{-1})H^1_{\mathrm{f}}(\mathbf{Q}(n)_\ell, T) = 0$. Thus by Proposition A.8,

$$\begin{aligned}\mathrm{res}_I((\kappa_m)_{\ell,\mathrm{f}}) &= \frac{P_\ell(1)}{I}((D_m c_{\mathbf{Q}(m)})_\ell - I\beta_m) = \frac{P_\ell(1)}{I}(D_m c_{\mathbf{Q}(m)})_\ell - P_\ell(1)\beta_m \\ &= \frac{P_\ell(1)}{I}(D_m c_{\mathbf{Q}(m)})_\ell + (P_\ell(\mathrm{Fr}_\ell^{-1}) - P_\ell(1))\beta_m.\end{aligned}$$

Since $P_\ell(\mathrm{Fr}_\ell^{-1}) - P_\ell(1)$ is in the augmentation ideal of $\mathbf{Z}[G(n)]$, the definition of β_m shows that

$$(P_\ell(\mathrm{Fr}_\ell^{-1}) - P_\ell(1))\beta_m = c_{\mathrm{f}}(I^{-1}(P_\ell(\mathrm{Fr}_\ell^{-1}) - P_\ell(1))D_m x_m).$$

Combining these identities proves the proposition. □

PROOF OF THEOREM A.4. Theorem A.4 is now immediate from Propositions A.13 and A.15, and the injectivity of res_I. This concludes the proof of Theorem 3.2.4 as well. □

APPENDIX B

Proof of Theorem 4.3.3, by Benjamin Howard

In this appendix we give the proof of Theorem 4.3.3. It is a pleasure to thank Karl Rubin for his suggestions and encouragement.

Let R be a principal, artinian, local ring with maximal ideal $\mathfrak{m}$ and finite residue field. If M is an R-module and $\psi \in \mathrm{Hom}(M, R)$ we define for any integer r a map, also denoted ψ

$$\bigwedge^r M \longrightarrow \bigwedge^{r-1} M$$

by the rule

$$m_1 \wedge \cdots \wedge m_r \mapsto \sum_{i=1}^{r} (-1)^{i+1} \psi(m_i) m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \wedge \cdots \wedge m_r.$$

We define a map

$$\bigwedge^s \mathrm{Hom}(M, R) \longrightarrow \mathrm{Hom}(\bigwedge^r M, \bigwedge^{r-s} M)$$

for $s \leq r$ by iteration of the above construction:

$$\psi_1 \wedge \cdots \wedge \psi_s = \psi_s \circ \cdots \circ \psi_1.$$

LEMMA B.1. *Suppose M is a free R-module of rank $\geq r+1$ and we are given $\psi_1, \ldots, \psi_r \in \mathrm{Hom}(M, R)$. Define*

$$\begin{aligned} \psi &= \psi_1 \oplus \cdots \oplus \psi_r : M \longrightarrow R^r \\ \Psi &= \psi_1 \wedge \cdots \wedge \psi_r : \bigwedge^{r+1} M \longrightarrow M. \end{aligned}$$

Then

$$\Psi(\bigwedge^{r+1} M) = \mathfrak{m}^{\mathrm{length}(\mathrm{coker}(\psi))} \ker(\psi).$$

PROOF. First suppose ψ is surjective with kernel $A \subset M$. The image is projective, and so there is a $B \subset M$ such that $M = A \oplus B$ and ψ maps B isomorphically onto R^r. The map

$$\bigwedge^{r+1} M = \bigoplus_{p+q=r+1} (\bigwedge^p A \otimes \bigwedge^q B) \xrightarrow{\Psi} A \oplus B$$

takes the factor $A \otimes \bigwedge^r B$ isomorphically onto A and kills the other summands. This proves the claim in this special case.

In general, the image of Ψ and the kernel and cokernel of ψ depend only on the submodule of $\mathrm{Hom}(M, R)$ generated by the maps $\psi_1, \ldots, \psi_r$, so we may assume

that $\psi_i = \pi^{a_i}\phi_i$ where π is a uniformizer of R and $\{\phi_i\}_{1\leq i\leq r}$ extends to a basis of $\mathrm{Hom}(M,R)$. Let

$$\phi = \phi_1 \oplus \cdots \oplus \phi_r : M \to R^r \qquad \Phi = \phi_1 \wedge \cdots \wedge \phi_r : \bigwedge^{r+1} M \to M.$$

By the preceding case,

$$\Psi(\bigwedge^{r+1} M) = \mathfrak{m}^a \cdot \Phi(\bigwedge^{r+1} M) = \mathfrak{m}^a \cdot \ker(\phi)$$

where $a = a_1 + \cdots + a_r = \mathrm{length}(\mathrm{coker}(\psi))$. Extending the ϕ_i's to a basis of $\mathrm{Hom}(M,R)$ and taking the dual basis fixes a splitting $M \cong \ker(\phi) \oplus R^r$. In this decomposition the kernel of ψ is

$$\ker(\psi) \cong \ker(\phi) \oplus \bigoplus_{i=1}^{r} \mathfrak{m}^{\mathrm{length}(R)-a_i} R.$$

Since $\mathfrak{m}^a$ kills $\mathfrak{m}^{\mathrm{length}(R)-a_i}R$ we have $\mathfrak{m}^a \ker(\phi) = \mathfrak{m}^a \ker(\psi)$ □

Let T be an R-module equipped with a continuous R-linear action of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Fix a Selmer triple $(T,\mathcal{F},\mathcal{P})$ of core rank $\chi = \chi(T) > 0$ which we assume satisfies Hypotheses (H.0) through (H.6) of §3.5, as well as $\mathcal{P} \subset \mathcal{P}_{\mathrm{length}(R)}$. If n is an integer we define $\nu(n)$ to be the number of prime divisors of n.

THEOREM B.2. *If $n \in \mathcal{N} = \mathcal{N}(\mathcal{P})$ is a core vertex then $H^1_{\mathcal{F}^n}(\mathbf{Q},T)$ is free of rank $\nu(n)+\chi$.*

PROOF. If n a core vertex then $H^1_{\mathcal{F}(n)^*}(\mathbf{Q},T) = 0$ and so global duality (Theorem 5.3) gives an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}(n)}(\mathbf{Q},T) \longrightarrow H^1_{\mathcal{F}^n}(\mathbf{Q},T) \longrightarrow \bigoplus_{\ell \mid n} H^1(\mathbf{Q}_\ell,T)/H^1_{\mathrm{tr}}(\mathbf{Q}_\ell,T) \longrightarrow 0.$$

The term on the left is free of rank χ and the term on the right is free (so projective) of rank $\nu(n)$ by Lemma 3.5.6. □

For each $\ell \in \mathcal{P}$ choose a generator of $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_\ell)/\mathbf{Q})$ so that we may view the finite singular comparison map as an isomorphism

$$H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T) \xrightarrow{\phi^{\mathrm{fs}}_\ell} H^1(\mathbf{Q}_\ell,T)/H^1_{\mathrm{f}}(\mathbf{Q}_\ell,T) \cong H^1_{\mathrm{tr}}(\mathbf{Q}_\ell,T)$$

and choose also for each $\ell \in \mathcal{P}$ an isomorphism $H^1_{\mathrm{tr}}(\mathbf{Q}_\ell,T) \xrightarrow{\iota_\ell} R$. Fix a core vertex $n \in \mathcal{N} = \mathcal{N}(\mathcal{P})$ and order the primes $\ell_1, \cdots, \ell_{\nu(n)}$ dividing n arbitrarily. Let $\mathrm{loc}^{\mathrm{f}}_i$ (resp. $\mathrm{loc}^{\mathrm{tr}}_i$) from $H^1(\mathbf{Q},T)$ to R be localization at ℓ_i, followed by projection onto the finite (resp. transverse) submodule, followed by $\iota_{\ell_i} \circ \phi^{\mathrm{fs}}_{\ell_i}$ (resp. ι_{ℓ_i}). For each $m \mid n$ we define functions

$$\psi^{(m)}_i = \begin{cases} \mathrm{loc}^{\mathrm{f}}_i & \text{if } \ell_i \mid m \\ \mathrm{loc}^{\mathrm{tr}}_i & \text{if } \ell_i \nmid m \end{cases}$$

and

$$\psi^{(m)} = \psi^{(m)}_1 \oplus \cdots \oplus \psi^{(m)}_{\nu(n)} \quad : \quad H^1_{\mathcal{F}^n}(\mathbf{Q},T) \longrightarrow R^{\nu(n)}$$

$$\Psi^{(m)} = \psi^{(m)}_1 \wedge \cdots \wedge \psi^{(m)}_{\nu(n)} \quad : \quad \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n}(\mathbf{Q},T) \longrightarrow H^1_{\mathcal{F}^n}(\mathbf{Q},T).$$

PROPOSITION B.3. *Let* $\lambda(m,T^*)=\mathrm{length}(H^1_{\mathcal{F}(m)^*}(\mathbf{Q},T^*))$. *Then*

$$\Psi^{(m)}\left(\bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n}(\mathbf{Q},T)\right)=\mathfrak{m}^{\lambda(m,T^*)}H^1_{\mathcal{F}(m)}(\mathbf{Q},T).$$

PROOF. We have the exact sequence

$$0\longrightarrow H^1_{\mathcal{F}(m)}(\mathbf{Q},T)\longrightarrow H^1_{\mathcal{F}^n}(\mathbf{Q},T)\xrightarrow{\psi^{(m)}} R^{\nu(n)}\longrightarrow \mathrm{coker}(\psi^{(m)})\longrightarrow 0$$

immediately from the definitions, and the isomorphism

$$H^1_{\mathcal{F}(m)}(\mathbf{Q},T)\cong R^{\chi}\oplus H^1_{\mathcal{F}(m)^*}(\mathbf{Q},T^*)$$

by Theorem 4.1.13. From this and Theorem B.2 it follows that

$$\mathrm{length}(\mathrm{coker}(\psi^{(n)}))=\lambda(m,T^*).$$

The claim now follows from Lemma B.1. □

DEFINITION B.4. Choose $c\in\bigwedge^{\nu(n)+1}H^1_{\mathcal{F}^n}(\mathbf{Q},T)$ and for each $m\mid n$ define

$$\kappa_m=\kappa_m(n,c)=(-1)^{\nu(m)}\Psi^{(m)}(c)\in H^1_{\mathcal{F}(m)}(\mathbf{Q},T).$$

PROPOSITION B.5. *For* $m\ell_i\mid n$ *we have* $\mathrm{loc}^{\mathrm{f}}_{\ell_i}(\kappa_m)=\mathrm{loc}^{\mathrm{tr}}_{\ell_i}(\kappa_{m\ell_i})$.

PROOF.

$$\begin{aligned}
\mathrm{loc}^{\mathrm{f}}_{\ell_i}(\kappa_m) &= (-1)^{\nu(m)}\mathrm{loc}^{\mathrm{f}}_{\ell_i}(\Psi^{(m)}(c))\\
&= (-1)^{\nu(m)}(\Psi^{(m)}\wedge\mathrm{loc}^{\mathrm{f}}_{\ell_i})(c)\\
&= -(-1)^{\nu(m)}(\Psi^{(m\ell_i)}\wedge\mathrm{loc}^{\mathrm{tr}}_{\ell_i})(c)\\
&= (-1)^{\nu(m\ell_i)}\mathrm{loc}^{\mathrm{tr}}_{\ell_i}(\Psi^{(m\ell_i)}(c))\\
&= \mathrm{loc}^{\mathrm{tr}}_{\ell_i}(\kappa_{m\ell_i})
\end{aligned}$$

where the third equality is seen by transposing the factors $\mathrm{loc}^{\mathrm{f}}_{\ell_i}$, $\mathrm{loc}^{\mathrm{tr}}_{\ell_i}$ which both occur in $(\Psi^{(m)}\wedge\mathrm{loc}^{\mathrm{f}}_{\ell_i})$. □

The collection of all $\kappa_m(n,c)$ with $m\mid n$ therefore gives a section of the restriction of the stub Selmer sheaf $\mathcal{H}'$ of Definition 4.3.1 to the subgraph $\mathcal{X}_n$ of $\mathcal{X}(\mathcal{P})$ whose vertices are all divisors m of n. We would like to show that if $n'=nd$ is another core vertex then this section can be extended to a section of $\mathcal{H}'$ over $\mathcal{X}_{nd}$. The section $\kappa(n,c)$ depends on the choice of ordering of primes dividing n, but only up to sign. When we extend our section from $\mathcal{X}_n$ to $\mathcal{X}_{nd}$ we maintain the same ordering on primes dividing n but put them *after* the "new" primes which divide d. This convention remains in effect in all that follows. Let

$$\mathrm{loc}^{\mathrm{tr}}_i,\mathrm{loc}^{\mathrm{f}}_i : H^1(\mathbf{Q},T)\longrightarrow R$$

and

$$\psi^{(m)}_i=\begin{cases}\mathrm{loc}^{\mathrm{f}}_i & \text{if } \ell_i\mid m\\ \mathrm{loc}^{\mathrm{tr}}_i & \text{if } \ell_i\nmid m\end{cases}$$

be defined exactly as before but with our new indexing $1\le i\le\nu(n')$.

LEMMA B.6. *Keep the notation of the previous paragraph. In the following diagram the image of the horizontal arrow contains the image of the vertical arrow.*

$$\begin{array}{ccc} \bigwedge^{\nu(n')+1} H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T) & \xrightarrow{\mathrm{loc}_1^{\mathrm{tr}}\wedge\cdots\wedge\mathrm{loc}_{\nu(d)}^{\mathrm{tr}}} & \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T) \\ & & \uparrow \\ & & \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{n}}(\mathbf{Q},T) \end{array}$$

If the image of $c' \in \bigwedge^{\nu(n')+1} H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T)$ under the horizontal arrow agrees with the image of c under the vertical arrow then the section $\kappa(n',c')$ of $\mathcal{X}_{nd}$ extends the section $\kappa(n,c)$ of $\mathcal{X}_n$.

PROOF. Global duality and $H^1_{(\mathcal{F}^n)^*}(\mathbf{Q},T) = 0$ imply that we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^n}(\mathbf{Q},T) \longrightarrow H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T) \xrightarrow{\mathrm{loc}_d} \bigoplus_{\ell\mid d} H^1(\mathbf{Q}_\ell,T)/H^1_f(\mathbf{Q}_\ell,T) \longrightarrow 0.$$

The right hand side is projective and so we may choose a free rank $\nu(d)$ summand A, complementary to $H^1_{\mathcal{F}^n}(\mathbf{Q},T) \subset H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T)$. We may extend our diagram to

$$\begin{array}{ccc} \bigwedge^{\nu(n')+1} H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T) & \xrightarrow{\mathrm{loc}_1^{\mathrm{tr}}\wedge\cdots\wedge\mathrm{loc}_{\nu(d)}^{\mathrm{tr}}} & \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{nd}}(\mathbf{Q},T) \\ \uparrow & & \uparrow \\ \bigwedge^{\nu(d)} A \otimes \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{n}}(\mathbf{Q},T) & \xrightarrow{\mathrm{loc}_1^{\mathrm{tr}}\wedge\cdots\wedge\mathrm{loc}_{\nu(d)}^{\mathrm{tr}}\otimes\mathrm{id}} & \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^{n}}(\mathbf{Q},T) \end{array}$$

The map $\bigoplus \mathrm{loc}_i^{\mathrm{tr}} : A \to R^{\nu(d)}$ being an isomorphism implies that

$$\bigwedge^{\nu(d)} \mathrm{loc}_i^{\mathrm{tr}} : \bigwedge^{\nu(d)} A \longrightarrow \bigwedge^{\nu(d)} R^{\nu(d)} = R$$

is as well, and so also is the bottom horizontal arrow. This proves the first claim. To prove the second claim, we compute for $m \mid n$

$$\begin{aligned} \kappa_m(n,c) &= (-1)^{\nu(m)}(\psi^{(m)}_{\nu(d)+1} \wedge \cdots \wedge \psi^{(m)}_{\nu(nd)})(c) \\ &= (-1)^{\nu(m)}(\psi^{(m)}_{\nu(d)+1} \wedge \cdots \wedge \psi^{(m)}_{\nu(nd)})((\mathrm{loc}_1^{\mathrm{tr}} \wedge \cdots \wedge \mathrm{loc}_{\nu(d)}^{\mathrm{tr}})(c')) \\ &= (-1)^{\nu(m)}(\psi^{(m)}_{\nu(d))} \wedge \cdots \wedge \psi^{(m)}_{\nu(nd)})((\psi^{(m)}_1 \wedge \cdots \wedge \psi^{(m)}_{\nu(d)})(c')) \\ &= (-1)^{\nu(m)}(\psi^{(m)}_1 \wedge \cdots \wedge \psi^{(m)}_{\nu(nd)})(c') \\ &= \kappa_m(n',c'). \end{aligned}$$

□

THEOREM B.7. *For any $m \in \mathcal{N}$ the map*

$$\Gamma(\mathcal{H}') \longrightarrow \mathcal{H}'(m)$$

is surjective.

PROOF. We have fixed a generator of G_m, so $\mathcal{H}'(m) = \mathfrak{m}^{\lambda(m,T^*)} H^1_{\mathcal{F}(m)}(\mathbf{Q},T)$. Fix $\alpha \in \mathfrak{m}^{\lambda(m,T^*)} H^1_{\mathcal{F}(m)}(\mathbf{Q},T)$ and (using Lemma 4.1.9(iii)) choose a core vertex n_0 divisible by m. By Proposition B.3 there is $c_0 \in \bigwedge^{\nu(n_0)+1} H^1_{\mathcal{F}^{n_0}}(\mathbf{Q},T)$ such that $\kappa_m(n_0,c_0) = \alpha$.

Now we choose a sequence of core vertices $n_1 \mid n_2 \cdots$ such that $n_0 \mid n_1$ and every $n \in \mathcal{N}$ divides n_i for some i. By Lemma B.6 we may choose for each $i > 0$

$$c_i \in \bigwedge^{\nu(n_i)+1} H^1_{\mathcal{F}^{n_i}}(\mathbf{Q}, T)$$

in such a way that the section $\kappa(n_{i+1}, c_{i+1})$ of $\mathcal{X}_{n_{i+1}}$ restricts to $\kappa(n_i, c_i)$ on $\mathcal{X}_{n_i}$. We now define the desired $\kappa \in \Gamma(\mathcal{H}')$ by $\kappa_n = \kappa_n(n_i, c_i)$ for i chosen sufficiently large. □

Corollary B.8. *$\Gamma(\mathcal{H}')$ has a free R-submodule of rank χ.*

Proof. Take m to be a core vertex. Then $\mathcal{H}'(m)$ is free of rank χ, so the corollary follows immediately from Theorem B.7. □

Lemma B.9. *Suppose $\chi > 1$ and let n be a core vertex. There is an $\ell \in \mathcal{P}$ such that $n\ell$ is also a core vertex, $H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T)$ is free of rank $\nu(n) + \chi - 1$, and in the composition*

$$\bigwedge^{\nu(n)+2} H^1_{\mathcal{F}^n}(\mathbf{Q}, T) \xrightarrow{\mathrm{loc}^{\mathrm{f}}_\ell} \bigwedge^{\nu(n)+1} H^1_{\mathcal{F}^n_\ell}(\mathbf{Q}, T) \xrightarrow{\bigwedge_{q|n} \mathrm{loc}^{\mathrm{f}}_q} H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T) \tag{39}$$

both arrows are surjective.

Proof. Let $k = \mathrm{length}(R)$. By Proposition 10.2 we may choose $l \in \mathcal{P}$ so that the sequence

$$0 \longrightarrow H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T) \longrightarrow H^1_{\mathcal{F}(n)}(\mathbf{Q}, T) \xrightarrow{\mathrm{loc}_\ell} H^1_f(\mathbf{Q}_\ell, T) \longrightarrow 0$$

is exact. Then by Lemma 4.1.7(ii), $n\ell$ is a core vertex and that $H^1_{\mathcal{F}_\ell(n)^*}(\mathbf{Q}, T^*) = 0$. By global duality the sequence

$$0 \longrightarrow H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T) \longrightarrow H^1_{\mathcal{F}^n_\ell}(\mathbf{Q}, T) \xrightarrow{\oplus_{q|n} \mathrm{loc}^{\mathrm{f}}_q} \bigoplus_{q|n} H^1_f(\mathbf{Q}_q, T) \longrightarrow 0$$

is exact and so Lemma B.1 implies that the second arrow of (39) is surjective.

The surjectivity of the first arrow follows from the exactness of

$$0 \longrightarrow H^1_{\mathcal{F}^n_\ell}(\mathbf{Q}, T) \longrightarrow H^1_{\mathcal{F}^n}(\mathbf{Q}, T) \xrightarrow{\mathrm{loc}_\ell} H^1_f(\mathbf{Q}_\ell, T) \longrightarrow 0$$

and the observation that if $M \cong A \oplus R$ is free of rank $\geq r+1$ and $\pi_R : A \oplus R \to R$ is projection onto the second factor then the map

$$\bigwedge^{r+1} M \xrightarrow{\pi_R} \bigwedge^{r} A$$

is a surjection. Apply this with $M = H^1_{\mathcal{F}^n}(\mathbf{Q}, T)$ and $A = H^1_{\mathcal{F}^n_\ell}(\mathbf{Q}, T)$. □

Proposition B.10. *Suppose $\chi > 1$ and $n \in \mathcal{N}$. There is a $\kappa \in \Gamma(\mathcal{H}')$ such that $R \cdot \kappa$ is free of rank one and the restriction of κ to $\mathcal{X}_n$ is trivial.*

Proof. By Corollary 4.1.9(iii) we may assume that n is a core vertex. Fix $\ell \in \mathcal{P}$ as in Lemma B.9 and choose $c \in \bigwedge^{\nu(n)+2} H^1_{\mathcal{F}^n}(\mathbf{Q}, T)$ which is taken by the composition (39) to an element $\alpha \in H^1_{\mathcal{F}_\ell(n)}(\mathbf{Q}, T)$ which generates a free submodule. View c as an element of $\bigwedge^{\nu(n\ell)+1} H^1_{\mathcal{F}^{n\ell}}(\mathbf{Q}, T)$ and let $\kappa_{n\ell}(n\ell, c)$ be as in Definition B.4. By construction $\kappa_{n\ell}(n\ell, c) = \alpha$, but because $\mathrm{loc}^{\mathrm{tr}}_\ell$ kills c, $\kappa_m(n\ell, c) = 0$ whenever $m \mid n$.

Thus $\kappa(n\ell, c)$ gives a section of $\mathcal{X}_{n\ell}$ with the desired properties and we need only extend it to a section of all of $\mathcal{X}$ in exactly the same manner as the proof of Theorem B.7. Choose a sequence of core vertices $n_1 \mid n_2 \mid \cdots$ with $n\ell = n_1$ in such a way that every $m \in \mathcal{N}$ divides some n_i. Choose $c_i \in \bigwedge^{\nu(n_i)+1} H^1_{\mathcal{F}^{n_i}}(\mathbf{Q}, T)$ in such a way that the section $\kappa(n_{i+1}, c_{i+1})$ restricts to $\kappa(n_i, c_i)$ on $\mathcal{X}_{n_i}$ (by Lemma B.6) and pass to the limit. □

THEOREM B.11. *If $\chi > 1$ then for any integer n, $\Gamma(\mathcal{H}')$ has a free rank-n submodule.*

PROOF. Construct a sequence $\kappa^i \in \Gamma(\mathcal{H}')$ inductively as follows. Start with any vertex m_1 and choose κ^1 which vanishes on $\mathcal{X}_{m_1}$ and with $R \cdot \kappa^1 \cong R$. Once κ^i has been constructed, choose a core vertex m_{i+1} which is divisible both by m_i and by a vertex at which κ^i generates a free submodule of the stalk. By the previous lemma we may construct κ^{i+1} whose restriction to $\mathcal{X}_{m_{i+1}}$ is trivial and such that $R \cdot \kappa^{i+1} \cong R$.

If there is a nontrivial linear relation among $\kappa^1, \dots, \kappa^n$, say

$$r_1\kappa^1 + \cdots + r_n\kappa^n = 0$$

then let r_i be the first nonzero coefficient. Then $r_i\kappa^i$ restricted to $\mathcal{X}_{m_{i+1}}$ is trivial and so $r_i = 0$ by construction of m_{i+1}, a contradiction. □

PROOF OF THEOREM 4.3.3. Assertions (i), (ii), and (iii) of Theorem 4.3.3 are Theorem B.7, Corollary B.8, and Theorem B.11, respectively. □

Bibliography

[BK] Bloch, S., Kato, K.: L-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift (Vol. I), P. Cartier, et al., eds., *Prog. in Math.* **86**, Boston: Birkhäuser (1990) 333–400.

[Co] Colmez, P.: Théorie d'Iwasawa des représentations de de Rham d'un corps local, *Ann. of Math.* **148** (1998) 485–571.

[Fl] Flach, M.: A finiteness theorem for the symmetric square of an elliptic curve, *Invent. math.* **109** (1992) 307–327.

[Gr1] Greenberg, R.: On the Iwasawa invariants of totally real number fields, *Amer. J. Math* **98** (1976) 263–284.

[Gr2] ———: Iwasawa theory for p-adic representations. In: Algebraic number theory, J. Coates et al., eds., *Adv. Stud. Pure Math.* **17**, Boston: Academic Press (1989) 97–137.

[Ka1] Kato, K.: Euler systems, Iwasawa theory, and Selmer groups, *Kodai Math. J.* **22** (1999) 313–372.

[Ka2] ———: p-adic Hodge theory and values of zeta functions of modular forms. To appear.

[Ko] Kolyvagin, V.: Euler systems. In: The Grothendieck Festschrift (Vol. II), P. Cartier et al., eds., *Prog. in Math* **87**, Boston: Birkhäuser (1990) 435–483.

[Ma1] Mazur, B.: Deforming Galois representations. In: Galois groups over $\mathbf{Q}$ (Berkeley, CA, 1987), *Math. Sci. Res. Inst. Publ.* **16**, New York: Springer (1989) 385–437.

[Ma2] ———: *Galois deformations and Hecke curves*, Harvard University course notes, spring 1994.

[MW] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbf{Q}$, *Invent. math.* **76** (1984) 179–330.

[Mi] Milne, J.S.: Arithmetic duality theorems, *Perspectives in Math.* **1**, Orlando: Academic Press (1986).

[Ne] Nekovář, J.: Selmer complexes (preprint), `http://www.math.jussieu.fr/~nekovar/pu`.

[PR1] Perrin-Riou, B.: Théorie d'Iwasawa et hauteurs p-adiques, *Invent. math.* **199** (1992) 137-185.

[PR2] ———: Théorie d'Iwasawa des représentations p-adiques sur un corps local, *Invent. Math.* **115** (1994) 81–161.

[PR3] ———: Fonctions L p-adiques des représentations p-adiques, *Astérisque* **229** (1995).

[PR4] ———: Systèmes d'Euler p-adiques et théorie d'Iwasawa, *Ann. Inst. Fourier (Grenoble)* **48** (1998) 1231–1307.

[PR5] ———: Arithmétique des courbes elliptiques à réduction supersingulière en p. To appear.

[Ru1] Rubin, K.: The main conjecture. Appendix to: Cyclotomic fields I and II, S. Lang, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990) 397–419.

[Ru2] ———: Kolyvagin's system of Gauss sums. In: Arithmetic Algebraic Geometry, G. van der Geer et al., eds., *Prog. in Math* **89**, Boston: Birkhäuser (1991) 435–324.

[Ru3] ———: The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991) 25–68.

[Ru4] ———: A Stark conjecture "over $\mathbf{Z}$" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)* **46** (1996) 33–62.

[Ru5] ———: Euler systems and modular elliptic curves, in: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds., *London Math. Soc. Lect. Notes* **254** Cambridge: Cambridge Univ. Press (1998) 351–367.

[Ru6] ———: Euler Systems. *Annals of Math. Studies* **147**, Princeton: Princeton University Press (2000).

[Sch] Scholl, A.: An introduction to Kato's Euler systems, in: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds., *London Math. Soc. Lect. Notes* **254** Cambridge: Cambridge Univ. Press (1998) 379–460.

[Seo] Seo, S.: Circular distributions and Euler systems, *J. Number Theory* **93** (2002) 76–85.

[Si] Silverman, J.: The arithmetic of elliptic curves, *Graduate Texts in Math.* **106**, New York: Springer-Verlag (1986).

[T] Tate, J.: Duality theorems in Galois cohomology over number fields. In: *Proc. Intern. Cong. Math.*, Stockholm (1962) 234–241.

[We] Weston, T.: Algebraic cycles, modular forms and Euler systems, *J. für die reine und angew. Math.* **543** (2002) 103–145.

[Wi] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem, *Annals of Math.* **141** (1995) 443–551.