JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Barry MAZUR et Karl RUBIN

Controlling Selmer groups in the higher core rank case

Tome 28, nº 1 (2016), p. 145-183.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_1_145_0>

© Société Arithmétique de Bordeaux, 2016, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 145–183

Controlling Selmer groups in the higher core rank case

par Barry MAZUR et Karl RUBIN

Résumé. Nous définissons les systèmes de Kolyvagin et les systèmes de Stark attachés aux représentations p-adiques dans le cas de "core rank" (qui est une mesure du rang de Selmer générique dans une famille de groupes de Selmer) arbitraire. Les travaux antérieurs traitaient seulement le cas de "core rank" 1, où les systèmes de Kolyvagin et de Stark sont des collections de classes cohomologiques. Dans le cas général, ce sont des collections d'éléments de produits extérieurs de groupes cohomologiques. Nous montrons, sous des conditions faibles, que ces systèmes contrôlent encore la taille et la structure des groupes de Selmer, et que le module des systèmes de Kolyvagin (ou de Stark) est libre de rang 1.

Abstract. We define Kolyvagin systems and Stark systems attached to p-adic representations in the case of arbitrary "core rank" (the core rank is a measure of the generic Selmer rank in a family of Selmer groups). Previous work dealt only with the case of core rank one, where the Kolyvagin and Stark systems are collections of cohomology classes. For general core rank, they are collections of elements of exterior powers of cohomology groups. We show under mild hypotheses that for general core rank these systems still control the size and structure of Selmer groups, and that the module of all Kolyvagin (or Stark) systems is free of rank one.

Introduction

Let K be a number field and $G_K := \mathrm{Gal}(\bar{K}/K)$ its Galois group. Let R be either a principal artinian local ring, or a discrete valuation ring, and T an $R[G_K]$-module that is free over R of finite rank. Let $T^* := \mathrm{Hom}(T, \boldsymbol{\mu}_\infty)$ be its Cartier dual.

A cohomology class c in $H^1(G_K, T)$ provides (after localization and cup-product) a linear functional $\mathcal{L}_{c,v}$ on $H^1(G_{K_v}, T^*)$ for any place v of K.

Manuscrit reçu le 17 décembre 2013, accepté le 29 mai 2015.
Mathematics Subject Classification. 11G40, 11F80, 11R23, 11R34.
Mots-clefs. Euler systems, Kolyvagin systems, core rank, Selmer groups.
This material is based upon work supported by the National Science Foundation under grants DMS-1302409 and DMS-1065904.

Thanks to the duality theorems of class field theory, these $\mathcal{L}_{c,v}$, when summed over all places v of K, give a linear functional $\mathcal{L}_c$ that annihilates the adelic image of $H^1(G_K, T^*)$. By imposing local conditions on the class c, we get a linear functional that annihilates a Selmer group in $H^1(G_K, T^*)$. Following this thread, a systematic construction of classes c can be of used to control the size of Selmer groups. Even better, a sufficiently full collection (a *system*) of classes c can sometimes be used to completely determine the structure of the relevant Selmer groups.

We have just described a very vague outline of the strategy of controlling Selmer groups of Galois representations T^*, by systems of cohomology classes for T. In practice there are variants of this strategy. First, we will control the local conditions that we impose on our cohomology classes. That is, we will require our classes to lie in certain Selmer groups for T. But more importantly, in general one encounters situations where sufficiently many of the relevant Selmer groups for T are free over R of some (fixed) rank $r \geq 1$. We call r the *core rank* of T; see Definition 3.4 below. In the natural cases that we consider, all relevant Selmer groups contain a free module of rank equal to the core rank r, and r is maximal with respect to this property.

If R is a discrete valuation ring and our initial local conditions are what we call *unramified* (see Definition 5.1 and Theorem 5.4), then under mild hypotheses the core rank r of T is given by the simple formula

$$r = \sum_{v \mid \infty} \operatorname{corank} H^0(G_{K_v}, T^*).$$

So, for example, if T is the p-adic Tate module of an abelian variety of dimension d over K, then the core rank is $d\,[K : \mathbf{Q}]$.

To deal with the case where r is greater than 1 we will ask for elements in the r-th exterior powers (over R) of those Selmer groups, so that for every r we will be seeking systems of classes in R-modules that are often free of rank one over R.

One of the main aims of this article is to extend the more established theory of core rank $r = 1$ (see for example [1]) to the case of higher core rank. We deal with two types of systems of cohomology classes: *Stark systems* (collections of classes generalizing the units predicted by Stark-type conjectures) and *Kolyvagin systems* (generalizing Kolyvagin's original formulation). Our Stark systems are similar to the "unit systems" that occur in the recent work of Sano [8]. There is a third type, *Euler systems* (see for example [5] or [7]), which we do not deal with in this paper. When $r = 1$, Euler systems provide the crucial link ([1, Theorem 3.2.4]) between Kolyvagin or Stark systems and L-values. We expect that when $r > 1$ there is still a connection between Euler systems on the one hand, and Stark and Kolyvagin systems on the other, but this connection is still mysterious. For an example of the sort of connection that we expect, see the forthcoming paper [2].

The Euler systems that have been already constructed in the literature, or that are conjectured to exist, are motivic: they come from arithmetic objects such as circular units or more generally the conjectural Stark units; or—in another context—Heegner points; or elements of K-theory. Euler systems are 'vertically configured' in the sense that they provide classes in many abelian extensions of the base number field, and the classes cohere via norm projection from one abelian extension to a smaller one when modified by the multiplication of appropriate 'Euler factors' (hence the terminology 'Euler system').

On the other hand, the Stark and Kolyvagin systems are 'horizontally configured' in the sense that they consist only of cohomology classes over the base number field, but conform to a range of local conditions. The local conditions for Stark systems are more elementary and—correspondingly—the Stark systems are somewhat easier to handle than Kolyvagin systems. In contrast, the local conditions for Kolyvagin systems connect more directly with the changes of local conditions that arise from twisting the Galois representation T by characters.

One of the main results of this paper (Theorem 12.4) is that—under suitable hypotheses, but for general core rank—there is an equivalence between Stark systems and special Kolyvagin systems that we call *stub Kolyvagin systems*, and, up to a scalar unit, there is a unique 'best' Stark (equivalently: stub Kolyvagin) system (Theorems 6.7 and 7.4). We show, as mentioned in the title of this article, that the corresponding Selmer modules are controlled by (either of) these systems (Theorems 8.7 and 13.4), in the sense that there is a relatively simple description of the elementary divisors (and hence the isomorphy type) of the Selmer group of T starting with any Stark or stub Kolyvagin system. When the core rank is one, every Kolyvagin system is a stub Kolyvagin system [1, Theorem 4.4.1].

Although we have restricted our scalar rings R to be either principal artinian local rings or complete discrete valuation rings with finite residue field, it is natural to wish to extend the format of our systems of cohomology classes to encompass Galois representations T that are free of finite rank over more general complete local rings, so as to be able to deal effectively with deformational questions.

Layout of the paper. In Part 1 (sections 1–5) we recall basic facts that we will need about local and global cohomology groups, and define our abstract Selmer groups and the core rank. In Part 2 (sections 6–8) we define Stark systems and investigate the relations between Stark systems and the structure of Selmer groups. Part 3 (sections 9–14) deals with Kolyvagin systems, and the relation between Kolyvagin systems and Stark systems.

The results of [1] were restricted to the case where the base field K is $\mathbf{Q}$. In many cases the proofs for general K are the same, and in those cases we will feel free to use results from [1] without further comment.

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 $\mathbf{m}$ denote the maximal ideal of R. The basic cases to keep in mind are $R = \mathbf{Z}/p^n\mathbf{Z}$ or $R = \mathbf{Z}_p$.

If K is a field, $\bar{K}$ will denote a fixed separable closure of K and G_K the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. If A is an R-module and I is an ideal of R, we will write $A[I]$ for the submodule of A killed by I. If A is a G_K-module, we write $K(A)$ for the fixed field in $\bar{K}$ of the kernel of the map $G_K \to \mathrm{Aut}(A)$.

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

If n is a positive integer, $\boldsymbol{\mu}_n$ will denote the group of n-th roots of unity in $\bar{K}$.

Part 1. Cohomology groups and Selmer structures

1. Local cohomology groups

For this section K will be a local field (archimedean or nonarchimedean). If K is nonarchimedean let $\mathcal{O}$ be the ring of integers in K, $\mathbf{F}$ its residue field, $K^{\mathrm{ur}} \subset \bar{K}$ the maximal unramified subfield of $\bar{K}$, and $\mathcal{I}$ the inertia group $\mathrm{Gal}(\bar{K}/K^{\mathrm{ur}})$, so $G_{\mathbf{F}} = G_K/\mathcal{I} = \mathrm{Gal}(K^{\mathrm{ur}}/K)$.

Fix an R-module T endowed with a continuous G_K-action. We will denote by $H^*(K,T) := H^*(G_K,T)$ the cohomology groups computed with respect to continuous cochains.

Definition 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 I is an ideal of R, then a local condition on T induces local conditions on T/IT and $T[I]$ by taking $H^1_{\mathcal{F}}(K,T/IT)$ and $H^1_{\mathcal{F}}(K,T[I])$ to be the image and inverse image, respectively, of $H^1_{\mathcal{F}}(K,T)$ under the maps induced by

$$T \twoheadrightarrow T/IT, \qquad T[I] \hookrightarrow T.$$

One can similarly propagate the local condition $\mathcal{F}$ canonically to arbitrary subquotients of T, and if $R \to R'$ is a homomorphism of complete noetherian local PID's, then $\mathcal{F}$ induces a local condition on the R'-module $T \otimes_R R'$.

Definition 1.2. Suppose K is nonarchimedean and T is unramified (i.e. $\mathcal{I}$ acts trivially on T). Define the *finite* (or *unramified*) local condition by

$$H^1_{\mathrm{f}}(K,T) := \ker\big[H^1(K,T) \to H^1(K^{\mathrm{ur}},T)\big] = H^1(K^{\mathrm{ur}}/K,T).$$

More generally, if L is a Galois extension of K we define the L*-transverse* local condition by

$$H^1_{L\text{-tr}}(K,T) := \ker\big[H^1(K,T) \to H^1(L,T)\big] = H^1(L/K,T^{G_L}).$$

Suppose for the rest of this section that the local field K is nonarchimedean, the R-module T is of finite type, and the action of G_K on T is unramified.

Fix a totally tamely ramified cyclic extension L of K such that $[L:K]$ annihilates T. We will write simply $H^1_{\mathrm{tr}}(K,T)$ for $H^1_{L\text{-tr}}(K,T) \subset H^1(K,T)$.

Lemma 1.3.

(i) *The composition*

$$H^1_{\mathrm{tr}}(K,T) \hookrightarrow H^1(K,T) \twoheadrightarrow H^1(K,T)/H^1_{\mathrm{f}}(K,T)$$

is an isomorphism, so there is a canonical splitting

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

There are canonical functorial isomorphisms

(ii) $H^1_{\mathrm{f}}(K,T) \cong T/(\mathrm{Fr}-1)T$,

(iii) $H^1_{\mathrm{tr}}(K,T) \cong \mathrm{Hom}(\mathcal{I},T^{\mathrm{Fr}=1})$, $\quad H^1_{\mathrm{tr}}(K,T)\otimes\mathrm{Gal}(L/K) \cong T^{\mathrm{Fr}=1}$.

Proof. Assertion (i) is [1, Lemma 1.2.4]. The rest is well known; see for example [1, Lemma 1.2.1]. □

Definition 1.4. 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, and it follows that $Q(\mathrm{Fr}^{-1})T \subset T^{\mathrm{Fr}=1}$. We define the *finite-singular comparison map* ϕ^{fs} on T to be the composition, using the isomorphisms of Lemma 1.3(ii,iii),

$$H^1_{\mathrm{f}}(K,T) \xrightarrow{\sim} T/(\mathrm{Fr}-1)T \xrightarrow{Q(\mathrm{Fr}^{-1})} T^{\mathrm{Fr}=1} \xrightarrow{\sim} H^1_{\mathrm{tr}}(K,T)\otimes\mathrm{Gal}(L/K).$$

Lemma 1.5. *Suppose that T is free of finite rank over R, and $T/(\mathrm{Fr}-1)T$ is a free R-module of rank one. Then $\det(1-\mathrm{Fr}\mid T)=0$ and the map*

$$\phi^{\mathrm{fs}} : H^1_{\mathrm{f}}(K,T) \longrightarrow H^1_{\mathrm{tr}}(K,T)\otimes\mathrm{Gal}(L/K)$$

of Definition 1.4 is an isomorphism. In particular both $H^1_{\mathrm{f}}(K,T)$ and $H^1_{\mathrm{tr}}(K,T)$ are free of rank one over R.

Proof. This is [1, Lemma 1.2.3]. □

Definition 1.6. 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 $\langle\ ,\ \rangle$.

Proposition 1.7. *With notation as above, we have:*

(i) $H^1_{\mathrm{f}}(K,T)$ *and* $H^1_{\mathrm{f}}(K,T^*)$ *are orthogonal complements under* $\langle\ ,\ \rangle$.
(ii) $H^1_{\mathrm{tr}}(K,T)$ *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 [3]. Both assertions are [1, Lemma 1.3.2]. □

2. Global cohomology groups and Selmer structures

For the rest of this paper, K will be a number field and T will be a finitely generated free R-module with a continuous action of G_K, that is unramified outside a finite set of primes.

Global notation. Let $\bar{K} \subset \mathbf{C}$ be the algebraic closure of K in $\mathbf{C}$, and for each prime $\mathfrak{q}$ of K fix an algebraic closure $\overline{K_\mathfrak{q}}$ of $K_\mathfrak{q}$ containing $\bar{K}$. This determines a choice of extension of $\mathfrak{q}$ to $\bar{K}$. Let $\mathcal{D}_\mathfrak{q} := \mathrm{Gal}(\overline{K_\mathfrak{q}}/K_\mathfrak{q})$, which we identify with a closed subgroup of $G_K := \mathrm{Gal}(\bar{K}/K)$. In other words $\mathcal{D}_\mathfrak{q}$ is a particular decomposition group at $\mathfrak{q}$ in G_K, and $H^1(\mathcal{D}_\mathfrak{q}, T) = H^1(K_\mathfrak{q}, T)$. Let $\mathcal{I}_\mathfrak{q} \subset \mathcal{D}_\mathfrak{q}$ be the inertia group, and $\mathrm{Fr}_\mathfrak{q} \in \mathcal{D}_\mathfrak{q}/\mathcal{I}_\mathfrak{q}$ the Frobenius element. If T is unramified at $\mathfrak{q}$, then $\mathcal{D}_\mathfrak{q}/\mathcal{I}_\mathfrak{q}$ acts on T, and hence so does $\mathrm{Fr}_\mathfrak{q}$. If we choose a different decomposition group at $\mathfrak{q}$, then the action of $\mathrm{Fr}_\mathfrak{q}$ changes by conjugation in G_K. We will write $\mathrm{loc}_\mathfrak{q}$ for the localization map $H^1(K,T) \to H^1(K_\mathfrak{q}, T)$

If $\mathfrak{q}$ is a prime of K, let $K(\mathfrak{q})$ denote the p-part of the ray class field of K modulo $\mathfrak{q}$ (i.e. the maximal p-power extension of K in the ray class field), and $K(\mathfrak{q})_\mathfrak{q}$ the completion of $K(\mathfrak{q})$ at the chosen prime above $\mathfrak{q}$. If $\mathfrak{q}$ is principal then $K(\mathfrak{q})_\mathfrak{q}/K_\mathfrak{q}$ is cyclic and totally tamely ramified.

If $\mathfrak{q}$ is principal, T is unramified at $\mathfrak{q}$, and $[K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]T = 0$, the *transverse submodule* of $H^1(K_\mathfrak{q}, T)$ is the submodule

$$H^1_{\mathrm{tr}}(K_\mathfrak{q}, T) := H^1_{K(\mathfrak{q})_\mathfrak{q}\text{-}\mathrm{tr}}(K_\mathfrak{q}, T) = \ker\big[H^1(K_\mathfrak{q}, T) \to H^1(K(\mathfrak{q})_\mathfrak{q}, T)\big]$$

of Definition 1.2.

Definition 2.1. A *Selmer structure* $\mathcal{F}$ on T is a collection of the following data:

- a finite set $\Sigma(\mathcal{F})$ of places of K, including all infinite places, all primes above p, and all primes where T is ramified,
- for every $\mathfrak{q} \in \Sigma(\mathcal{F})$ (including archimedean places), a local condition (in the sense of Definition 1.1) on T over $K_\mathfrak{q}$, i.e. a choice of R-submodule $H^1_\mathcal{F}(K_\mathfrak{q}, T) \subset H^1(K_\mathfrak{q}, T)$.

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

$$H^1(K_{\Sigma(\mathcal{F})}/K, T) \longrightarrow \bigoplus_{\mathfrak{q}\in\Sigma(\mathcal{F})} \Big(H^1(K_\mathfrak{q}, T)/H^1_\mathcal{F}(K_\mathfrak{q}, T)\Big)$$

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

For examples of Selmer structures see [1]. Note that if $\mathcal{F}$ is a Selmer structure on T and I is an ideal of R, then $\mathcal{F}$ induces canonically (see Definition 1.1) Selmer structures on the R/I-modules T/IT and $T[I]$, that we will also denote by $\mathcal{F}$.

Definition 2.2. Suppose now that T is free over R, $\mathfrak{q} \nmid p\infty$ is prime, and T is unramified at $\mathfrak{q}$. If $\mathfrak{q}$ is principal, let $I_\mathfrak{q} \subset R$ be the largest power of $\mathbf{m}$ (i.e. $\mathbf{m}^k$ with k maximal) such that $[K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]R \subset I_\mathfrak{q}$ and $T/((\mathrm{Fr}_\mathfrak{q}-1)T+I_\mathfrak{q}T)$ is free of rank one over $R/I_\mathfrak{q}$. If no such $k \geq 1$ exists, or if $\mathfrak{q}$ is not principal, we set $I_\mathfrak{q} = R$.

Let $\mathcal{P}$ denote a set of prime ideals of K, disjoint from $\Sigma(\mathcal{F})$. Typically $\mathcal{P}$ will be a set of positive density. Define a filtration $\mathcal{P} \supset \mathcal{P}_1 \supset \mathcal{P}_2 \supset \cdots$ by

$$\mathcal{P}_k = \{\mathfrak{q} \in \mathcal{P} : I_\mathfrak{q} \subset \mathbf{m}^k\}$$

for $k \geq 1$. Let $\mathcal{N} := \mathcal{N}(\mathcal{P})$ denote the set of squarefree products of primes in $\mathcal{P}$ (with the convention that the trivial ideal $1 \in \mathcal{N}$). Let $I_1 := 0$ and if $\mathfrak{n} \in \mathcal{N}$, $\mathfrak{n} \neq 1$, define

$$I_\mathfrak{n} := \sum_{\mathfrak{q}\mid\mathfrak{n}} I_\mathfrak{q} \subset R.$$

Definition 2.3. Suppose $\mathcal{F}$ is a Selmer structure, and $\mathfrak{a}, \mathfrak{b}, \mathfrak{n}$ are pairwise relatively prime ideals of K with $\mathfrak{n} \in \mathcal{N}$ and $I_\mathfrak{n}T = 0$. Define a new Selmer structure $\mathcal{F}^\mathfrak{b}_\mathfrak{a}(\mathfrak{n})$ by

- $\Sigma(\mathcal{F}^\mathfrak{b}_\mathfrak{a}(\mathfrak{n})) := \Sigma(\mathcal{F}) \cup \{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{abn}\}$,

- $$H^1_{\mathcal{F}^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{n})}(K_{\mathfrak{q}},T) := \begin{cases} H^1_{\mathcal{F}}(K_{\mathfrak{q}},T) & \text{if } \mathfrak{q} \in \Sigma(\mathcal{F}), \\ 0 & \text{if } \mathfrak{q} \mid \mathfrak{a}, \\ H^1(K_{\mathfrak{q}},T) & \text{if } \mathfrak{q} \mid \mathfrak{b}, \\ H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) & \text{if } \mathfrak{q} \mid \mathfrak{n}. \end{cases}$$

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

If any of $\mathfrak{a},\mathfrak{b},\mathfrak{n}$ are the trivial ideal, we may suppress them from the notation. For example, we will be especially interested in Selmer groups of the form

$$H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) : \text{no restriction if } \mathfrak{q} \mid \mathfrak{n}, \text{ same as } \mathcal{F} \text{ elsewhere},$$

$$H^1_{\mathcal{F}(\mathfrak{n})}(K,T/I_{\mathfrak{n}}T) : \text{transverse condition if } \mathfrak{q} \mid \mathfrak{n}, \text{ same as } \mathcal{F} \text{ elsewhere}.$$

If $\mathfrak{m} \mid \mathfrak{n} \in \mathcal{N}$, the definition leads to an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^{\mathfrak{m}}}(K,T) \longrightarrow H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \longrightarrow \bigoplus_{\mathfrak{q}\mid(\mathfrak{n}/\mathfrak{m})} H^1(K_{\mathfrak{q}},T)/H^1_{\mathrm{f}}(K_{\mathfrak{q}},T). \tag{2.1}$$

Definition 2.4. The *dual* of T is the $R[[G_K]]$-module $T^* := \mathrm{Hom}(T,\boldsymbol{\mu}_{p^\infty})$. For every $\mathfrak{q}$ we have the local Tate pairing

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

as in §1.

Just as every local condition on T determines a local condition on T^* (Definition 1.6), 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 $\mathfrak{q} \in \Sigma(\mathcal{F})$ take $H^1_{\mathcal{F}^*}(K_{\mathfrak{q}},T^*)$ to be the local condition induced by $\mathcal{F}$, i.e. the orthogonal complement of $H^1_{\mathcal{F}}(K_{\mathfrak{q}},T)$ under $\langle\ ,\ \rangle_{\mathfrak{q}}$.

3. Selmer structures and the core rank

Suppose for this section that the R is a principal local ring. We continue to assume for the rest of this paper that T is free of finite rank over R, in addition to being a G_K-module.

Definition 3.1. A Selmer structure $\mathcal{F}$ on T is called *cartesian* if for every $\mathfrak{q} \in \Sigma(\mathcal{F})$, the local condition $\mathcal{F}$ at $\mathfrak{q}$ is "cartesian on the category of quotients of T" as defined in [1, Definition 1.1.4].

Remark 3.2. If $\mathcal{F}$ is cartesian then for every k the induced Selmer structure on the $R/\mathbf{m}^k$-module $T/\mathbf{m}^kT$ is cartesian. If R is a field (i.e. $\mathbf{m} = 0$) then every Selmer structure on T is cartesian. If R is a discrete valuation ring and $H^1(K_{\mathfrak{q}},T)/H^1_{\mathcal{F}}(K_{\mathfrak{q}},T)$ is torsion-free for every $\mathfrak{q} \in \Sigma(\mathcal{F})$, then $\mathcal{F}$ is cartesian (see [1, Lemma 3.7.1(i)]).

Proposition 3.3. *Suppose R is a principal artinian local ring of length k (i.e. $\mathbf{m}^k = 0$ and $\mathbf{m}^{k-1} \neq 0$), $\mathcal{F}$ is a cartesian Selmer structure on T, and $T^{G_K} = (T^*)^{G_K} = 0$.*

If $\mathfrak{n} \in \mathcal{N}$ and $I_\mathfrak{n} = 0$ then:

(i) *the exact sequence*

$$0 \longrightarrow T/\mathbf{m}^i T \longrightarrow T \longrightarrow T/\mathbf{m}^{k-i} T \to 0$$

induces an isomorphism $H^1_{\mathcal{F}(\mathfrak{n})}(K, T/\mathbf{m}^i T) \xrightarrow{\sim} H^1_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathbf{m}^i]$ and an exact sequence

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

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

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

(iii) *there is a unique integer r, independent of $\mathfrak{n}$, such that there is a noncanonical isomorphism*

$$\begin{aligned} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) &\cong H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) \oplus R^r \quad \text{if } r \geq 0, \\ H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \oplus R^{-r} &\cong H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) \qquad\quad \text{if } r \leq 0. \end{aligned}$$

Proof. These assertions are [1, Lemma 3.5.4], [1, Lemma 3.5.3], and [1, Theorem 4.1.5], respectively. ☐

Definition 3.4. Suppose $\mathcal{F}$ is a cartesian Selmer structure on T. If R is artinian, then the *core rank* of $(T, \mathcal{F})$ is the integer r of Proposition 3.3(iii). If R is a discrete valuation ring, then the core rank of $(T, \mathcal{F})$ is the core rank of $(T/\mathbf{m}^k T, \mathcal{F})$ for every $k > 0$, which by Proposition 3.3 is independent of k.

We will denote the core rank by $\chi(T, \mathcal{F})$, or simply $\chi(T)$ when $\mathcal{F}$ is understood.

For $\mathfrak{n} \in \mathcal{N}$, let $\nu(\mathfrak{n})$ denote the number of primes dividing $\mathfrak{n}$.

Corollary 3.5. *Suppose R is artinian, $\chi(T) \geq 0$, $\mathfrak{n} \in \mathcal{N}$, and $I_\mathfrak{n} = 0$. Let $\lambda(\mathfrak{n}) := \mathrm{length}(H^1_{(\mathcal{F}(\mathfrak{n})^*}(K, T^*))$ and $\mu(\mathfrak{n}) := \mathrm{length}(H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K, T^*))$. There are noncanonical isomorphisms*

(i) $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \cong H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) \oplus R^{\chi(T)}$,

(ii) $H^1_{\mathcal{F}^\mathfrak{n}}(K,T) \cong H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K,T^*) \oplus R^{\chi(T)+\nu(\mathfrak{n})}$,

(iii) $\mathbf{m}^{\lambda(\mathfrak{n})} \wedge^{\chi(T)} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \cong \mathbf{m}^{\lambda(\mathfrak{n})}$,

(iv) $\mathbf{m}^{\mu(\mathfrak{n})} \wedge^{\chi(T)+\nu(\mathfrak{n})} H^1_{\mathcal{F}^\mathfrak{n}}(K,T) \cong \mathbf{m}^{\mu(\mathfrak{n})}$.

Proof. The first isomorphism is just Proposition 3.3(iii). For (ii), observe that the Selmer structure $\mathcal{F}^\mathfrak{n}$ is cartesian by [1, Lemma 3.7.1(i)], so applying

Proposition 3.3(iii) to $(T, \mathcal{F}^{\mathfrak{n}})$ we have

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

To complete the proof of (ii) we need only show that $\chi(T,\mathcal{F}^{\mathfrak{n}}) = \chi(T)+\nu(\mathfrak{n})$, and this follows without difficulty from Poitou-Tate global duality (see for example [1, Theorem 2.3.4]).

Assertions (iii) and (iv) follow directly from (i) and (ii), respectively. □

4. Running hypotheses

Definition 4.1. By *Selmer data* we mean a tuple $(T, \mathcal{F}, \mathcal{P}, r)$ where

- T is a G_K-module, free of finite rank over R, unramified outside finitely many primes,
- $\mathcal{F}$ is a Selmer structure on T,
- $\mathcal{P}$ is a set of primes of K disjoint from $\Sigma(\mathcal{F})$,
- $r \geq 1$.

Definition 4.2. If L is a finite Galois extension of K and $\tau \in G_K$, define

$$\mathcal{P}(L,\tau) := \{\text{primes } \mathfrak{q} \notin \Sigma(\mathcal{F}) : \mathfrak{q} \text{ is unramified in } L/K \\ \text{and } \mathrm{Fr}_{\mathfrak{q}} \text{ is conjugate to } \tau \text{ in } \mathrm{Gal}(L/K)\}.$$

Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$ as in Definition 4.1. Let $\bar{T} = T/\mathbf{m}T$, so $\bar{T}^* = T^*[\mathbf{m}]$. If R is artinian, let M denote the smallest power of p such that $MR = 0$. If R is a discrete valuation ring, let $M := p^\infty$. Let $\mathcal{H}$ denote the Hilbert class field of K, and $\mathcal{H}_M := \mathcal{H}(\boldsymbol{\mu}_M, (\mathcal{O}_K^\times)^{1/M})$. Let $\Bbbk$ denote the residue field $R/\mathbf{m}$. In order to obtain the strongest results, we will usually make the following additional assumptions.

(H.1) $\bar{T}^{G_K} = (\bar{T}^*)^{G_K} = 0$ and $\bar{T}$ is an absolutely irreducible $\Bbbk[[G_K]]$-module,

(H.2) there is a $\tau \in \mathrm{Gal}(\bar{K}/\mathcal{H}_M)$ and a finite Galois extension L of K in $\mathcal{H}_M$ such that $T/(\tau-1)T$ is free of rank one over R and $\mathcal{P}(L,\tau) \subset \mathcal{P}$,

(H.3) $H^1(\mathcal{H}_M(T)/K, T/\mathbf{m}T) = H^1(\mathcal{H}_M(T)/K, T^*[\mathbf{m}]) = 0$,

(H.4) either $\bar{T} \not\cong \bar{T}^*$ as $\Bbbk[[G_K]]$-modules, or $p > 3$,

(H.5) the Selmer structure $\mathcal{F}$ is cartesian (Definition 3.1),

(H.6) $r = \chi(T) > 0$, where $\chi(T)$ is the core rank of T.

(Only) when R is artinian, we will also sometimes assume

(H.7) $I_{\mathfrak{q}} = 0$ for every $\mathfrak{q} \in \mathcal{P}$.

Remark 4.3. Note that if the above properties hold for $(T, \mathcal{F}, \mathcal{P}, r)$, then they also hold if R is replaced by $R/\mathbf{m}^k$ and T by $T/\mathbf{m}^k$, for $k \geq 0$. If R is artinian and (H.1) through (H.6) hold, then Lemma 4.5 below shows that (H.1) through (H.7) hold if we replace L by $\mathcal{H}_M$ and $\mathcal{P}$ by $\mathcal{P}(\mathcal{H}_M, \tau)$.

Remark 4.4. Assumption (H.5) is needed to have a well-defined notion of core rank. Assumption (H.2) is needed to provide is with a large selection of primes $\mathfrak{q}$ such that $T/(\mathrm{Fr}_\mathfrak{q} - 1, \mathbf{m}^k)$ is free of rank one, for large k.

We deduce from assumption (H.3) that restriction from K to $\mathcal{H}_M(T)$ is injective on the Selmer group; this allows us to view Selmer classes in $\mathrm{Hom}(G_{\mathcal{H}_M(T)}, T)$. Assumptions (H.1) and (H.4) then allow us to satisfy various Cebotarev conditions simultaneously.

Lemma 4.5. *Suppose R is artinian and τ is as in* (H.2). *If $\mathfrak{q} \in \mathcal{P}(\mathcal{H}_M, \tau)$, then $I_\mathfrak{q} = 0$.*

Proof. Since $\mathrm{Fr}_\mathfrak{q}$ fixes $\mathcal{H}$, $\mathfrak{q}$ is principal. By class field theory we have

$$\mathrm{Gal}(K(\mathfrak{q})_\mathfrak{q}/K_\mathfrak{q}) \cong (\mathcal{O}_K/\mathfrak{q})^\times/\mathrm{image}(\mathcal{O}_K^\times). \tag{4.1}$$

Since τ acts trivially on $\boldsymbol{\mu}_M$, so does $\mathrm{Fr}_\mathfrak{q}$, so $|(\mathcal{O}_K/\mathfrak{q})^\times|$ is cyclic of order divisible by M. Since τ acts trivially on $(\mathcal{O}_K^\times)^{1/M}$, so does $\mathrm{Fr}_\mathfrak{q}$, so the reduction of $\mathcal{O}_K^\times$ is contained in $((\mathcal{O}_K/\mathfrak{q})^\times)^M$. By (4.1) we conclude that $[K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]$ is divisible by M, so $[K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]R = 0$. We also have that $T/(\mathrm{Fr}_\mathfrak{q} - 1)T \cong T/(\tau - 1)T$ is free of rank one over R, so the lemma follows from the definition of $I_\mathfrak{q}$. □

5. Examples

5.1. A canonical Selmer structure.

Definition 5.1. When R is a discrete valuation ring, we define a canonical *unramified Selmer structure* $\mathcal{F}_{\mathrm{ur}}$ on T by

- $\Sigma(\mathcal{F}_{\mathrm{ur}}) := \{\mathfrak{q} : T \text{ is ramified at } \mathfrak{q}\} \cup \{\mathfrak{p} : \mathfrak{p} \mid p\} \cup \{v : v \mid \infty\}$,
- if $\mathfrak{q} \in \Sigma(\mathcal{F}_{\mathrm{ur}})$ and $\mathfrak{q} \nmid p\infty$ then
$$H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{q}, T) := \ker\big[H^1(K_\mathfrak{q}, T) \to H^1(K_\mathfrak{q}^{\mathrm{ur}}, T \otimes \mathbf{Q}_p)\big],$$
- if $\mathfrak{p} \mid p$ then define the universal norm subgroup
$$H^1(K_\mathfrak{p}, T)^{\mathrm{u}} := \cap_{K_\mathfrak{p} \subset L \subset K_\mathfrak{p}^{\mathrm{ur}}} \mathrm{Cor}_{L/K_\mathfrak{p}} H^1(L, T),$$
intersection over all finite unramified extensions L of $K_\mathfrak{p}$. Define
$$H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T) := H^1(K_\mathfrak{p}, T)^{\mathrm{u,sat}},$$
the saturation of $H^1(K_\mathfrak{p}, T)^{\mathrm{u}}$ in $H^1(K_\mathfrak{p}, T)$. (In other words, the quotient $H^1(K_\mathfrak{p}, T)/H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T)$ is R-torsion-free and the quotient $H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T)/H^1(K_\mathfrak{p}, T)^{\mathrm{u}}$ has finite length.)
- if $v \mid \infty$ then $H^1_{\mathcal{F}_{\mathrm{ur}}}(K_v, T) := H^1(K_v, T)$.

In other words, $H^1_{\mathcal{F}_{\mathrm{ur}}}(K, T)$ is the Selmer group of classes that (after multiplication by some power of p) are unramified away from p, and universal norms in the unramified $\mathbf{Z}_p$-extension above p.

Note that the Selmer structure $\mathcal{F}_{\mathrm{ur}}$ satisfies (H.5) by Remark 3.2.

Lemma 5.2. *If $\mathfrak{p} \mid p$ then* $\mathrm{corank}_R H^1_{\mathcal{F}^*_{\mathrm{ur}}}(K_\mathfrak{p}, T^*) = \mathrm{corank}_R H^0(K_\mathfrak{p}, T^*)$.

Proof. By the Lemma in [4, §2.1.1] (applied to the unramified $\mathbf{Z}_p$-extension of $K_\mathfrak{p}$), $H^1_{\mathcal{F}^*_{\mathrm{ur}}}(K_\mathfrak{p}, T^*)$ is the maximal divisible submodule of the image of the (injective) inflation map

$$H^1(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p}, (T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}}) \longrightarrow H^1(K_\mathfrak{p}, T^*).$$

We have

$$H^1(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p}, (T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}}) \cong (T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}}/(\gamma - 1)(T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}}$$

where γ is a topological generator of $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p})$. Thus we have an exact sequence

$$0 \longrightarrow H^0(K_\mathfrak{p}, T^*) \longrightarrow (T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}} \xrightarrow{\gamma-1} (T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}} \longrightarrow H^1(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p}, (T^*)^{G_{K_\mathfrak{p}^{\mathrm{ur}}}}) \longrightarrow 0$$

and the lemma follows. □

Corollary 5.3. *If $\mathfrak{p} \mid p$ and $H^0(K_\mathfrak{p}, T^*)$ has finite length, then*

$$H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T) = H^1(K_\mathfrak{p}, T).$$

Proof. By Lemma 5.2 $H^1_{\mathcal{F}^*_{\mathrm{ur}}}(K_\mathfrak{p}, T^*)$ has finite length, and therefore so does $H^1(K_\mathfrak{p}, T)/H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T)$. But by definition $H^1(K_\mathfrak{p}, T)/H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T)$ has no R-torsion, so $H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{p}, T) = H^1(K_\mathfrak{p}, T)$. □

Theorem 5.4. *Suppose R is a discrete valuation ring. Then*

$$\chi(T, \mathcal{F}_{\mathrm{ur}}, \mathcal{P}) = \sum_{v \mid \infty} \mathrm{corank}_R(H^0(K_v, T^*)).$$

Proof. For every $k > 0$ let $T_k = T/\mathbf{m}^k T$. 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 definition of core rank (see Definition 3.4 and Proposition 3.3(iii)), the theorem will follow if we can show that

$$\text{(5.1)}\quad \mathrm{length}(H^1_{\mathcal{F}_{\mathrm{ur}}}(K, T_k)) - \mathrm{length}(H^1_{\mathcal{F}^*_{\mathrm{ur}}}(K, T_k^*)) \sim k \sum_{v \mid \infty} \mathrm{corank}_R(H^0(K_v, T^*)).$$

By [1, Proposition 2.3.5] (which is essentially [10, Lemma 1.6]), for every $k \in \mathbf{Z}^+$

$$\begin{aligned}\text{(5.2)}\quad & \mathrm{length}(H^1_{\mathcal{F}_{\mathrm{ur}}}(K, T_k)) - \mathrm{length}(H^1_{\mathcal{F}^*_{\mathrm{ur}}}(K, T_k^*)) \\ &= \mathrm{length}(H^0(K, T_k)) - \mathrm{length}(H^0(K, T_k^*)) \\ &\quad + \sum_{v \in \Sigma(\mathcal{F}_{\mathrm{ur}})} (\mathrm{length}(H^0(K_v, T_k^*)) - \mathrm{length}(H^1_{\mathcal{F}^*_{\mathrm{ur}}}(K_v, T_k^*))).\end{aligned}$$

By hypothesis (H.1), $H^0(K,T_k) = H^0(K,T_k^*) = 0$. If $v \mid \infty$, then

$$\text{length}(H^0(K_v,T_k^*)) \sim k\ \text{corank}_R(H^0(K_v,T^*)),$$
$$\text{length}(H^1_{\mathcal{F}^*_{\text{ur}}}(K_v,T_k^*)) \sim 0.$$

Suppose $\mathfrak{q} \in \Sigma(\mathcal{F})$, $\mathfrak{q} \nmid p\infty$. Let $\mathcal{I}_\mathfrak{q}$ denote an inertia group above $\mathfrak{q}$ in G_K. By [7, Lemma 1.3.5], we have

$$\text{length}(H^1_{\mathcal{F}^*_{\text{ur}}}(K_\mathfrak{q},T_k^*)) \sim \text{length}((T_k^*)^{\mathcal{I}_\mathfrak{q}}/(\text{Fr}_\mathfrak{q}-1)(T_k^*)^{\mathcal{I}_\mathfrak{q}}).$$

On the other hand, the exact sequence

$$0 \to H^0(K_\mathfrak{q},T_k^*) \to (T_k^*)^{\mathcal{I}_\mathfrak{q}} \xrightarrow{\text{Fr}_\mathfrak{q}-1} (T_k^*)^{\mathcal{I}_\mathfrak{q}} \to (T_k^*)^{\mathcal{I}_\mathfrak{q}}/(\text{Fr}_\mathfrak{q}-1)(T_k^*)^{\mathcal{I}_\mathfrak{q}} \to 0$$

shows that

$$\text{length}(H^0(K_\mathfrak{q},T_k^*)) = \text{length}((T_k^*)^{\mathcal{I}_\mathfrak{q}}/(\text{Fr}_\mathfrak{q}-1)(T_k^*)^{\mathcal{I}_\mathfrak{q}}).$$

Thus the term for $v = \mathfrak{q}$ in (5.2) is bounded independent of k.

Now suppose $\mathfrak{p} \mid p$. By Lemma 5.2,

$$\text{corank}_R H^1_{\mathcal{F}^*}(K_\mathfrak{p},T^*) = \text{corank}_R H^0(K_\mathfrak{p},T^*).$$

By definition $H^1_{\mathcal{F}^*_{\text{ur}}}(K_\mathfrak{p},T_k^*)$ is the inverse image of $H^1_{\mathcal{F}^*_{\text{ur}}}(K_\mathfrak{p},T^*)$ under the natural map $H^1(K_\mathfrak{p},T_k^*) \to H^1(K_\mathfrak{p},T^*)[\mathbf{m}^k]$. A simple exercise shows that the kernel and cokernel of this map have length bounded independent of k, so we see that

$$\text{length}(H^1_{\mathcal{F}^*_{\text{ur}}}(K_\mathfrak{p},T_k^*)) \sim k\ \text{corank}_R H^1_{\mathcal{F}^*_{\text{ur}}}(K_\mathfrak{p},T^*) = k\ \text{corank}_R H^0(K_\mathfrak{p},T^*).$$

Thus the term for $v = \mathfrak{p}$ in (5.2) is bounded independent of k.

Combining these calculations proves (5.1), and hence the theorem. □

5.2. Multiplicative groups. Suppose K is a number field and ρ is a character of G_K of finite order. For simplicity we will assume that $p > 2$, ρ is nontrivial, and ρ takes values in $\mathbf{Z}_p^\times$. (Everything that follows holds more generally, only assuming that ρ has order prime to p, but we would have to tensor everything with the extension $\mathbf{Z}_p[\rho]$ where ρ takes its values.)

Let $T := \mathbf{Z}_p(1) \otimes \rho^{-1}$, a free $\mathbf{Z}_p$-module of rank one with G_K acting via the product of ρ^{-1} and the cyclotomic character. Let E be the cyclic extension of K cut out by ρ, i.e. such that ρ factors through an injective homomorphism $\text{Gal}(E/K) \hookrightarrow \mathbf{Z}_p^\times$. Let

$$\mathcal{P} = \{\text{primes } \mathfrak{q} \text{ of } K : \mathfrak{q} \nmid p \text{ and } \rho \text{ is unramified at } \mathfrak{q}\}.$$

A simple exercise in Galois cohomology (see for example [1, §6.1] or [7, §1.6.C]) shows that

$$H^1(K,T) \cong (E^\times \otimes \mathbf{Z}_p)^\rho$$

where the superscript ρ means the subgroup on which $\mathrm{Gal}(E/K)$ acts via ρ, and for every prime $\mathfrak{q}$,

$$H^1(K_\mathfrak{q}, T) \cong (E_\mathfrak{q}^\times \otimes \mathbf{Z}_p)^\rho$$

where $E_\mathfrak{q} = E \otimes_K K_\mathfrak{q}$ is the product of the completions of E above $\mathfrak{q}$. With these identifications, the unramified Selmer structure of Definition 5.1 is given by

$$H^1_{\mathcal{F}_{\mathrm{ur}}}(K_\mathfrak{q}, T) := (\mathcal{O}_{E,\mathfrak{q}}^\times \otimes \mathbf{Z}_p)^\rho$$

for every $\mathfrak{q}$, where $\mathcal{O}_{E,\mathfrak{q}}$ is the ring of integers of $E_\mathfrak{q}$.

Proposition 5.5. *Let* $\mathrm{Cl}(E)$ *denote the ideal class group of* E*. There are natural isomorphisms*

$$H^1_{\mathcal{F}_{\mathrm{ur}}}(K, T) \cong (\mathcal{O}_E^\times \otimes \mathbf{Z}_p)^\rho, \quad H^1_{\mathcal{F}_{\mathrm{ur}}^*}(K, T^*) \cong \mathrm{Hom}(\mathrm{Cl}(E)^\rho, \mathbf{Q}_p/\mathbf{Z}_p)$$

and for every $k \geq 0$ *an exact sequence*

$$0 \longrightarrow (\mathcal{O}_E^\times/(\mathcal{O}_E^\times)^{p^k})^\rho \longrightarrow H^1_{\mathcal{F}_{\mathrm{ur}}}(K, T/p^kT) \longrightarrow \mathrm{Cl}(E)[p^k]^\rho \longrightarrow 0$$

and an isomorphism

$$H^1_{\mathcal{F}_{\mathrm{ur}}^*}(K, T^*[p^k]) \cong \mathrm{Hom}(\mathrm{Cl}(E)^\rho, \mathbf{Z}/p^k\mathbf{Z}).$$

Proof. See for example [1, Proposition 6.1.3]. □

Suppose in addition now that $\rho \neq \omega$, and either $\rho^2 \neq \omega$ or $p > 3$, where $\omega : G_K \to \mathbf{Z}_p^\times$ is the Teichmüller character giving the action of G_K on $\boldsymbol{\mu}_p$. Then conditions (H.1), (H.3), and (H.4) of §4 all hold. By Remark 3.2, the Selmer structure $\mathcal{F}_{\mathrm{ur}}$ satisfies (H.5) as well, and condition (H.2) holds with $\tau = 1$ and $L = E$. Finally, if there is at least one real place v of K such that ρ is trivial on complex conjugation at v, then the following corollary shows that condition (H.6) holds.

Corollary 5.6. *The core rank* $\chi(T, \mathcal{F}_{\mathrm{ur}})$ *is*

$$\begin{aligned}\chi(T) = \dim_{\mathbf{F}_p}(\mathcal{O}_E^\times/(\mathcal{O}_E^\times)^p)^\rho &= \mathrm{rank}_{\mathbf{Z}_p}(\mathcal{O}_E^\times \otimes \mathbf{Z}_p)^\rho \\ &= |\{\textit{archimedean } v : \rho(\sigma_v) = 1\}|\end{aligned}$$

where $\sigma_v \in \mathrm{Gal}(E/K)$ *is the complex conjugation at* v*.*

Proof. The first equality follows from Proposition 5.5 and the definition of core rank, and the second because $\rho \neq \omega$. The third equality is well-known (using that $\rho \neq 1$); see for example [9, Proposition I.3.4]. □

Thus if E/K is an extension of totally real fields and $\rho \neq 1$, then $\chi(T, \mathcal{F}_{\mathrm{ur}}) = [K : \mathbf{Q}]$ by Corollary 5.6, and all conditions (H.1) through (H.6) are satisfied.

If $K = \mathbf{Q}$, then $\chi(T) = 1$, and a Kolyvagin system (see §10) can be constructed from the Euler system of cyclotomic units (see [1]).

For a general totally real field K, if we assume the version of Stark's Conjecture described in [6], then the so-called "Rubin-Stark" elements predicted by that conjecture can be used to construct both an Euler system and a Stark system (see §6). For the details and a thorough discussion of this example, see [2].

5.3. Abelian varieties. Suppose A is an abelian variety of dimension d defined over the number field K. Let

$$\mathcal{P} = \{\text{primes } \mathfrak{q} \text{ of } K : \mathfrak{q} \nmid p \text{ and } A \text{ has good reduction at } \mathfrak{q}\}.$$

Let T be the Tate module $T_p(A) := \varprojlim A[p^k]$. Then T is a free $\mathbf{Z}_p$-module of rank $2d$ with a natural action of G_K, and $T^* = \check{A}[p^\infty]$ where $\check{A}$ is the dual abelian variety to A.

Let $\mathcal{F}$ be the Selmer structure on T given by $H^1_{\mathcal{F}}(K_v, T) = H^1(K_v, T)$ for every v. Then $\mathcal{F}$ is the unramified Selmer structure $\mathcal{F}_{\mathrm{ur}}$ given by Definition 5.1. (For v dividing p, this follows from the Lemma in [4, §2.1.1], and for v not dividing p it follows from the fact that $H^1(K_v, T)$ is finite.) Further, $\mathcal{F}$ is the usual Selmer structure attached to an abelian variety, with the local conditions at primes above p relaxed (see for example [7, §1.6.4]). Hence we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}}(K, T^*) \longrightarrow \mathrm{Sel}_{p^\infty}(\check{A}/K) \longrightarrow \oplus_{\mathfrak{p}|p} H^1(K_{\mathfrak{p}}, \check{A}[p^\infty]).$$

Suppose now that $p > 3$, and in addition that the image of G_K in $\mathrm{Aut}(A[p]) \cong \mathrm{GL}_{2d}(\mathbf{F}_p)$ is large enough so that conditions (H.1), (H.2), and (H.3) of §4 all hold. For example, this will be true if the image of G_K contains $\mathrm{GSp}_{2d}(\mathbf{F}_p)$. Condition (H.4) holds since $p > 3$, and $\mathcal{F}$ satisfies (H.5) by Remark 3.2. The following consequence of Theorem 5.4 shows that condition (H.6) holds as well.

Proposition 5.7. *The core rank of T is given by $\chi(T) = d\,[K : \mathbf{Q}]$.*

Proof. By Theorem 5.4, we have

$$\chi(T) = \sum_{v|\infty} \mathrm{corank}_{\mathbf{Z}_p} H^0(K_v, \check{A}[p^\infty]).$$

If v is a real place, then $\mathrm{corank}_{\mathbf{Z}_p} H^0(K_v, \check{A}[p^\infty]) = d$, and if v is a complex place then $\mathrm{corank}_{\mathbf{Z}_p} H^0(K_v, \check{A}[p^\infty]) = \mathrm{corank}_{\mathbf{Z}_p} \check{A}[p^\infty] = 2d$. Thus

$$\sum_{v|\infty} \mathrm{corank}_{\mathbf{Z}_p} H^0(K_v, \check{A}[p^\infty]) = \sum_{v|\infty} d\,[K_v : \mathbf{R}] = d\,[K : \mathbf{Q}]. \qquad \square$$

If $K = \mathbf{Q}$ and $d = 1$ (i.e. A is an elliptic curve), then Proposition 5.7 shows that $\chi(T) = 1$. In this case Kato has constructed an Euler system for T, from which one can produce a Kolyvagin system ([1, Theorem 3.2.4]).

Part 2. Stark systems and the structure of Selmer groups

6. Stark systems

Suppose for this section that R is a principal artinian ring of length k, so $\mathbf{m}^k = 0$ and $\mathbf{m}^{k-1} \neq 0$. Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$ as in Definition 4.1. We assume throughout this section that (H.7) of §4 holds, i.e. $I_\mathfrak{q} = 0$ for every $\mathfrak{q} \in \mathcal{P}$.

Recall that $\nu(\mathfrak{n})$ denotes the number of prime factors of $\mathfrak{n}$.

Definition 6.1. For every $\mathfrak{n} \in \mathcal{N}$, define

$$W_\mathfrak{n} := \oplus_{\mathfrak{q}|\mathfrak{n}} \mathrm{Hom}(H^1_{\mathrm{tr}}(K_\mathfrak{q}, T), R),$$
$$Y_\mathfrak{n} := \wedge^{r+\nu(\mathfrak{n})} H^1_{\mathcal{F}^\mathfrak{n}}(K, T) \otimes \wedge^{\nu(\mathfrak{n})} W_\mathfrak{n},$$

where as usual the exterior powers are taken in the category of R-modules.

Then $W_\mathfrak{n}$ is a free R-module of rank $\nu(\mathfrak{n})$, since each $H^1_{\mathrm{tr}}(K_\mathfrak{q}, T)$ is free of rank one (Lemma 1.5). If we fix an ordering $\mathfrak{n} = \mathfrak{q}_i \cdots \mathfrak{q}_{\nu(\mathfrak{n})}$ of the primes dividing $\mathfrak{n}$, and a generator h_i of $\mathrm{Hom}(H^1_{\mathrm{tr}}(K_{\mathfrak{q}_i}, T), R)$ for every i, then $h_1 \wedge \cdots \wedge h_{\nu(\mathfrak{n})}$ is a generator of the free, rank-one R-module $\wedge^{\nu(\mathfrak{n})} W_\mathfrak{n}$.

For the structure of $Y_\mathfrak{n}$ when r is the core rank of T, see Lemma 6.6 below.

Definition 6.2. For every $\mathfrak{q} \in \mathcal{P}$, define the transverse localization map

$$\mathrm{loc}^{\mathrm{tr}}_\mathfrak{q} : H^1(K, T) \xrightarrow{\mathrm{loc}_\mathfrak{q}} H^1(K_\mathfrak{q}, T) \twoheadrightarrow H^1_{\mathrm{tr}}(K_\mathfrak{q}, T),$$

where the second map is projection (using the direct sum decomposition of Lemma 1.3(i)) with kernel $H^1_{\mathrm{f}}(K_\mathfrak{q}, T)$. If $\mathfrak{n} \in \mathcal{N}$ and $\mathfrak{q} \mid \mathfrak{n}$, then

$$\ker\big(\mathrm{loc}^{\mathrm{tr}}_\mathfrak{q} | H^1_{\mathcal{F}^\mathfrak{n}}(K, T)\big) = H^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{q}}}(K, T). \tag{6.1}$$

In exactly the same way, we can define a composition $\mathrm{loc}^{\mathrm{f}}_\mathfrak{q}$ by using the finite projection and the isomorphism $\phi^{\mathrm{fs}}_\mathfrak{q}$ of Definition 1.4

$$\mathrm{loc}^{\mathrm{f}}_\mathfrak{q} : H^1(K, T) \xrightarrow{\mathrm{loc}_\mathfrak{q}} H^1(K_\mathfrak{q}, T) \twoheadrightarrow H^1_{\mathrm{f}}(K, T)$$
$$\xrightarrow{\phi^{\mathrm{fs}}_\mathfrak{q}} H^1_{\mathrm{tr}}(K_\mathfrak{q}, T) \otimes \mathrm{Gal}(K(\mathfrak{q})_\mathfrak{q}/K_\mathfrak{q}),$$

and then

$$\ker\big(\mathrm{loc}^{\mathrm{f}}_\mathfrak{q} | H^1_{\mathcal{F}^\mathfrak{n}}(K, T)\big) = H^1_{\mathcal{F}^{\mathfrak{n}/\mathfrak{q}}_{(\mathfrak{q})}}(K, T). \tag{6.2}$$

Definition 6.3. Suppose $\mathfrak{n} \in \mathcal{N}$ and $\mathfrak{m} \mid \mathfrak{n}$. By (6.1) we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^\mathfrak{m}}(K, T) \longrightarrow H^1_{\mathcal{F}^\mathfrak{n}}(K, T) \xrightarrow{\oplus \mathrm{loc}^{\mathrm{tr}}_\mathfrak{q}} \bigoplus_{\mathfrak{q}|(\mathfrak{n}/\mathfrak{m})} H^1_{\mathrm{tr}}(K_\mathfrak{q}, T)$$

and it follows that the square

$$
(6.3)\qquad \begin{array}{ccc}
H^1_{\mathcal{F}^{\mathfrak{m}}}(K,T) & \hookrightarrow & H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \\
\downarrow{\scriptstyle \oplus\mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}}} & & \downarrow{\scriptstyle \oplus\mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}}} \\
\bigoplus_{\mathfrak{q}\mid\mathfrak{m}} H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) & \hookrightarrow & \bigoplus_{\mathfrak{q}\mid\mathfrak{n}} H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T)
\end{array}
$$

is cartesian. Let

$$\Psi_{\mathfrak{n},\mathfrak{m}} : Y_{\mathfrak{n}} \longrightarrow Y_{\mathfrak{m}}$$

be the map of Proposition A.2(i) attached to this diagram.

Concretely, $\Psi_{\mathfrak{n},\mathfrak{m}}$ is given as follows. Fix a factorization $\mathfrak{n} = \mathfrak{q}_1 \cdots \mathfrak{q}_t$, with $\mathfrak{m} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, and a generator h_i of $\mathrm{Hom}(H^1_{\mathrm{tr}}(K_{\mathfrak{q}_i},T),R)$ for every i. Let $\mathfrak{n}_i = \prod_{j\leq i} \mathfrak{q}_j$. These choices lead to a map

$$\widehat{h_{s+1} \circ \mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}_{s+1}}} \circ \cdots \circ \widehat{h_t \circ \mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}_t}} : \wedge^{r+t} H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \longrightarrow \wedge^{r+s} H^1_{\mathcal{F}^{\mathfrak{m}}}(K,T)$$

(where $\widehat{h_i \circ \mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}_i}} : \wedge^i H^1_{\mathcal{F}^{\mathfrak{n}_i}}(K,T) \to \wedge^{i-1} H^1_{\mathcal{F}^{\mathfrak{n}_{i-1}}}(K,T)$ is given by Proposition A.1) and an isomorphism $\wedge^{\nu(\mathfrak{n})} W_{\mathfrak{n}} \xrightarrow{\sim} \wedge^{\nu(\mathfrak{m})} W_{\mathfrak{m}}$ given by

$$h_1 \wedge \cdots \wedge h_t \mapsto h_1 \wedge \cdots \wedge h_s.$$

The tensor product of these two maps is the map $\Psi_{\mathfrak{n},\mathfrak{m}} : Y_{\mathfrak{n}} \longrightarrow Y_{\mathfrak{m}}$, and is independent of the choices made.

Proposition 6.4. *Suppose* $\mathfrak{n} \in \mathcal{N}$, $\mathfrak{n}' \mid \mathfrak{n}$, *and* $\mathfrak{n}'' \mid \mathfrak{n}'$. *Then*

$$\Psi_{\mathfrak{n}',\mathfrak{n}''} \circ \Psi_{\mathfrak{n},\mathfrak{n}'} = \Psi_{\mathfrak{n},\mathfrak{n}''}.$$

Proof. This is Proposition A.2(iii). □

Definition 6.5. Thanks to Proposition 6.4, we can define the R-module $\mathbf{SS}_r(T) = \mathbf{SS}_r(T,\mathcal{F},\mathcal{P})$ of *Stark systems of rank* r to be the inverse limit

$$\mathbf{SS}_r(T) := \varprojlim_{\mathfrak{n}\in\mathcal{N}} Y_{\mathfrak{n}}$$

with respect to the maps $\Psi_{\mathfrak{n},\mathfrak{m}}$.

We call these collections Stark systems because a fundamental example is given by elements predicted by a generalized Stark conjecture [2, 6].

Let $Y'_{\mathfrak{n}} = \mathbf{m}^{\mathrm{length}(H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*))} Y_{\mathfrak{n}}$.

Lemma 6.6. *Suppose that hypotheses* (H.1) *through* (H.7) *of §4 are satisfied, so in particular* r *is the core rank of* T. *Then:*

(i) $Y'_{\mathfrak{n}}$ *is a cyclic* R*-module of length* $\max\{k - \mathrm{length}(H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*)), 0\}$.

(ii) *There are* $\mathfrak{n} \in \mathcal{N}$ *such that* $H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*) = 0$.

(iii) *If* $H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*) = 0$ *then* $Y_{\mathfrak{n}}$ *is free of rank one over* R.

(iv) *If* $H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*) = 0$ *and* $\mathfrak{m} \mid \mathfrak{n}$, *then* $\Psi_{\mathfrak{n},\mathfrak{m}}(Y_{\mathfrak{n}}) = Y'_{\mathfrak{m}}$.

Proof. Assertions (i) and (iii) follow directly from Corollary 3.5(iv). Since $H^1_{\mathcal{F}^*}(K,T^*)$ is finite, we can choose generators $c_1,\ldots,c_t$ of $H^1_{\mathcal{F}^*}(K,T^*)[\mathbf{m}]$. For each i, use [1, Proposition 3.6.1] to choose $\mathfrak{q}_i \in \mathcal{N}$ such that $\mathrm{loc}_{\mathfrak{q}_i}(c_i) \neq 0$, and let $\mathfrak{n} = \prod_i \mathfrak{q}_i$. Then $H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K,T^*) = 0$, so (ii) holds.

Proposition A.2(ii) applied to the diagram (6.3) shows that

$$\Psi_{\mathfrak{n},\mathfrak{m}}(Y_\mathfrak{n}) = \mathbf{m}^{\mathrm{length}(H^1_{\mathcal{F}^\mathfrak{m}}(K,T))-(r+\nu(\mathfrak{m}))k}Y_\mathfrak{m}.$$

Corollary 3.5(ii) shows that

$$\mathrm{length}(H^1_{\mathcal{F}^\mathfrak{m}}(K,T)) - (r+\nu(\mathfrak{m}))k = \mathrm{length}(H^1_{(\mathcal{F}^*)_\mathfrak{m}}(K,T^*))$$

which proves (iv). □

Theorem 6.7. *Suppose that hypotheses* (H.1) *through* (H.7) *of §4 are satisfied. Then the R-module $\mathbf{SS}_r(T)$ is free of rank one, and for every $\mathfrak{n} \in \mathcal{N}$, the image of the projection map $\mathbf{SS}_r(T) \to Y_\mathfrak{n}$ is $Y'_\mathfrak{n}$.*

Proof. Using Lemma 6.6(ii), choose an $\mathfrak{d} \in \mathcal{N}$ such that $H^1_{(\mathcal{F}^*)_\mathfrak{d}}(K,T^*) = 0$. Then $H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K,T) = 0$ for every $\mathfrak{n} \in \mathcal{N}$ divisible by $\mathfrak{d}$. Now the theorem follows from Lemma 6.6(iv). □

7. Stark systems over discrete valuation rings

For this section we assume that R is a discrete valuation ring, and we fix Selmer data $(T,\mathcal{F},\mathcal{P},r)$ as in Definition 4.1. We assume throughout this section that hypotheses (H.1) through (H.6) of §4 are satisfied. For $k > 0$ recall from Definition 2.2 that

$$\mathcal{P}_k := \{\mathfrak{q} \in \mathcal{P} : I_\mathfrak{q} \in \mathbf{m}^k\},$$

and $\mathcal{N}_k$ is the set of squarefree products of primes in $\mathcal{P}_k$. By Remark 4.3, the Selmer data $(T/\mathbf{m}^kT,\mathcal{F},\mathcal{P}_k,r)$ satisfies (H.1) through (H.7) over the ring $R/\mathbf{m}^k$. In this section we will define the module $\mathbf{SS}_r(T)$ of Stark systems of rank r over T, and use the results of §6 about $\mathbf{SS}_r(T/\mathbf{m}^kT)$ to study $\mathbf{SS}_r(T)$.

Definition 7.1. For every $\mathfrak{n} \in \mathcal{N}$, define

$$\begin{aligned} W_\mathfrak{n} &:= \oplus_{\mathfrak{q}|\mathfrak{n}}\mathrm{Hom}(H^1_{\mathrm{tr}}(K_\mathfrak{q},T/I_\mathfrak{n}T),R/I_\mathfrak{n}),\\ Y_\mathfrak{n} &:= \wedge^{r+\nu(\mathfrak{n})}H^1_{\mathcal{F}^\mathfrak{n}}(K,T/I_\mathfrak{n}T)\otimes\wedge^{\nu(\mathfrak{n})}W_\mathfrak{n},\\ Y'_\mathfrak{n} &:= \mathbf{m}^{\mathrm{length}(H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K,T^*[I_\mathfrak{n}]))}Y_\mathfrak{n}.\end{aligned}$$

A *Stark system of rank r for T* (more precisely, for $(T,\mathcal{F},\mathcal{P})$) is a collection $\{\epsilon_\mathfrak{n} \in Y_\mathfrak{n} : \mathfrak{n} \in \mathcal{N}\}$ such that if $\mathfrak{n} \in \mathcal{N}$ and $\mathfrak{m} \mid \mathfrak{n}$, then

$$\Psi_{\mathfrak{n},\mathfrak{m}}(\epsilon_\mathfrak{n}) = \bar{\epsilon}_\mathfrak{m}$$

where $\bar{\epsilon}_{\mathfrak{m}}$ is the image of $\epsilon_{\mathfrak{m}}$ in $Y_{\mathfrak{m}} \otimes R/I_{\mathfrak{n}}$, and $\Psi_{\mathfrak{n},\mathfrak{m}} : Y_{\mathfrak{n}} \to Y_{\mathfrak{m}} \otimes R/I_{\mathfrak{n}}$ is the map of Definition 6.3 applied to $T/I_{\mathfrak{n}}T$ and $R/I_{\mathfrak{n}}$. Denote by $\mathbf{SS}_r(T) = \mathbf{SS}_r(T, \mathcal{F}, \mathcal{P})$ the R-module of Stark systems for T.

Lemma 7.2. *If $j \le k$, then the projection map $T/\mathbf{m}^kT \to T/\mathbf{m}^jT$ and restriction to $\mathcal{P}_k$ induce a surjection and an isomorphism, respectively*

$$\mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k) \twoheadrightarrow \mathbf{SS}_r(T/\mathbf{m}^jT, \mathcal{P}_k) \xleftarrow{\sim} \mathbf{SS}_r(T/\mathbf{m}^jT, \mathcal{P}_j)$$

Proof. Let $\mathfrak{n} \in \mathcal{N}_k$ be such that $H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K, T^*[\mathbf{m}]) = 0$. Then by Theorem 6.7, projecting to $Y_{\mathfrak{n}}$ gives a commutative diagram with vertical isomorphisms

$$\begin{array}{ccccc} \mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k) & \longrightarrow & \mathbf{SS}_r(T/\mathbf{m}^jT, \mathcal{P}_k) & \longleftarrow & \mathbf{SS}_r(T/\mathbf{m}^jT, \mathcal{P}_j) \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ Y_{\mathfrak{n}} \otimes R/\mathbf{m}^k & \twoheadrightarrow & Y_{\mathfrak{n}} \otimes R/\mathbf{m}^j & \xleftarrow{=} & Y_{\mathfrak{n}} \otimes R/\mathbf{m}^j \end{array}$$

Since the bottom maps are a surjection and an isomorphism, so are the top ones. □

Proposition 7.3. *The natural maps $T \twoheadrightarrow T/\mathbf{m}^k$ and $\mathcal{P}_k \hookrightarrow \mathcal{P}$ induce an isomorphism*

$$\mathbf{SS}_r(T, \mathcal{P}) \xrightarrow{\sim} \varprojlim \mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k)$$

where the inverse limit is with respect to the maps of Lemma 7.2.

Proof. Suppose $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$ is nonzero. Then we can find an $\mathfrak{n}$ such that $\epsilon_{\mathfrak{n}} \neq 0$ in $Y_{\mathfrak{n}}$. If $\mathfrak{n} \neq 1$ then $I_{\mathfrak{n}} \neq 0$, and we let k be such that $\mathbf{m}^k = I_{\mathfrak{n}}$. If $\mathfrak{n} = 1$ choose k so that $\epsilon_1 \neq 0$ in $\wedge^r H^1_{\mathcal{F}}(K, T/\mathbf{m}^kT)$. In either case $I_{\mathfrak{n}} \subset \mathbf{m}^k$, and the image of $\boldsymbol{\epsilon}$ in $\mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k)$ is nonzero. Thus the map in the proposition is injective.

Now suppose $\{\boldsymbol{\epsilon}^{(k)}\} \in \varprojlim \mathbf{SS}_r(T/\mathbf{m}^k, \mathcal{P}_k)$. If $\mathfrak{n} \in \mathcal{N}$ and $\mathfrak{n} \neq 1$, let j be such that $I_{\mathfrak{n}} = \mathbf{m}^j$ and define

$$\epsilon_{\mathfrak{n}} := \epsilon_{\mathfrak{n}}^{(j)} \in Y_{\mathfrak{n}}.$$

If $\mathfrak{n} = 1$, define

$$\epsilon_1 = \lim_{k\to\infty} \epsilon_1^{(k)} \in \lim_{k\to\infty} \wedge^r H^1_{\mathcal{F}}(K, T/\mathbf{m}^kT) = \wedge^r H^1_{\mathcal{F}}(K, T) = Y_1.$$

It is straightforward to verify that this defines an element $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T, \mathcal{P})$ that maps to $\boldsymbol{\epsilon}^{(k)} \in \mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k)$ for every k. Thus the map in the proposition is surjective as well. □

Theorem 7.4. *Suppose R is a discrete valuation ring and hypotheses (H.1) through (H.6) hold. Then the R-module of Stark systems of rank r, $\mathbf{SS}_r(T, \mathcal{P})$, is free of rank one, generated by a Stark system $\boldsymbol{\epsilon}$ whose image in*

$\mathbf{SS}_r(T/\mathbf{m}T, \mathcal{P})$ is nonzero. The map $\mathbf{SS}_r(T,\mathcal{P}) \to \mathbf{SS}_r(T/\mathbf{m}^k, \mathcal{P}_k)$ is surjective for every k.

Proof. By Theorem 6.7, $\mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k)$ is free of rank one over $R/\mathbf{m}^k$ for every k. The maps $\mathbf{SS}_r(T/\mathbf{m}^{k+1}T, \mathcal{P}_{k+1}) \to \mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k)$ are surjective by Lemma 7.2, so the theorem follows from Proposition 7.3. □

8. Structure of the dual Selmer group

In this section R is either a principal artinian local ring or a discrete valuation ring. We let $k := \mathrm{length}(R)$, so k is finite in the artinian case and $k = \infty$ in the discrete valuation ring case.

Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$. We continue to assume that hypotheses (H.1) through (H.6) are satisfied, and if R is artinian we assume that (H.7) is satisfied as well. Recall that if $\mathfrak{n} \in \mathcal{N}$ then $\nu(\mathfrak{n})$ denotes the number of prime divisors of $\mathfrak{n}$.

Definition 8.1. Define functions $\mu, \lambda, \varphi_{\boldsymbol{\epsilon}} \in \mathrm{Maps}(\mathcal{N}, \mathbf{Z}_{\geq 0} \cup \{\infty\})$

- $\mu(\mathfrak{n}) = \mathrm{length}(H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K, T^*))$,
- $\lambda(\mathfrak{n}) = \mathrm{length}(H^1_{\mathcal{F}(\mathfrak{n})^*}(K, T^*))$,

and if $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$ is a Stark system

- $\varphi_{\boldsymbol{\epsilon}}(\mathfrak{n}) = \max\{j : \epsilon_\mathfrak{n} \in \mathbf{m}^j Y_\mathfrak{n}\}$.

Define $\partial : \mathrm{Maps}(\mathcal{N}, \mathbf{Z}_{\geq 0} \cup \{\infty\}) \to \mathrm{Maps}(\mathbf{Z}_{\geq 0}, \mathbf{Z}_{\geq 0} \cup \{\infty\})$ by

$$\partial f(i) = \min\{f(\mathfrak{n}) : \mathfrak{n} \in \mathcal{N} \text{ and } \nu(\mathfrak{n}) = i\}.$$

Definition 8.2. The *order of vanishing* of a nonzero Stark system $\boldsymbol{\epsilon}$ in $\mathbf{SS}_r(T)$ is

$$\mathrm{ord}(\boldsymbol{\epsilon}) := \min\{\nu(\mathfrak{n}) : \mathfrak{n} \in \mathcal{N}, \epsilon_\mathfrak{n} \neq 0\} = \min\{i : \partial\varphi_{\boldsymbol{\epsilon}}(i) \neq \infty\}.$$

We say $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$ is *primitive* if its image in $\mathbf{SS}_r(T/\mathbf{m}T)$ is nonzero. We also define the sequence of *elementary divisors*

$$d_{\boldsymbol{\epsilon}}(i) := \partial\varphi_{\boldsymbol{\epsilon}}(i) - \partial\varphi_{\boldsymbol{\epsilon}}(i+1), \quad i \geq \mathrm{ord}(\boldsymbol{\epsilon}).$$

Note that $\partial\varphi_{\boldsymbol{\epsilon}}(i) = \infty$ if $i < \mathrm{ord}(\boldsymbol{\epsilon})$; Theorems 8.5 and 8.7 below show that the converse is true as well, so the $d_{\boldsymbol{\epsilon}}(i)$ are well-defined and finite.

Proposition 8.3. *Suppose R is artinian, and $H^1_{\mathcal{F}^*}(K, T^*) \cong \oplus_{i \geq 1} R/\mathbf{m}^{e_i}$ with $e_1 \geq e_2 \geq \cdots$. Then for every $t \geq 0$,*

$$\partial\lambda(t) = \partial\mu(t) = \sum_{i > t} e_i.$$

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

$$H^1_{\mathcal{F}^*}(K, T^*) \longrightarrow \bigoplus_{\mathfrak{q} \mid \mathfrak{n}} H^1_{\mathrm{f}}(K_\mathfrak{q}, T^*).$$

The right-hand side is free of rank t over R, and R is principal, so the image is a quotient of $H^1_{\mathcal{F}^*}(K,T^*)$ generated by (at most) t elements. Hence the image has length at most $\sum_{i\le t} e_i$, so the kernel has length at least $\sum_{i>t} e_i$. But by definition this kernel is $H^1_{(\mathcal{F}^*)_\mathfrak{n}}(K,T^*)$, which is contained in $H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*)$, so

$$\lambda(\mathfrak{n}) \ge \mu(\mathfrak{n}) \ge \sum_{i>t} e_i. \tag{8.1}$$

We will prove by induction on t that $\mathfrak{n}$ can be chosen so that $\nu(\mathfrak{n}) = t$ and $H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) \cong \oplus_{i>t} R/\mathbf{m}^{e_i}$. For such an $\mathfrak{n}$ equality holds in (8.1), and the lemma follows. When $t = 0$ we can just take $\mathfrak{n} = 1$.

Suppose $t \ge 1$, $\mathfrak{n} \in \mathcal{N}$, $\nu(\mathfrak{n}) = t-1$, and $H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) \cong \oplus_{i>t-1} R/\mathbf{m}^{e_i}$. Since $\chi(T) > 0$, Corollary 3.5 shows that $\mathbf{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \ne 0$. Fix a nonzero element $c \in \mathbf{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \subset H^1_{\mathcal{F}(\mathfrak{n})}(K,T)[\mathbf{m}]$. If $e_t > 0$ then choose a nonzero element $c' \in \mathbf{m}^{e_t-1} H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) \subset H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*)[\mathbf{m}]$. By [1, Proposition 3.6.1] we can use the Cebotarev theorem to choose a prime $\mathfrak{q} \in \mathcal{P}$ such that the localization $\mathrm{loc}_\mathfrak{q}(c) \ne 0$ and, if $e_t > 0$, such that $\mathrm{loc}_\mathfrak{q}(c') \ne 0$ as well.

Since $H^1_\mathrm{f}(K_\mathfrak{q},T)$ is free of rank one over R, and (by our choice of $\mathfrak{q}$) the localization of $\mathbf{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K,T)$ at $\mathfrak{q}$ is nonzero, it follows that the localization map $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_\mathrm{f}(K_\mathfrak{q},T)$ is surjective. Similarly, we have that $H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*)$ has exponent $\mathbf{m}^{e_t}$, and if $e_t > 0$ then the localization of $\mathbf{m}^{e_t-1} H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*)$ at $\mathfrak{q}$ is nonzero, so

$$H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*)/H^1_{\mathcal{F}^\mathfrak{q}(\mathfrak{n})^*}(K,T^*) \cong \mathrm{loc}_\mathfrak{q}(H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*)) \cong R/\mathbf{m}^{e_t}$$

and therefore $H^1_{\mathcal{F}^\mathfrak{q}(\mathfrak{n})^*}(K,T^*) \cong \oplus_{i>t} R/\mathbf{m}^{e_i}$. By [1, Theorem 4.1.7(ii)] we have $H^1_{\mathcal{F}(\mathfrak{n}\mathfrak{q})^*}(K,T^*) = H^1_{\mathcal{F}^\mathfrak{q}(\mathfrak{n})^*}(K,T^*)$, so $\mathfrak{n}\mathfrak{q} \in \mathcal{N}$ has the desired property. □

Proposition 8.4. *Suppose R is artinian of length k, and $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$. Fix $s \ge 0$ such that $\boldsymbol{\epsilon}$ generates $\mathbf{m}^s \mathbf{SS}_r(T)$, and integers $e_1 \ge e_2 \ge \cdots \ge 0$ such that*

$$H^1_{\mathcal{F}^*}(K,T^*) \cong \oplus_i R/\mathbf{m}^{e_i}.$$

Then for every $t \ge 0$,

$$\partial\varphi_{\boldsymbol{\epsilon}}(t) = \begin{cases} s + \sum_{i>t} e_i & \text{if } s + \sum_{i>t} e_i < k, \\ \infty & \text{if } s + \sum_{i>t} e_i \ge k. \end{cases}$$

Proof. It is enough to prove the proposition when $s = 0$, and the general case will follow. So we may assume that $\boldsymbol{\epsilon}$ generates $\mathbf{SS}_r(T)$. By Theorem 6.7 and Lemma 6.6(i), we have that $\epsilon_\mathfrak{n}$ generates $Y'_\mathfrak{n} = \mathbf{m}^{\mu(\mathfrak{n})} Y_\mathfrak{n}$, which is cyclic of length $\max\{k-\mu(\mathfrak{n}),0\}$. Hence $\epsilon_\mathfrak{n} \in \mathbf{m}^{\mu(\mathfrak{n})}Y_\mathfrak{n}$, and $\epsilon_\mathfrak{n} \in \mathbf{m}^{\mu(\mathfrak{n})+1}Y_\mathfrak{n}$ if and only if $\mu(\mathfrak{n}) \geq k$. Therefore

$$\partial\varphi_{\boldsymbol{\epsilon}}(t) = \begin{cases} \partial\mu(t) & \text{if } \partial\mu(t) < k, \\ \infty & \text{if } \partial\mu(t) \geq k. \end{cases}$$

Now the proposition follows from the calculation of $\partial\mu(t)$ in Lemma 8.3. ☐

Theorem 8.5. *Suppose R is artinian, $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$, and $\epsilon_1 \neq 0$. Then*

$$\begin{aligned} \partial\varphi_{\boldsymbol{\epsilon}}(0) \geq \partial\varphi_{\boldsymbol{\epsilon}}(1) \geq \partial\varphi_{\boldsymbol{\epsilon}}(2) \geq \cdots, \\ d_{\boldsymbol{\epsilon}}(0) \ \geq \ d_{\boldsymbol{\epsilon}}(1) \ \geq \ d_{\boldsymbol{\epsilon}}(2) \ \geq \ \cdots \ \geq 0, \end{aligned}$$

and

$$H^1_{\mathcal{F}^*}(K,T^*) \cong \bigoplus_{i\geq 0} R/\mathbf{m}^{d_{\boldsymbol{\epsilon}}(i)}.$$

Proof. Let s be such that $\boldsymbol{\epsilon}$ generates $\mathbf{m}^s\mathbf{SS}_r(T)$. If $\epsilon_1 \neq 0$ then $\partial\varphi_{\boldsymbol{\epsilon}}(0) < k$, so in Proposition 8.4 we have $\partial\varphi_{\boldsymbol{\epsilon}}(t) = s + \sum_{i>t} e_i$ for every t. The theorem follows directly. ☐

If R is a discrete valuation ring then F will denote the field of fractions of R, and if M is an R-module we define

- $\mathrm{rank}_R M := \dim_F M \otimes F$,
- $\mathrm{corank}_R M := \mathrm{rank}_R \mathrm{Hom}_R(M, F/R)$,
- M_{div} is the maximal divisible submodule of M.

Proposition 8.6. *Suppose R is a discrete valuation ring, and $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$ generates $\mathbf{m}^s\mathbf{SS}_r(T)$. Let $a := \mathrm{corank}_R(H^1_{\mathcal{F}^*}(K,T^*))$ and write*

$$H^1_{\mathcal{F}^*}(K,T^*)/(H^1_{\mathcal{F}^*}(K,T^*))_{\mathrm{div}} \cong \bigoplus_{i>a} R/\mathbf{m}^{e_i}$$

with $e_{a+1} \geq e_{a+2} \geq \cdots$. Then

$$\partial\varphi_{\boldsymbol{\epsilon}}(t) = \begin{cases} \infty & \textit{if } t < a, \\ s + \sum_{i>t} e_i & \textit{if } t \geq a. \end{cases}$$

Proof. Let $e_1 = \cdots = e_a := \infty$. Since

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

Proposition 3.3(ii) applied to all the $T/\mathbf{m}^kT$ shows that for every $k \in \mathbf{Z}^+$ we have

$$H^1_{\mathcal{F}^*}(K,T^*[\mathbf{m}^k]) = H^1_{\mathcal{F}^*}(K,T^*)[\mathbf{m}^k] \cong \bigoplus_{i\geq 1} R/\mathbf{m}^{\min\{k,e_i\}}. \tag{8.2}$$

For every $k \geq 0$ let $\boldsymbol{\epsilon}^{(k)}$ denote the image of $\boldsymbol{\epsilon}$ in $\mathbf{SS}_r(T/\mathbf{m}^kT, \mathcal{P}_k)$. Fix $s \geq 0$ such that $\boldsymbol{\epsilon}$ generates $\mathbf{m}^s\mathbf{SS}_r(T)$. Then by Theorem 7.4, $\boldsymbol{\epsilon}^{(k)}$ generates $\mathbf{m}^s\mathbf{SS}_r(T/\mathbf{m}^kT)$ for every k.

Fix t, and choose $\mathfrak{n} \in \mathcal{N}$ with $\nu(\mathfrak{n}) = t$. Let k be such that $I_\mathfrak{n} = \mathbf{m}^k$. By (8.2) and Proposition 8.4 we have

$$\epsilon_\mathfrak{n}^{(k)} \begin{cases} = 0 & \text{if } t < a, \\ \in \mathbf{m}^{s+\sum_{i>t} e_i} Y_\mathfrak{n} & \text{if } t > a. \end{cases}$$

But $\epsilon_\mathfrak{n}^{(k)} = \epsilon_\mathfrak{n} \in Y_\mathfrak{n}$, so we conclude that

$$\partial\varphi_{\boldsymbol{\epsilon}}(t) \begin{cases} = \infty & \text{if } t < a, \\ \geq s + \sum_{i>t} e_i & \text{if } t \geq a. \end{cases}$$

Now suppose $t \geq a$, and fix $k > s + \sum_{i>t} e_i$. By Proposition 8.4 we can find $\mathfrak{n} \in \mathcal{N}$ with $I_\mathfrak{n} \subset \mathbf{m}^k$ such that $\epsilon_\mathfrak{n}^{(k)} \notin \mathbf{m}^{s+1+\sum_{i>t} e_i} Y_\mathfrak{n}$. Since $\epsilon_\mathfrak{n}^{(k)}$ is the image of $\epsilon_\mathfrak{n}$, we have that $\epsilon_\mathfrak{n} \notin \mathbf{m}^{s+1+\sum_{i>t} e_i} Y_\mathfrak{n}$. This shows that $\partial\varphi_{\boldsymbol{\epsilon}}(t) \leq s + \sum_{i>t} e_i$, and the proof is complete. □

Theorem 8.7. *Suppose R is a discrete valuation ring, $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$ and $\boldsymbol{\epsilon} \neq 0$. Then:*

(i) *the sequence $\partial\varphi_{\boldsymbol{\epsilon}}(t)$ is nonincreasing, finite for $t \geq \operatorname{ord}(\boldsymbol{\epsilon})$, and nonnegative,*

(ii) *the sequence $d_{\boldsymbol{\epsilon}}(i)$ is nonincreasing, finite for $i \geq \operatorname{ord}(\boldsymbol{\epsilon})$, and nonnegative,*

(iii) $\operatorname{ord}(\boldsymbol{\epsilon})$ *and the $d_{\boldsymbol{\epsilon}}(i)$ are independent of the choice of nonzero $\boldsymbol{\epsilon}$ in* $\mathbf{SS}_r(T)$,

(iv) $\operatorname{corank}_R(H^1_{\mathcal{F}^*}(K, T^*)) = \operatorname{ord}(\boldsymbol{\epsilon})$,

(v) $H^1_{\mathcal{F}^*}(K, T^*)/(H^1_{\mathcal{F}^*}(K, T^*))_{\mathrm{div}} \cong \oplus_{i \geq \operatorname{ord}(\boldsymbol{\epsilon})} R/\mathbf{m}^{d_{\boldsymbol{\epsilon}}(i)}$,

(vi) $\operatorname{length}_R(H^1_{\mathcal{F}^*}(K, T^*)/(H^1_{\mathcal{F}^*}(K, T^*))_{\mathrm{div}}) = \partial\varphi_{\boldsymbol{\epsilon}}(\operatorname{ord}(\boldsymbol{\epsilon})) - \partial\varphi_{\boldsymbol{\epsilon}}(\infty)$, *where* $\partial\varphi_{\boldsymbol{\epsilon}}(\infty) := \lim_{t\to\infty} \partial\varphi_{\boldsymbol{\epsilon}}(t)$,

(vii) $\boldsymbol{\epsilon}$ *is primitive if and only if* $\partial\varphi_{\boldsymbol{\epsilon}}(\infty) = 0$,

(viii) $\operatorname{length}(H^1_{\mathcal{F}^*}(K, T^*))$ *is finite if and only if* $\epsilon_1 \neq 0$,

(ix) $\operatorname{length}(H^1_{\mathcal{F}^*}(K, T^*)) \leq \partial\varphi_{\boldsymbol{\epsilon}}(0) = \max\{s : \epsilon_1 \in \mathbf{m}^s \wedge^r H^1_{\mathcal{F}}(K, T)\}$, *with equality if and only if $\boldsymbol{\epsilon}$ is primitive.*

Proof. The theorem follows directly from Proposition 8.6. □

Part 3. Kolyvagin systems

9. Sheaves and monodromy

In this section we recall some concepts and definitions from [1].

Definition 9.1. If X is a graph, a sheaf $\mathcal{S}$ (of R-modules) on X is a rule assigning:

- to each vertex v of X, an R-module $\mathcal{S}(v)$ (the stalk of X at v),
- to each edge e of X, an R-module $\mathcal{S}(e)$,

- to each pair (e, v) where v is an endpoint of the edge e, an R-module map $\psi_v^e : \mathcal{S}(v) \to \mathcal{S}(e)$.

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 $\Gamma(\mathcal{S})$ for the R-module of global sections of $\mathcal{S}$.

Definition 9.2. We say that a sheaf $\mathcal{S}$ on a graph X is *locally cyclic* if all the R-modules $\mathcal{S}(v)$, $\mathcal{S}(e)$ are cyclic and all the maps ψ_v^e 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 e_i is the edge joining v_i and v_{i+1}, then $\psi_{v_{i+1}}^{e_i}$ 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

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

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 $\psi_w^e \circ \psi_P = \psi_{w'}^e \circ \psi_{P'} \in \operatorname{Hom}(\mathcal{S}(v), \mathcal{S}(e))$. 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 $\psi_P = \psi_{P'} \in \operatorname{Hom}(\mathcal{S}(v), \mathcal{S}(w))$.

Proposition 9.3. *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) *If $\boldsymbol{\kappa} \in \Gamma(\mathcal{S})$, and if u is a vertex such that $\kappa_u \neq 0$ and κ_u generates $\mathbf{m}^i\mathcal{S}(u)$ for some $i \in \mathbf{Z}^+$, then κ_w generates $\mathbf{m}^i\mathcal{S}(w)$ for every vertex w.*

Proof. This is [1, Proposition 3.4.4]. □

Definition 9.4. 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 9.3 that a locally cyclic sheaf $\mathcal{S}$ with a hub has a primitive global section if and only if $\mathcal{S}$ has trivial monodromy.

10. Kolyvagin systems and the Selmer sheaf

Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$ as in Definition 4.1. Recall that we have defined a Selmer structure $\mathcal{F}(\mathfrak{n})$ for every $\mathfrak{n} \in \mathcal{N}$ (Definition 2.3) by modifying the local condition at primes dividing $\mathfrak{n}$, and that $K(\mathfrak{q})$ is the p-part of the ray class field of K modulo $\mathfrak{q}$.

Definition 10.1. For every $\mathfrak{n} \in \mathcal{N}$, define

$$G_{\mathfrak{n}} := \bigotimes_{\mathfrak{q}|\mathfrak{n}} \mathrm{Gal}(K(\mathfrak{q})_{\mathfrak{q}}/K_{\mathfrak{q}}).$$

Each $\mathrm{Gal}(K(\mathfrak{q})_{\mathfrak{q}}/K_{\mathfrak{q}})$ is cyclic with order contained in $I_{\mathfrak{n}}$, so $G_{\mathfrak{n}} \otimes (R/I_{\mathfrak{n}})$ is free of rank one over $R/I_{\mathfrak{n}}$.

If $\mathfrak{q}$ is a prime dividing $\mathfrak{n}$, then $(T/I_{\mathfrak{n}}T)/(\mathrm{Fr}_{\mathfrak{q}} - 1)(T/I_{\mathfrak{n}}T)$ is free of rank one over $R/I_{\mathfrak{n}}$, so we can apply the results of §1 to $H^1(K_{\mathfrak{q}}, T/I_{\mathfrak{n}}T)$. In particular we will write

$$\phi_{\mathfrak{q}}^{\mathrm{fs}} : H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}}T) \longrightarrow H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}}T) \otimes G_{\mathfrak{q}}$$

for the finite-singular isomorphism of Definition 1.4 applied to $K_{\mathfrak{q}}$.

If $\mathfrak{q}$ is a prime, $\mathfrak{n}\mathfrak{q} \in \mathcal{N}$, and $r \geq 1$, then we can compare

$$\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_{\mathfrak{n}}T) \otimes G_{\mathfrak{n}} \quad \text{and} \quad \wedge^r H^1_{\mathcal{F}(\mathfrak{n}\mathfrak{q})}(K, T/I_{\mathfrak{n}\mathfrak{q}}T) \otimes G_{\mathfrak{n}\mathfrak{q}}$$

using the exterior algebra of Appendix A. Namely, applying Proposition A.1 with the localization maps of Definition 6.2

$$\mathrm{loc}_{\mathfrak{q}}^{\mathrm{f}} : H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_{\mathfrak{n}\mathfrak{q}}T) \longrightarrow H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}\mathfrak{q}}T) \xrightarrow{\phi_{\mathfrak{q}}^{\mathrm{fs}}} H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}\mathfrak{q}}T) \otimes G_{\mathfrak{q}},$$
$$\mathrm{loc}_{\mathfrak{q}}^{\mathrm{tr}} : H^1_{\mathcal{F}(\mathfrak{n}\mathfrak{q})}(K, T/I_{\mathfrak{n}\mathfrak{q}}T) \longrightarrow H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}\mathfrak{q}}T)$$

gives the top and bottom maps, respectively, in the following diagram:

$$\begin{array}{c} (\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_{\mathfrak{n}}T)) \otimes G_{\mathfrak{n}} \\ \big\downarrow {\scriptstyle \widehat{\mathrm{loc}_{\mathfrak{q}}^{f}} \otimes 1} \\ H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}\mathfrak{q}}T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K, T/I_{\mathfrak{n}\mathfrak{q}}T)) \otimes G_{\mathfrak{n}\mathfrak{q}} \\ \big\uparrow {\scriptstyle \widehat{\mathrm{loc}_{\mathfrak{q}}^{\mathrm{tr}}} \otimes 1} \\ (\wedge^r H^1_{\mathcal{F}(\mathfrak{n}\mathfrak{q})}(K, T/I_{\mathfrak{n}\mathfrak{q}}T)) \otimes G_{\mathfrak{n}\mathfrak{q}} \end{array} \tag{10.1}$$

Definition 10.2. 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), and whenever $\mathfrak{n}, \mathfrak{n}\mathfrak{q} \in \mathcal{N}$ (with $\mathfrak{q}$ prime) we join $\mathfrak{n}$ and $\mathfrak{n}\mathfrak{q}$ by an edge.

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

- $\mathcal{S}(\mathfrak{n}) := (\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_{\mathfrak{n}}T)) \otimes G_{\mathfrak{n}}$ for $\mathfrak{n} \in \mathcal{N}$,

and if e is the edge joining $\mathfrak{n}$ and $\mathfrak{n}\mathfrak{q}$ define

- $\mathcal{S}(e) := H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T/I_{\mathfrak{n}\mathfrak{q}}T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K, T/I_{\mathfrak{n}\mathfrak{q}}T)) \otimes G_{\mathfrak{n}\mathfrak{q}}$,
- $\psi_{\mathfrak{n}}^e : \mathcal{S}(\mathfrak{n}) \to \mathcal{S}(e)$ is the upper map of (10.1),
- $\psi_{\mathfrak{n}\mathfrak{q}}^e : \mathcal{S}(\mathfrak{n}\mathfrak{q}) \to \mathcal{S}(e)$ is the lower map of (10.1).

We call $\mathcal{S}(n) := \wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_{\mathfrak{n}}T) \otimes G_{\mathfrak{n}}$ the *Selmer stalk* at n.

Definition 10.3. A *Kolyvagin system* for $(T, \mathcal{F}, \mathcal{P}, r)$ (or simply a Kolyvagin system of rank r for T, if $\mathcal{F}$ and $\mathcal{P}$ are fixed) is a global section of the Selmer sheaf $\mathcal{S}$. We write $\mathbf{KS}_r(T, \mathcal{F}, \mathcal{P})$, or simply $\mathbf{KS}_r(T)$ when there is no risk of confusion, for the R-module of Kolyvagin systems $\Gamma(\mathcal{S})$.

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

$$\{\kappa_\mathfrak{n} \in (\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_\mathfrak{n}T)) \otimes G_\mathfrak{n} : \mathfrak{n} \in \mathcal{N}\}$$

such that if $\mathfrak{q}$ is prime and $\mathfrak{nq} \in \mathcal{N}$, the images of $\kappa_\mathfrak{n}$ and $\kappa_{\mathfrak{nq}}$ coincide in the diagram (10.1).

Remark 10.4. The definition of Kolyvagin system given in [1] corresponds to the definition above with $r = 1$.

11. Stub Kolyvagin systems

Suppose until the final result of this section that R is a principal artinian ring of length k. Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$ as in Definition 4.1 such that hypotheses (H.1) through (H.7) of §4 hold. In particular $r = \chi(T)$ is the core rank of T.

Recall that for $\mathfrak{n} \in \mathcal{N}$ we defined

$$\lambda(\mathfrak{n}) := \mathrm{length}_R(H^1_{\mathcal{F}(\mathfrak{n})^*}(K, T^*)) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}.$$

We say that a vertex $\mathfrak{n} \in \mathcal{N}$ is a *core vertex* if $\lambda(\mathfrak{n}) = 0$.

Proposition 11.1. *The following are equivalent:*

(i) $\mathfrak{n}$ *is a core vertex for* T*,*
(ii) $H^1_{\mathcal{F}(\mathfrak{n})}(K, T)$ *is free of rank* r *over* R*,*
(iii) $\mathcal{S}(\mathfrak{n})$ *is free of rank one over* R*,*
(iv) $\mathfrak{n}$ *is a core vertex for* $T/\mathbf{m}T$*.*

Proof. We have (i) $\iff$ (ii) by Corollary 3.5, and (i) $\iff$ (iv) by Proposition 3.3(ii). It is easy to see that (ii) $\iff$ (iii). ☐

Proposition 11.2. *If* $\mathfrak{n}, \mathfrak{nq} \in \mathcal{N}$ *and* e *is the edge joining them, then*

$$\psi^e_\mathfrak{n}(\mathbf{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})) = \psi^e_{\mathfrak{nq}}(\mathbf{m}^{\lambda(\mathfrak{nq})}\mathcal{S}(\mathfrak{nq})) \subset \mathcal{S}(e).$$

Proof. By Proposition A.1(ii) and Definition 10.2 of $\psi^e_\mathfrak{n}$ and $\psi^e_{\mathfrak{nq}}$, we have

$$\psi^e_\mathfrak{n}(\mathcal{S}(\mathfrak{n})) = \phi^{\mathrm{fs}}_\mathfrak{q}(\mathrm{loc}_\mathfrak{q}(H^1_{\mathcal{F}(\mathfrak{n})}(K, T))) \otimes \wedge^{r-1} H^1_{\mathcal{F}_\mathfrak{q}(\mathfrak{n})}(K, T) \otimes G_\mathfrak{n},$$
$$\psi^e_{\mathfrak{nq}}(\mathcal{S}(\mathfrak{nq})) = \mathrm{loc}_\mathfrak{q}(H^1_{\mathcal{F}(\mathfrak{nq})}(K, T)) \otimes \wedge^{r-1} H^1_{\mathcal{F}_\mathfrak{q}(\mathfrak{n})}(K, T) \otimes G_{\mathfrak{nq}}.$$

By [1, Lemma 4.1.7], global duality shows that

$$\mathbf{m}^{\lambda(\mathfrak{n})}\phi^{\mathrm{fs}}_\mathfrak{q}(\mathrm{loc}_\mathfrak{q}(H^1_{\mathcal{F}(\mathfrak{n})}(K, T))) = \mathbf{m}^{\lambda(\mathfrak{nq})}\mathrm{loc}_\mathfrak{q}(H^1_{\mathcal{F}(\mathfrak{nq})}(K, T)) \otimes G_\mathfrak{q}$$

and the proposition follows. ☐

We define a subsheaf $\mathcal{S}'$ of the Selmer sheaf $\mathcal{S}$ as follows.

Definition 11.3. The *sheaf of stub Selmer modules* $\mathcal{S}' = \mathcal{S}'_{(T,\mathcal{F},\mathcal{P},r)} \subset \mathcal{S}$ is the subsheaf of $\mathcal{S}$ defined by

- $\mathcal{S}'(\mathfrak{n}) := \mathbf{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n}) = \mathbf{m}^{\lambda(\mathfrak{n})}(\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T)) \otimes G_{\mathfrak{n}} \subset \mathcal{S}(\mathfrak{n})$ if $\mathfrak{n} \in \mathcal{N}$,
- $\mathcal{S}'(e)$ is the image of $\mathcal{S}'(\mathfrak{n})$ in $\mathcal{S}(e)$ under the vertex-to-edge map of $\mathcal{S}$, if $\mathfrak{n}$ is a vertex of the edge e (this is well-defined by Proposition 11.2),

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

Definition 11.4. A *stub Kolyvagin system* is a global section of the sheaf $\mathcal{S}'$. We let $\mathbf{KS}'_r(T) = \mathbf{KS}'_r(T,\mathcal{F},\mathcal{P}) := \Gamma(\mathcal{S}') \subset \mathbf{KS}_r(T)$ denote the R-module of stub Kolyvagin systems.

Remark 11.5. It is shown in [1, Theorem 4.4.1] that when the core rank $\chi(T) = 1$, we have $\mathbf{KS}'_1(T) = \mathbf{KS}_1(T)$. In other words, in that case for every Kolyvagin system $\boldsymbol{\kappa} \in \mathbf{KS}_1(T)$ and $\mathfrak{n} \in \mathcal{N}$, we have that $\kappa_{\mathfrak{n}} \in \mathbf{m}^{\lambda(\mathfrak{n})} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \otimes G_{\mathfrak{n}}$.

Theorem 11.6.

(i) *There are core vertices.*

(ii) *Suppose $\mathfrak{n}, \mathfrak{n}'$ are core vertices. Then there is a path*

$$\mathfrak{n} = \mathfrak{n}_0 \overset{e_1}{\text{———}} \mathfrak{n}_1 \overset{e_2}{\text{———}} \cdots \overset{e_t}{\text{———}} \mathfrak{n}_t = \mathfrak{n}'$$

in $\mathcal{X}$ such that every $\mathfrak{n}_i$ is a core vertex and all of the maps $\psi^{e_{i+1}}_{\mathfrak{n}_i}$ and $\psi^{e_i}_{\mathfrak{n}_i}$ are isomorphisms.

(iii) *The stub subsheaf $\mathcal{S}'$ is locally cyclic, and every core vertex is a hub. For every vertex $\mathfrak{n} \in \mathcal{N}$, there is a core vertex $\mathfrak{n}' \in \mathcal{N}$ divisible by $\mathfrak{n}$.*

Theorem 11.6 will be proved in §14. In the remainder of this section we derive some consequences of it.

Theorem 11.7.

(i) *The module $\mathbf{KS}'_r(T)$ of stub Kolyvagin systems is free of rank one over R, and for every core vertex $\mathfrak{n}$ the specialization map*

$$\mathbf{KS}'_r(T) \longrightarrow \mathcal{S}'(\mathfrak{n}) = (\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T)) \otimes G_{\mathfrak{n}}$$

given by $\boldsymbol{\kappa} \mapsto \kappa_{\mathfrak{n}}$ is an isomorphism.

(ii) *There is a Kolyvagin system $\boldsymbol{\kappa} \in \mathbf{KS}'_r(T)$ such that $\kappa_{\mathfrak{n}}$ generates $\mathcal{S}'(\mathfrak{n})$ for every $\mathfrak{n} \in \mathcal{N}$.*

(iii) *The locally cyclic sheaf $\mathcal{S}'$ has trivial monodromy.*

Proof. This follows from Proposition 9.3, using Theorem 11.6(i,iii). □

For the next theorem we take R to be a discrete valuation ring.

Theorem 11.8. *Suppose that R is a discrete valuation ring, and hypotheses* (H.1) *through* (H.6) *are satisfied for the Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$. For $k > 0$ let $\mathcal{P}_k \subset \mathcal{P}$ be as in Definition 2.2.*

(i) *The natural maps $T \twoheadrightarrow T/\mathbf{m}^k$ and $\mathcal{P}_k \hookrightarrow \mathcal{P}$ induce an isomorphism*

$$\mathbf{KS}'_r(T, \mathcal{P}) \xrightarrow{\sim} \varprojlim \mathbf{KS}'_r(T/\mathbf{m}^k T, \mathcal{P}_k).$$

(ii) *The R-module $\mathbf{KS}'_r(T, \mathcal{P})$, is free of rank one, generated by a Kolyvagin system $\boldsymbol{\kappa}$ whose image in $\mathbf{KS}'_r(T/\mathbf{m}T)$ is nonzero.*

(iii) *The maps $\mathbf{KS}'_r(T, \mathcal{P}) \to \mathbf{KS}'_r(T/\mathbf{m}^k, \mathcal{P}_k)$ are surjective.*

Proof. This can be proved easily directly from Theorem 11.7, as in the proofs of Proposition 7.3 and Theorem 7.4 for Stark systems. See also [1, Proposition 5.2.9]. □

Remark 11.9. When $r = \chi(T) > 1$, we can have $\mathbf{KS}'_r(T) \neq \mathbf{KS}_r(T)$. For example, suppose R is principal artinian of length $k > 1$, and suppose $\mathfrak{m} \in \mathcal{N}$ is such that $H^1_{\mathcal{F}(\mathfrak{m})}(K, T) \cong R^r \oplus (R/\mathbf{m})^r$, with corresponding basis $c_1, \ldots, c_r, d_1, \ldots, d_r$. Let $g_\mathfrak{m}$ be a generator of $G_\mathfrak{m}$.

For every $\mathfrak{q} \in \mathcal{P}$ and every i, $\mathrm{loc}_\mathfrak{q}(d_i)$ is killed by $\mathbf{m}$, so it is divisible by $\mathbf{m}^{k-1}$ in the free R-module $H^1(K_\mathfrak{q}, T)$. It follows that if we define $\boldsymbol{\kappa} := \{\kappa_\mathfrak{n}\}$ where

$$\kappa_\mathfrak{n} := \begin{cases} (d_1 \wedge \cdots \wedge d_r) \otimes g_\mathfrak{m} & \text{if } \mathfrak{n} = \mathfrak{m}, \\ 0 & \text{if } \mathfrak{n} \neq \mathfrak{m}, \end{cases}$$

then $\boldsymbol{\kappa}$ is a Kolyvagin system, but $\kappa_\mathfrak{m} \notin \mathcal{S}'(\mathfrak{m})$ so $\boldsymbol{\kappa} \notin \mathbf{KS}'_r(T)$.

12. Kolyvagin systems and Stark systems

Suppose that R is a principal artinian ring. Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$ as in Definition 4.1 such that $I_\mathfrak{q} = 0$ for every $\mathfrak{q} \in \mathcal{P}$. Recall the R module $Y_\mathfrak{n}$ of Definition 6.1, and let the maps $\mathrm{loc}^\mathrm{f}_\mathfrak{q} : H^1(K, T) \to H^1_\mathrm{tr}(K, T) \otimes G_\mathfrak{q}$ and $\mathrm{loc}^\mathrm{tr}_\mathfrak{q} : H^1(K, T) \to H^1_\mathrm{tr}(K, T)$ be as in Definition 6.2.

Definition 12.1. Suppose $\mathfrak{n} \in \mathcal{N}$. By (6.2) we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \longrightarrow H^1_{\mathcal{F}^\mathfrak{n}}(K, T) \xrightarrow{\oplus \mathrm{loc}^\mathrm{f}_\mathfrak{q}} \bigoplus_{\mathfrak{q} \mid \mathfrak{n}} H^1_\mathrm{tr}(K_\mathfrak{q}, T) \otimes G_\mathfrak{q}$$

and it follows that the square

$$\begin{array}{ccc} H^1_{\mathcal{F}(\mathfrak{n})}(K, T) & \hookrightarrow & H^1_{\mathcal{F}^\mathfrak{n}}(K, T) \\ \downarrow & & \downarrow \oplus \mathrm{loc}^\mathrm{f}_\mathfrak{q} \\ 0 & \hookrightarrow & \bigoplus_{\mathfrak{q} \mid \mathfrak{n}} H^1_\mathrm{tr}(K_\mathfrak{q}, T) \otimes G_\mathfrak{q} \end{array}$$

is cartesian. Proposition A.2(i,iv) attaches to this diagram a map

$$\wedge^{r+\nu(\mathfrak{n})} H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \otimes \wedge^{\nu(\mathfrak{n})} \mathrm{Hom}(\oplus_{\mathfrak{q}|\mathfrak{n}} H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) \otimes G_{\mathfrak{q}}, R) \longrightarrow \wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T).$$

Tensoring both sides with $G_{\mathfrak{n}}$ defines a map

$$\Pi_{\mathfrak{n}} : Y_{\mathfrak{n}} \longrightarrow \wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \otimes G_{\mathfrak{n}}.$$

See the proof of Proposition 12.3 below for an explicit description of the map $\Pi_{\mathfrak{n}}$. Recall that if $\mathfrak{m} \mid \mathfrak{n} \in \mathcal{N}$, then $\Psi_{\mathfrak{n},\mathfrak{m}} : Y_{\mathfrak{n}} \to Y_{\mathfrak{m}}$ is the map of Definition 6.3.

Lemma 12.2. *Suppose that hypotheses* (H.1) *through* (H.7) *of §4 are satisfied, so in particular r is the core rank of T. If $H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*) = 0$ and $\mathfrak{m} \mid \mathfrak{n}$, then*

$$(\Pi_{\mathfrak{m}} \circ \Psi_{\mathfrak{n},\mathfrak{m}})(Y_{\mathfrak{n}}) = \mathbf{m}^{\mathrm{length}(H^1_{\mathcal{F}(\mathfrak{m})^*}(K,T^*))} \mathcal{S}(\mathfrak{m}) = \mathcal{S}'(\mathfrak{m}).$$

Proof. If $H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*) = 0$ then $H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T)$ is free of rank $r + \nu(\mathfrak{n})$ over R by Corollary 3.5(ii). By (6.1) and (6.2) we have

$$(\cap_{\mathfrak{q}|\mathfrak{m}} \ker(\mathrm{loc}^{\mathrm{f}}_{\mathfrak{q}} | H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T))) \cap (\cap_{\mathfrak{q}|(\mathfrak{n}/\mathfrak{m})} \ker(\mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}} | H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T))) = H^1_{\mathcal{F}(\mathfrak{m})}(K,T).$$

Now the lemma follows from Proposition A.2(ii,iii) applied to the cartesian square

$$\begin{array}{ccc} H^1_{\mathcal{F}(\mathfrak{m})}(K,T) & \hookrightarrow & H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \\ \downarrow & & \downarrow {\scriptstyle \oplus_{\mathfrak{q}|\mathfrak{m}} \mathrm{loc}^{\mathrm{f}}_{\mathfrak{q}} \oplus_{\mathfrak{q}|(\mathfrak{n}/\mathfrak{m})} \mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}}} \\ 0 & \hookrightarrow & \bigoplus_{\mathfrak{q}|\mathfrak{m}} (H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) \otimes G_{\mathfrak{q}}) \bigoplus_{\mathfrak{q}|(\mathfrak{n}/\mathfrak{m})} H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) \end{array}$$

□

Proposition 12.3. *Suppose $\boldsymbol{\epsilon} = \{\epsilon_{\mathfrak{n}} : \mathfrak{n} \in \mathcal{N}\}$ is a Stark system of rank r for T. Let $\Pi(\boldsymbol{\epsilon})$ denote the collection $\{(-1)^{\nu(n)} \Pi_{\mathfrak{n}}(\epsilon_{\mathfrak{n}}) : \mathfrak{n} \in \mathcal{N}\}$. Then:*

(i) $\Pi(\boldsymbol{\epsilon}) \in \mathbf{KS}_r(T)$.

(ii) *If hypotheses* (H.1) *through* (H.7) *of §4 hold, then* $\Pi(\boldsymbol{\epsilon}) \in \mathbf{KS}'_r(T)$.

Proof. By definition $\Pi_{\mathfrak{n}}(\epsilon_{\mathfrak{n}}) \in \wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \otimes G_{\mathfrak{n}}$, so we only need to check the compatibility (10.1).

Suppose $\mathfrak{n}\mathfrak{q} \in \mathcal{N}$, with $\mathfrak{n} = \mathfrak{q}_1 \cdots \mathfrak{q}_{\nu(\mathfrak{n})}$, and for every i let h_i be a generator of $\mathrm{Hom}(H^1_{\mathrm{tr}}(K_{\mathfrak{q}_i},T), R)$ and similarly for h and $\mathfrak{q}$. Let

$$\varpi^{\mathrm{tr}}_{\mathfrak{q},h} := \widehat{h \circ \mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}}} : \wedge^t H^1_{\mathcal{F}^{\mathfrak{n}\mathfrak{q}}}(K,T) \to \wedge^{t-1} H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T),$$

$$\varpi^{\mathrm{f}}_{\mathfrak{q},h} := \widehat{h \circ \mathrm{loc}^{\mathrm{f}}_{\mathfrak{q}}} : \wedge^t H^1_{\mathcal{F}^{\mathfrak{n}\mathfrak{q}}}(K,T) \to \wedge^{t-1} H^1_{\mathcal{F}^{\mathfrak{n}}(\mathfrak{q})}(K,T) \otimes G_{\mathfrak{q}}$$

be the maps given by Proposition A.1, for $t > 0$, and similarly for $\varpi^{\mathrm{tr}}_{\mathfrak{q}_i,h_i}$ and $\varpi^{\mathrm{f}}_{\mathfrak{q}_i,h_i}$.

Let $\epsilon_{\mathfrak{nq}} = d_{\mathfrak{nq}} \otimes (h_1 \wedge \cdots \wedge h_{\nu(\mathfrak{n})} \wedge h)$ with $d_{\mathfrak{nq}} \in \wedge^{r+\nu(\mathfrak{nq})} H^1_{\mathcal{F}^{\mathfrak{nq}}}(K,T)$, and similarly $\epsilon_{\mathfrak{n}} = d_{\mathfrak{n}} \otimes (h_1 \wedge \cdots \wedge h_{\nu(\mathfrak{n})})$. By definition of $\Psi_{\mathfrak{nq},\mathfrak{n}}$ we have $d_{\mathfrak{n}} = \varpi^{\mathrm{tr}}_{\mathfrak{q},h}(d_{\mathfrak{nq}})$. If e denotes the edge joining $\mathfrak{n}$ and $\mathfrak{nq}$, then

$$\begin{aligned}(h \otimes 1)(\psi^e_{\mathfrak{nq}}(\Pi_{\mathfrak{nq}}(\epsilon_{\mathfrak{nq}}))) &= \varpi^{\mathrm{tr}}_{\mathfrak{q},h}((\varpi^{\mathrm{f}}_{\mathfrak{q}_1,h_1} \circ \cdots \circ \varpi^{\mathrm{f}}_{\mathfrak{q}_{\nu(\mathfrak{n})},h_{\nu(\mathfrak{n})}} \circ \varpi^{\mathrm{f}}_{\mathfrak{q},h})(d_{\mathfrak{nq}})) \\ &= (-1)^{\nu(\mathfrak{n})+1}(\varpi^{\mathrm{f}}_{\mathfrak{q}_1,h_1} \circ \cdots \circ \varpi^{\mathrm{f}}_{\mathfrak{q}_{\nu(\mathfrak{n})},h_{\nu(\mathfrak{n})}} \circ \varpi^{\mathrm{f}}_{\mathfrak{q},h} \circ \varpi^{\mathrm{tr}}_{\mathfrak{q},h})(d_{\mathfrak{nq}}) \\ &= (-1)^{\nu(\mathfrak{n})+1}(\varpi^{\mathrm{f}}_{\mathfrak{q}_1,h_1} \circ \cdots \circ \varpi^{\mathrm{f}}_{\mathfrak{q}_{\nu(\mathfrak{n})},h_{\nu(\mathfrak{n})}} \circ \varpi^{\mathrm{f}}_{\mathfrak{q},h})(d_{\mathfrak{n}}) \\ &= -\varpi^{\mathrm{f}}_{\mathfrak{q},h}((\varpi^{\mathrm{f}}_{\mathfrak{q}_1,h_1} \circ \cdots \circ \varpi^{\mathrm{f}}_{\mathfrak{q}_{\nu(\mathfrak{n})},h_{\nu(\mathfrak{n})}})(d_{\mathfrak{n}})) \\ &= -(h \otimes 1)(\psi^e_{\mathfrak{n}}(\Pi_{\mathfrak{n}}(\epsilon_{\mathfrak{n}}))).\end{aligned}$$

Since h is an isomorphism, it follows that $\psi^e_{\mathfrak{nq}}(\Pi_{\mathfrak{nq}}(\epsilon_{\mathfrak{nq}})) = -\psi^e_{\mathfrak{n}}(\Pi_{\mathfrak{n}}(\epsilon_{\mathfrak{n}}))$, so the collection $\{(-1)^{\nu(\mathfrak{n})}\Pi_{\mathfrak{n}}(\epsilon_{\mathfrak{n}})\}$ is a Kolyvagin system. This proves (i), and (ii) follows from Lemma 12.2 (using Lemma 6.6(ii)). ☐

Theorem 12.4. *If hypotheses* (H.1) *through* (H.7) *of §4 hold, then the R-module map $\Pi : \mathbf{SS}_r(T) \to \mathbf{KS}'_r(T)$ of Proposition 12.3 is an isomorphism.*

Proof. By Lemma 12.2 and Theorem 6.7, for every $\mathfrak{n}$ the composition

$$\mathbf{SS}_r(T) \xrightarrow{\Pi} \mathbf{KS}'_r(T) \longrightarrow \mathcal{S}'(\mathfrak{n})$$

is surjective. Since $\mathbf{SS}'_r(T)$ and $\mathbf{KS}'_r(T)$ are both free of rank one over R (Theorems 6.7 and 11.7(i)), it follows that Π is an isomorphism. ☐

13. Stub Kolyvagin systems and the dual Selmer group

Suppose for this section that R is either a principal artinian local ring or a discrete valuation ring. We let $k := \mathrm{length}(R)$, so k is finite in the artinian case and $k = \infty$ in the discrete valuation ring case.

Fix Selmer data $(T, \mathcal{F}, \mathcal{P}, r)$ satisfying hypotheses (H.1) through (H.6), and if R is artinian satisfying (H.7) as well. In this section we prove analogues for stub Kolyvagin systems of the results of §8 for Stark systems. We will say that a stub Kolyvagin system $\boldsymbol{\kappa}$ is primitive if it is primitive as a global section of the stub Selmer sheaf $\mathcal{S}'$ (Definition 9.4), i.e. if $\boldsymbol{\kappa}$ generates the R-module $\mathbf{KS}'_r(T)$, or equivalently, if $\kappa_{\mathfrak{n}}$ generates $\mathbf{m}^{\lambda(\mathfrak{n})}(\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T)) \otimes G_{\mathfrak{n}}$ for every $\mathfrak{n} \in \mathcal{N}$.

Corollary 13.1. *Suppose R is a principal artinian ring of length k, and $\boldsymbol{\kappa} \in \mathbf{KS}'_r(T)$.*

(i) *If $\kappa_1 \neq 0$ then*

$$\mathrm{length}(H^1_{\mathcal{F}^*}(K,T^*)) \le k - \mathrm{length}(R\kappa_1) = \max\{i : \kappa_1 \in \mathbf{m}^i \wedge^r H^1_{\mathcal{F}}(K,T)\}.$$

(ii) *If $\boldsymbol{\kappa}$ is primitive and $\kappa_1 \neq 0$, then equality holds in* (i).

(iii) *If $\boldsymbol{\kappa}$ is primitive and $\kappa_1 = 0$, then* $\mathrm{length}(H^1_{\mathcal{F}^*}(K,T^*)) \ge k$.

Proof. By Corollary 3.5(iii), $\mathcal{S}'(1) = \mathbf{m}^{\lambda(1)} \wedge^r H^1_{\mathcal{F}}(K,T)$ is a cyclic R-module of length $\max\{0, k - \mathrm{length}(H^1_{\mathcal{F}^*}(K,T^*))\}$. Since $\kappa_1 \in \mathcal{S}'(1)$ by definition, (i) follows. If $\boldsymbol{\kappa}$ is primitive, then κ_1 generates $\mathcal{S}'(1)$, which proves (ii) and (iii). □

The following definition is the analogue for Kolyvagin systems of Definitions 8.1 and 8.2 for Stark systems.

Definition 13.2. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}_r(T)$ is a Kolyvagin system. Define $\varphi_{\boldsymbol{\kappa}} \in \mathrm{Maps}(\mathcal{N}, \mathbf{Z}_{\geq} 0 \cup \{\infty\})$ by $\varphi_{\boldsymbol{\kappa}}(\mathfrak{n}) := \max\{j : \kappa_{\mathfrak{n}} \in \mathfrak{m}^j H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T)\}$. The *order of vanishing* of $\boldsymbol{\kappa}$ is

$$\mathrm{ord}(\boldsymbol{\kappa}) := \min\{\nu(\mathfrak{n}) : \mathfrak{n} \in \mathcal{N}, \kappa_{\mathfrak{n}} \neq 0\} = \min\{i : \partial\varphi_{\boldsymbol{\kappa}}(i) \neq \infty\}.$$

We also define the sequence of *elementary divisors*

$$d_{\boldsymbol{\kappa}}(i) := \partial\varphi_{\boldsymbol{\kappa}}(i) - \partial\varphi_{\boldsymbol{\kappa}}(i+1), \quad i \geq \mathrm{ord}(\boldsymbol{\kappa}).$$

Proposition 13.3. *Suppose that* $\boldsymbol{\kappa} \in \mathbf{KS}'_r(T)$, $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$, *and* $\boldsymbol{\kappa} = \Pi(\boldsymbol{\epsilon})$. *Then* $\mathrm{ord}(\boldsymbol{\kappa}) = \mathrm{ord}(\boldsymbol{\epsilon})$, $\partial\varphi_{\boldsymbol{\kappa}}(i) = \partial\varphi_{\boldsymbol{\epsilon}}(i)$ *for every* i, *and* $d_{\boldsymbol{\kappa}}(i) = d_{\boldsymbol{\epsilon}}(i)$ *for every* i.

Proof. Suppose first that R is artinian of length k. Since Π is an isomorphism (Theorem 12.4), we may assume without loss of generality that $\boldsymbol{\kappa}$ and $\boldsymbol{\epsilon}$ generate $\mathbf{KS}'_r(T)$ and $\mathbf{SS}_r(T)$, respectively. Recall that we defined $\mu(\mathfrak{n}) := \mathrm{length}(H^1_{(\mathcal{F}^*)_{\mathfrak{n}}}(K,T^*))$.

For every $\mathfrak{n} \in \mathcal{N}$, Theorem 11.7(ii) shows that $\kappa_{\mathfrak{n}}$ generates $\mathbf{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})$, and Theorem 6.7 shows that $\epsilon_{\mathfrak{n}}$ generates $\mathbf{m}^{\mu(\mathfrak{n})}Y_{\mathfrak{n}}$. Thus

$$\partial\varphi_{\boldsymbol{\kappa}}(i) = \begin{cases} \partial\lambda(i) & \text{if } \partial\lambda(i) < k, \\ \infty & \text{if } \partial\lambda(i) \geq k, \end{cases} \qquad \partial\varphi_{\boldsymbol{\epsilon}}(i) = \begin{cases} \partial\mu(i) & \text{if } \partial\mu(i) < k, \\ \infty & \text{if } \partial\mu(i) \geq k. \end{cases}$$

By Proposition 8.3, $\partial\lambda(i) = \partial\mu(i)$ for every i, and all the equalities of the Proposition follow.

The case where R is a discrete valuation ring follows from the artinian case as in the proof of Proposition 8.6. □

Theorem 13.4. *Suppose* R *is a discrete valuation ring,* $\boldsymbol{\kappa} \in \mathbf{KS}'_r(T)$ *and* $\boldsymbol{\kappa} \neq 0$. *Then:*

(i) *the sequence* $\partial\varphi_{\boldsymbol{\kappa}}(t)$ *is nonincreasing, and finite for* $t \geq \mathrm{ord}(\boldsymbol{\kappa})$,
(ii) *the sequence* $d_{\boldsymbol{\kappa}}(i)$ *is nonincreasing, finite for* $i \geq \mathrm{ord}(\boldsymbol{\kappa})$, *and nonnegative,*
(iii) $\mathrm{ord}(\boldsymbol{\kappa})$ *and the* $d_{\boldsymbol{\kappa}}(i)$ *are independent of the choice of nonzero* $\boldsymbol{\kappa}$ *in* $\mathbf{KS}'_r(T)$,
(iv) $\mathrm{corank}_R(H^1_{\mathcal{F}^*}(K,T^*)) = \mathrm{ord}(\boldsymbol{\kappa})$,
(v) $H^1_{\mathcal{F}^*}(K,T^*)/(H^1_{\mathcal{F}^*}(K,T^*))_{\mathrm{div}} \cong \oplus_{i \geq \mathrm{ord}(\boldsymbol{\kappa})} R/\mathbf{m}^{d_{\boldsymbol{\kappa}}(i)}$,

(vi) $\mathrm{length}_R(H^1_{\mathcal{F}^*}(K,T^*)/(H^1_{\mathcal{F}^*}(K,T^*))_{\mathrm{div}}) = \partial\varphi_{\boldsymbol{\kappa}}(\mathrm{ord}(\boldsymbol{\kappa})) - \partial\varphi_{\boldsymbol{\kappa}}(\infty)$, *where* $\partial\varphi_{\boldsymbol{\kappa}}(\infty) := \lim_{t\to\infty}\partial\varphi_{\boldsymbol{\kappa}}(t)$,

(vii) $\boldsymbol{\kappa}$ *is primitive if and only if* $\partial\varphi_{\boldsymbol{\kappa}}(\infty) = 0$,

(viii) $\mathrm{length}(H^1_{\mathcal{F}^*}(K,T^*))$ *is finite if and only if* $\kappa_1 \neq 0$,

(ix) $\mathrm{length}(H^1_{\mathcal{F}^*}(K,T^*)) \leq \partial\varphi_{\boldsymbol{\kappa}}(0) = \max\{s : \kappa_1 \in \mathbf{m}^s \wedge^r H^1_{\mathcal{F}}(K,T)\}$, *with equality if and only if* $\boldsymbol{\kappa}$ *is primitive.*

Proof. By Theorem 12.4, there is a unique $\boldsymbol{\epsilon} \in \mathbf{SS}_r(T)$ such that $\Pi(\boldsymbol{\epsilon}) = \boldsymbol{\kappa}$. By Proposition 13.3, all the invariants of Definition 13.2 attached to $\boldsymbol{\kappa}$ are equal to the corresponding invariants of $\boldsymbol{\epsilon}$. Now the theorem follows from Theorem 8.7. □

14. Proof of Theorem 11.6

Keep the notation of §11, so R is principal and artinian of length k, hypotheses (H.1) through (H.7) hold. In particular we assume $r = \chi(T)$, the core rank of T.

Lemma 14.1. *The sheaf* $\mathcal{S}'$ *is locally cyclic.*

Proof. By Corollary 3.5(iii), for every $\mathfrak{n} \in \mathcal{N}$ the stalk $\mathcal{S}'(\mathfrak{n})$ is a cyclic R-module. By Definition 11.3 and Proposition 11.2 the vertex-to-edge maps $\psi^e_{\mathfrak{n}}$ are all surjective, and so the edge stalks $\mathcal{S}'(e)$ are all cyclic as well. □

Lemma 14.2. *Suppose* $\mathfrak{n}$ *is a core vertex, and* $\mathfrak{q} \in \mathcal{P}$ *does not divide* $\mathfrak{n}$. *Let* e *denote the edge joining* $\mathfrak{n}$ *and* $\mathfrak{nq}$. *Then the following are equivalent:*

(i) $\mathrm{loc}_{\mathfrak{q}} : H^1_{\mathcal{F}(\mathfrak{n})}(K,T)[\mathbf{m}] \to H^1_{\mathrm{f}}(K_{\mathfrak{q}},T)$ *is nonzero,*

(ii) $\mathfrak{nq}$ *is a core vertex and both of the maps* $\psi^e_{\mathfrak{n}} : \mathcal{S}(\mathfrak{n}) \to \mathcal{S}(e)$ *and* $\psi^e_{\mathfrak{nq}} : \mathcal{S}(\mathfrak{nq}) \to \mathcal{S}(e)$ *are isomorphisms.*

Proof. Suppose that (i) holds. Since $I_{\mathfrak{q}} = 0$ by (H.7), Lemma 1.3(ii) shows that $H^1_{\mathrm{f}}(K_{\mathfrak{q}},T)$ is free of rank one over R. Since $\mathfrak{n}$ is a core vertex, $H^1_{\mathcal{F}(\mathfrak{n})}(K,T)$ is a free R-module of rank r. In particular we have $H^1_{\mathcal{F}(\mathfrak{n})}(K,T)[\mathbf{m}] = \mathbf{m}^{k-1}H^1_{\mathcal{F}(\mathfrak{n})}(K,T)$, and it follows that the localization map $\mathrm{loc}_{\mathfrak{q}} : H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}},T)$ is surjective. By Proposition A.1, it follows that $\psi^e_{\mathfrak{n}}$ is an isomorphism.

Since $\mathrm{loc}_{\mathfrak{q}} : H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}},T)$ is surjective, and $H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T)$ is free of rank one over R, and $H^1_{\mathcal{F}(\mathfrak{n})^*}(K,T^*) = 0$, Lemma 4.1.6 of [1] shows that $\mathfrak{nq}$ is a core vertex and $\mathrm{loc}_{\mathfrak{q}} : H^1_{\mathcal{F}(\mathfrak{nq})}(K,T) \to H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T)$ is surjective. Now Proposition A.1 shows that that $\psi^e_{\mathfrak{nq}}$ is an isomorphism. Thus (ii) holds.

Conversely, if $\psi^e_{\mathfrak{n}}$ is an isomorphism then Proposition A.1 shows that the map $\mathrm{loc}_{\mathfrak{q}} : H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}},T)$ is surjective, and since $H^1_{\mathrm{f}}(K_{\mathfrak{q}},T)$ is free of rank one over R it follows that $\mathrm{loc}_{\mathfrak{q}}$ is not identically zero on $H^1_{\mathcal{F}(\mathfrak{n})}(K,T)[\mathbf{m}]$. Thus (ii) implies (i). □

Recall that $\bar{T} := T/\mathbf{m}T$.

Proposition 14.3. *Suppose* $\mathfrak{n} \in \mathcal{N}$ *and* $\lambda(\mathfrak{n}, \bar{T}^*) > 0$. *Then there is a* $\mathfrak{q} \in \mathcal{P}$ *prime to* $\mathfrak{n}$ *such that* $\lambda(\mathfrak{n}\mathfrak{q}, \bar{T}^*) < \lambda(\mathfrak{n}, \bar{T}^*)$ *and* $\psi_{\mathfrak{n}}^e : \mathcal{S}'(\mathfrak{n}) \to \mathcal{S}'(e)$ *is an isomorphism, where* e *is the edge joining* $\mathfrak{n}$ *and* $\mathfrak{n}\mathfrak{q}$.

Let $\bar{\lambda}(\mathfrak{n}) := \dim_{\Bbbk} H^1_{\mathcal{F}(\mathfrak{n})^*}(K, \bar{T}^*)$. By Proposition 3.3(ii), we have $\lambda(\mathfrak{n}) = 0$ if and only if $\bar{\lambda}(\mathfrak{n}) = 0$.

Proof. By [1, Proposition 3.6.1] we can use the Cebotarev theorem to choose a prime $\mathfrak{q} \in \mathcal{P}$ such that the localization maps

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

are both nonzero. (Note that $\mathbf{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \neq 0$ by Corollary 3.5(iii).) Then by Poitou-Tate global duality (for example [1, Lemma 4.1.7(iv)]), we have $\bar{\lambda}(\mathfrak{n}\mathfrak{q}) < \bar{\lambda}(\mathfrak{n})$. Further, the localization $H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T)$ is surjective, so by Proposition A.1(ii)

$$\widehat{\mathrm{loc}_{\mathfrak{q}}} : \wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \longrightarrow H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K, T))$$

is surjective as well. Since $\mathcal{S}'(e)$ is defined to be the image of

$$\mathcal{S}'(\mathfrak{n}) := \mathbf{m}^{\lambda(\mathfrak{n})}(\wedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T)) \otimes G_{\mathfrak{n}}$$

under the upper maps of (10.1), we deduce that

$$\mathcal{S}'(e) = \mathbf{m}^{\lambda(\mathfrak{n})} H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K, T)) \otimes G_{\mathfrak{n}\mathfrak{q}}.$$

Thus

$$\mathrm{length}_R(\mathcal{S}'(e)) \geq k - \lambda(\mathfrak{n}) = \mathrm{length}_R(\mathcal{S}'(\mathfrak{n})),$$

the equality by Corollary 3.5(iii). Since the map $\mathcal{S}'(\mathfrak{n}) \to \mathcal{S}'(e)$ is surjective by definition, it must be an isomorphism. □

Theorem 14.4. *Suppose* $\mathfrak{n}, \mathfrak{n}'$ *are core vertices. Then there is a path*

$$\mathfrak{n} = \mathfrak{n}_0 \overset{e_1}{\text{———}} \mathfrak{n}_1 \overset{e_2}{\text{———}} \cdots \overset{e_t}{\text{———}} \mathfrak{n}_t = \mathfrak{n}'$$

in $\mathcal{X}$ *such that every* $\mathfrak{n}_i$ *is a core vertex and all of the maps* $\psi_{\mathfrak{n}_i}^{e_{i+1}}$ *and* $\psi_{\mathfrak{n}_i}^{e_i}$ *are isomorphisms.*

Proof. When $\chi(T) = 1$, this is [1, Theorem 4.3.12]. The general case can be proved in the same way, but instead we will prove it here by induction on $r := \chi(T)$.

Denote by $\bar{\mathcal{F}}$ the induced Selmer structure on $\bar{T}$. By Proposition 3.3 and the definition of core vertices we see that the Selmer sheaves $\mathcal{S}_{(T,\mathcal{F},\mathcal{P})}$ and $\mathcal{S}_{(\bar{T},\bar{\mathcal{F}},\mathcal{P})}$ have the same core vertices and the same core rank r (see also [1, Theorem 4.1.3]).

Since $r > 0$, we can fix nonzero classes $c \in H^1_{\bar{\mathcal{F}}(\mathfrak{n})}(K, \bar{T})$ and $c' \in H^1_{\bar{\mathcal{F}}(\mathfrak{n}')}(K, \bar{T})$. By [1, Proposition 3.6.1], we can use the Cebotarev theorem to choose $\mathfrak{q} \in \mathcal{P}$, not dividing $\mathfrak{n}\mathfrak{n}'$, such that the localizations $c_{\mathfrak{q}}$ and $c'_{\mathfrak{q}}$ are both nonzero.

Note that the Selmer triple $(\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}, \mathcal{P} - \{\mathfrak{q}\})$ also satisfies hypotheses (H.1) through (H.6) (the only one of those conditions that depends on the Selmer structure is (H.5), and (H.5) is vacuous when we work over $R/\mathbf{m}$). By our choice of $\mathfrak{q}$, both localization maps

$$\mathrm{loc}_{\mathfrak{q}} : H^1_{\bar{\mathcal{F}}(\mathfrak{n})}(K, \bar{T}) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, \bar{T}), \qquad \mathrm{loc}_{\mathfrak{q}} : H^1_{\bar{\mathcal{F}}(\mathfrak{n}')}(K, \bar{T}) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, \bar{T})$$

are nonzero, and $H^1_{\mathrm{f}}(K_{\mathfrak{q}}, \bar{T})$ is a one-dimensional $R/\mathbf{m}$-vector space, so both maps are surjective. Since $\mathfrak{n}$ and $\mathfrak{n}'$ are core vertices for $(\bar{T}, \bar{\mathcal{F}})$, it follows that

$$\dim_{R/\mathbf{m}} H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n})}(K, \bar{T}) = \dim_{R/\mathbf{m}} H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n}')}(K, \bar{T}) = r - 1$$

and (by Poitou-Tate global duality, see for example [1, Theorem 2.3.4]) that $H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n})^*}(K, \bar{T}^*) = H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n}')^*}(K, \bar{T}^*) = 0$.

In particular we deduce that $\chi(\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}) = r - 1$, and that $\mathfrak{n}, \mathfrak{n}'$ are core vertices for the sheaf $\mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}$. By our induction hypotheses we conclude that there is a path $\mathfrak{n} = \mathfrak{n}_0, \mathfrak{n}_1, \ldots, \mathfrak{n}_t = \mathfrak{n}'$ from $\mathfrak{n}$ to $\mathfrak{n}'$ in $\mathcal{X}$ such that every $\mathfrak{n}_i$ is prime to $\mathfrak{q}$, every $\mathfrak{n}_i$ is a core vertex for $\mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}$, and every vertex-to-edge map (for $\mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}$) along the path is an isomorphism. We will show that every $\mathfrak{n}_i$ is a core vertex for $\mathcal{S}_{T, \mathcal{F}}$, and every vertex-to-edge map (for $\mathcal{S}_{T, \mathcal{F}}$) along the path is an isomorphism. This will prove the theorem.

Fix i, $0 \le i \le t$. The exact sequence

$$0 \longrightarrow H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n}_i)}(K, \bar{T}) \longrightarrow H^1_{\bar{\mathcal{F}}(\mathfrak{n}_i)}(K, \bar{T}) \xrightarrow{\mathrm{loc}_{\mathfrak{q}}} H^1_{\mathrm{f}}(K_{\mathfrak{q}}, \bar{T})$$

shows that $\dim_{R/\mathbf{m}} H^1_{\bar{\mathcal{F}}(\mathfrak{n}_i)}(K, \bar{T}) \le r$. Then Corollary 3.5(i) (applied to $\bar{T}$, $\bar{\mathcal{F}}$, and $R/\mathbf{m}$) shows that $\mathfrak{n}_i$ is a core vertex of $\mathcal{S}_{\bar{T}, \bar{\mathcal{F}}}$, and hence is a core vertex of $\mathcal{S}_{T, \mathcal{F}}$.

Further, suppose $\mathfrak{l}$ is a prime such that $\mathfrak{n}_{i \pm 1} = \mathfrak{n}_i \mathfrak{l}$, and let e be the edge joining those two vertices. By assumption, the maps

$$\mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}(\mathfrak{n}_i) \longrightarrow \mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}(e) \ \text{ and } \ \mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}(\mathfrak{n}_i \mathfrak{l}) \longrightarrow \mathcal{S}_{\bar{T}, \bar{\mathcal{F}}_{\mathfrak{q}}}(e)$$

are isomorphisms, so the localization map $H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n}_i)}(K, \bar{T}) \to H^1_{\mathrm{f}}(K_{\mathfrak{l}}, \bar{T})$ is nonzero by Lemma 14.2. But

$$H^1_{\bar{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{n}_i)}(K, \bar{T}) \subset H^1_{\bar{\mathcal{F}}(\mathfrak{n}_i)}(K, \bar{T}) = H^1_{\mathcal{F}(\mathfrak{n}_i)}(K, T)[\mathbf{m}],$$

so $\mathrm{loc}_{\mathfrak{l}} : H^1_{\mathcal{F}(\mathfrak{n}_i)}(K, T)[\mathbf{m}] \to H^1_{\mathrm{f}}(K_{\mathfrak{l}}, T)$ is nonzero, so by Lemma 14.2 both of the maps $\psi^e_{n_i}$ and $\psi^e_{n_{i \pm 1}}$ are isomorphisms. This completes the proof. □

Corollary 14.5. *There are core vertices. More precisely:*

(i) *for every* $\mathfrak{n} \in \mathcal{N}$ *there is an* $\mathfrak{n}' \in \mathcal{N}$ *prime to* $\mathfrak{n}$*, with* $\nu(\mathfrak{n}') = \bar{\lambda}(\mathfrak{n})$*, such that* $\mathfrak{n}\mathfrak{n}'$ *is a core vertex,*

(ii) $\min\{\nu(\mathfrak{n}) : \mathfrak{n}$ *is a core vertex*$\} = \dim_{R/\mathbf{m}} H^1_{\mathcal{F}^*}(K, T^*)[\mathbf{m}]$.

Proof. Choose $\mathfrak{n} \in \mathcal{N}$. For every $\mathfrak{n}' \in \mathcal{N}$ prime to $\mathfrak{n}$, global duality (see for example [1, Lemma 4.1.7(i)]) shows that

$$\bar{\lambda}(\mathfrak{n}\mathfrak{n}') \geq \bar{\lambda}(\mathfrak{n}) - \nu(\mathfrak{n}'). \tag{14.1}$$

Applying Proposition 14.3, we can construct $\mathfrak{n} = \mathfrak{n}_0, \mathfrak{n}_1, \mathfrak{n}_2, \ldots \in \mathcal{N}$ inductively, with $\mathfrak{n}_{i+1} = \mathfrak{n}_i \mathfrak{q}_i$ for some prime $\mathfrak{q}_i \in \mathcal{N}$ and $\bar{\lambda}(\mathfrak{n}_{i+1}) < \bar{\lambda}(\mathfrak{n}_i)$, until we reach $\mathfrak{n}_d \in \mathcal{N}$ with $\bar{\lambda}(\mathfrak{n}_d) = 0$. Then

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

so $\mathfrak{n}_d$ is a core vertex. Setting $\mathfrak{n}' := \mathfrak{n}_d/\mathfrak{n}$ we have

$$\nu(\mathfrak{n}') = d \leq \bar{\lambda}(\mathfrak{n}) = \dim_{R/\mathbf{m}} H^1_{\mathcal{F}^*}(K, T^*)[\mathbf{m}].$$

By (14.1), since $\bar{\lambda}(\mathfrak{n}\mathfrak{n}') = 0$ we have $\nu(\mathfrak{n}') \geq \bar{\lambda}(\mathfrak{n})$, and so $\nu(\mathfrak{n}') = \bar{\lambda}(\mathfrak{n})$. This proves (i), and applying (i) with $\mathfrak{n} = 1$ and (14.1) proves (ii). □

Proof of Theorem 11.6. Theorem 11.6(i) is Corollary 14.5, and Theorem 11.6(ii) is Theorem 14.4. Lemma 14.1 says that $\mathcal{S}'$ is locally cyclic. To complete the proof of Theorem 11.6 we need only show that every core vertex is a hub of $\mathcal{S}'$.

Fix a core vertex $\mathfrak{n}_0$, and let $\mathfrak{n} \in \mathcal{N}$ be any other vertex. We will show by induction on $\bar{\lambda}(\mathfrak{n})$ that there is an $\mathcal{S}'$-surjective path from $\mathfrak{n}_0$ to $\mathfrak{n}$.

If $\bar{\lambda}(\mathfrak{n}) = 0$, then $\mathfrak{n}$ is also a core vertex and the desired surjective path exists by Theorem 14.4.

Now suppose $\bar{\lambda}(\mathfrak{n}) > 0$. Use Proposition 14.3 to find $\mathfrak{q} \in \mathcal{P}$ not dividing $\mathfrak{n}$ such that $\bar{\lambda}(\mathfrak{n}\mathfrak{q}) < \bar{\lambda}(\mathfrak{n})$ and $\psi^e_{\mathfrak{n}} : \mathcal{S}'(\mathfrak{n}) \to \mathcal{S}'(e)$ is an isomorphism, where e is the edge joining $\mathfrak{n}$ and $\mathfrak{n}\mathfrak{q}$. By induction there is an $\mathcal{S}'$-surjective path from $\mathfrak{n}_0$ to $\mathfrak{n}\mathfrak{q}$, and if we adjoin to that path the edge e, we get an $\mathcal{S}'$-surjective path from $\mathfrak{n}_0$ to $\mathfrak{n}$. □

Appendix A. Some exterior algebra

Suppose for this appendix that R is a local principal ideal ring with maximal ideal $\mathbf{m}$.

Proposition A.1. *Suppose* $0 \to N \to M \xrightarrow{\psi} C$ *is an exact sequence of finitely-generated* R*-modules, with* C *free of rank one, and* $r \geq 1$*. Then there is a unique map*

$$\hat{\psi} : \wedge^r M \longrightarrow C \otimes \wedge^{r-1} N$$

such that

(i) *the composition* $\wedge^r M \xrightarrow{\hat{\psi}} C \otimes \wedge^{r-1} N \to C \otimes \wedge^{r-1} M$ *is given by*

$$m_1 \wedge \cdots \wedge m_r \mapsto \sum_{i=1}^{r} (-1)^{i+1} \psi(m_i) \otimes (m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \cdots \wedge m_r),$$

(ii) *the image of* $\hat{\psi}$ *is the image of* $\psi(M) \otimes \wedge^{r-1} N \to C \otimes \wedge^{r-1} N$.

If M *is free of rank* r *over* R*, then* $\hat{\psi}$ *is an isomorphism if and only if* ψ *is surjective.*

Proof. Since R is principal, we can "diagonalize" ψ and write $M = Rm \oplus N_0$ and $N = Im \oplus N_0$ where $N_0 \subset N$, $m \in M$ is such that $\psi(m)$ generates $\psi(M)$, and I is an ideal of R. In particular we have $0 = \psi(N) = I\psi(M)$.

The formula of (i) gives a well-defined R-module homomorphism

$$\hat{\psi}_0 : \wedge^r M \longrightarrow \psi(M) \otimes \wedge^{r-1} M.$$

Consider the diagram

$$\begin{array}{ccccc} \wedge^r M & \xrightarrow{\hat{\psi}_0} & \psi(M) \otimes \wedge^{r-1} M & \longrightarrow & C \otimes \wedge^{r-1} M \\ & & \uparrow{\scriptstyle \eta_1} & & \uparrow \\ & & \psi(M) \otimes \wedge^{r-1} N & \xrightarrow{\eta_2} & C \otimes \wedge^{r-1} N \end{array}$$

with maps induced by the inclusions $\psi \hookrightarrow C$ and $N \hookrightarrow M$. We will show that $\mathrm{image}(\hat{\psi}_0) \subset \mathrm{image}(\eta_1)$ and $\ker(\eta_1) \subset \ker(\eta_2)$. Then $\hat{\psi} := \eta_2 \circ \eta_1^{-1} \circ \hat{\psi}_0$ is well defined and satisfies (i) and (ii).

Since $M = Rm \oplus N_0$, we have that the image $\hat{\psi}_0(\wedge^r M)$ is generated by monomials $\psi(m) \otimes n_1 \wedge \cdots \wedge n_{r-1}$ with $n_i \in N_0$, so $\mathrm{image}(\hat{\psi}_0) \subset \mathrm{image}(\eta_1)$.

We also have

$$\wedge^{r-1} N = (Im \otimes \wedge^{r-2} N_0) \oplus \wedge^{r-1} N_0,$$
$$\wedge^{r-1} M = (Rm \otimes \wedge^{r-2} N_0) \oplus \wedge^{r-1} N_0.$$

Therefore, since $I\psi(M) = 0$,

$$\begin{aligned} \ker(\eta_1) = \ker(\psi(M) \otimes Im \otimes \wedge^{r-2} N_0 \to \psi(M) \otimes Rm \otimes \wedge^{r-2} N_0) \\ = \psi(M) \otimes Im \otimes \wedge^{r-2} N_0. \end{aligned}$$

We further have

$$\eta_2(\psi(M) \otimes Im \otimes \wedge^{r-2} N_0) = 0. \tag{A.1}$$

Thus $\ker(\eta_1) \subset \ker(\eta_2)$, so $\hat{\psi}$ is well-defined and has properties (i) and (ii). Uniqueness follows from the fact that by (A.1)

$$\eta_2(\psi(M) \otimes \wedge^{r-1} N) = \eta_2(\psi(M) \otimes \wedge^{r-1} N_0)$$

injects into $C \otimes \wedge^{r-1} M$.

The final assertion follows easily from the definition of $\hat{\psi}$ above. $\square$

If M is an R-module, let $M^\bullet := \mathrm{Hom}(M, R)$.

Proposition A.2. *Suppose R is artinian and there is a cartesian diagram of R-modules*

$$\begin{array}{ccc} M_1 & \hookrightarrow & M_2 \\ \downarrow & & \downarrow h \\ C_1 & \hookrightarrow & C_2 \end{array}$$

where C_1 and C_2 are free R-modules of finite rank, and the horizontal maps are injective.

(i) *Suppose $r \geq 0$ and $s_i = \mathrm{rank}_R(C_i)$. There is a canonical R-module homomorphism*

$$\wedge^{r+s_2} M_2 \otimes \wedge^{s_2} C_2^\bullet \longrightarrow \wedge^{r+s_1} M_1 \otimes \wedge^{s_1} C_1^\bullet$$

defined as follows. If $m \in \wedge^{r+s_2} M_2$, $\psi_1, \ldots, \psi_{s_2}$ is a basis of $C_2^\bullet$ such that $\psi_{s_1+1}, \ldots, \psi_{s_2}$ is a basis of $(C_2/C_1)^\bullet$, and $h_i = \psi_i \circ h$, then

$$m \otimes (\psi_1 \wedge \cdots \wedge \psi_{s_2}) \mapsto (\hat{h}_{s_1+1} \circ \cdots \circ \hat{h}_{s_2})(m) \otimes (\psi_1 \wedge \cdots \wedge \psi_{s_1})$$

with $\hat{h}_i$ as in Proposition A.1. This is independent of the choice of the ψ_i.

(ii) *If M_2 is free of rank $r + s_2$ over R, then the image of the map of (i) is*

$$\mathbf{m}^{\mathrm{length}(M_1)-(r+s_1)\mathrm{length}(R)} \wedge^{r+s_1} M_1 \otimes \wedge^{s_1} C_1^\bullet.$$

(iii) *If*

$$\begin{array}{ccc} M_2 & \hookrightarrow & M_3 \\ \downarrow & & \downarrow \\ C_2 & \hookrightarrow & C_3 \end{array}$$

is another such cartesian square, then the triangle

$$\begin{array}{ccc} \wedge^{r+s_3} M_3 \otimes \wedge^{s_3} C_3^\bullet & \longrightarrow & \wedge^{r+s_1} M_1 \otimes \wedge^{s_1} C_1^\bullet \\ & \searrow \quad \nearrow & \\ & \wedge^{r+s_2} M_2 \otimes \wedge^{s_2} C_2^\bullet & \end{array}$$

induced by the maps of (i) commutes.

(iv) *Suppose there is an exact sequence $0 \to M_1 \to M_2 \to C$, where C is free of rank s over R. Then for every $r \geq 0$, the map of (i) (with $C_1 = 0$ and $C_2 = C$) is a canonical map $\wedge^{r+s} M_2 \otimes \wedge^s C^\bullet \to \wedge^r M_1$.*

Proof. Since the square is cartesian, and by our choice of the ψ_i, we have

$$\ker(\oplus_{i>s_1} h_i) = h^{-1}(C_1) = M_1. \tag{A.2}$$

Applying Proposition A.1 repeatedly shows that the map defined in (i) takes values in $\wedge^{r+s_1} M_1 \otimes \wedge^{s_1} C_1^\bullet$. It is straightforward to check that this map is independent of the choice of the ψ_i. This proves (i), and (iv) is just a special case of (i).

Suppose now that M_2 is free of rank $r + s_2$, and let $s := s_2 - s_1$. Choose an R-basis $\eta_1, \ldots, \eta_{r+s_2}$ of $M_2^\bullet$ such that the span of $\eta_1, \ldots, \eta_s$ contains $h_{s_1+1}, \ldots, h_{s_2}$, i.e. there is an $s \times s$ matrix $A = [a_{ij}]$ with $a_{ij} \in R$ such that $h_{s_1+j} = \sum_i a_{ij}\eta_i$. Let $N := \cap_{i=1}^s \ker(\eta_i)$. Then N is free over R of rank $r + s_1$, and we have a split exact sequence of free modules

$$0 \longrightarrow N \longrightarrow M_2 \xrightarrow{\oplus_{i \le s}\eta_i} R^s \longrightarrow 0.$$

It follows that the composition $\hat{\eta}_1 \circ \cdots \circ \hat{\eta}_s : \wedge^{r+s_2} M_2 \to \wedge^{r+s_1} N$ of maps given by Proposition A.1 is an isomorphism.

We also have

$$\hat{h}_{s_1+1} \cdots \circ \hat{h}_{s_2} = \det(A)\, \hat{\eta}_1 \circ \cdots \circ \hat{\eta}_s,$$

and $N \subset M_1$ by (A.2). Since N is free, there is a noncanonical splitting

$$M_1 \cong N \oplus M_1/N,$$

so the map

$$\mathbf{m}^{\mathrm{length}(M_1/N)} \wedge^{r+s_1} N \longrightarrow \mathbf{m}^{\mathrm{length}(M_1/N)} \wedge^{r+s_1} M_1$$

induced by the inclusion $N \hookrightarrow M_1$ is surjective. Finally,

$$\det(A)R = \mathbf{m}^{\mathrm{length}(M_1/N)} = \mathbf{m}^{\mathrm{length}(M_1)-(r+s_1)\mathrm{length}(R)},$$

and combining these facts proves (ii).

Assertion (iii) follows from the independence of the choice of the ψ_i. Choose a basis $\psi_1, \ldots, \psi_{s_3}$ of $C_3^\bullet$ such that $\psi_{s_1+1}, \ldots, \psi_{s_3}$ is a basis of $(C_3/C_1)^\bullet$ and $\psi_{s_2+1}, \ldots, \psi_{s_3}$ is a basis of $(C_3/C_2)^\bullet$. Then restricting to C_2 gives a basis $\psi_{s_1+1}|_{C_2}, \ldots, \psi_{s_2}|_{C_2}$ of $(C_2/C_1)^\bullet$, and (iii) just reduces to the statement that

$$(\hat{\psi}_{s_1+1} \circ \cdots \circ \hat{\psi}_{s_2}) \circ (\hat{\psi}_{s_2+1} \circ \cdots \circ \hat{\psi}_{s_3}) = (\hat{\psi}_{s_1+1} \circ \cdots \circ \hat{\psi}_{s_3}). \qquad \square$$

Erratum to [1]***.*** We thank Clément Gomez for pointing out an error in the statement of [1, Lemma 2.1.4]. The correct statement (which is all that was used elsewhere in [1]) should be:

LEMMA 2.1.4. *If* $(T/\mathfrak{m}T)^{G_{\mathbf{Q}}} = 0$ *then* $(T/IT)^{G_{\mathbf{Q}}} = 0$ *for every ideal* I *of* R.

References

[1] B. Mazur & K. Rubin, "Kolyvagin systems", *Mem. Amer. Math. Soc.* **168** (2004), no. 799, p. viii+96.

[2] ———, "Refined class number formulas for $\mathbb{G}_m$", *J. Théor. Nombres Bordeaux* **28** (2016), no. 1, p. 185-211.

[3] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Inc., Boston, MA, 1986, x+421 pages.

[4] B. Perrin-Riou, "Théorie d'Iwasawa et hauteurs p-adiques", *Invent. Math.* **109** (1992), no. 1, p. 137-185.

[5] ———, "Systèmes d'Euler p-adiques et théorie d'Iwasawa", *Ann. Inst. Fourier (Grenoble)* **48** (1998), no. 5, p. 1231-1307.

[6] K. Rubin, "A Stark conjecture "over **Z**" for abelian L-functions with multiple zeros", *Ann. Inst. Fourier (Grenoble)* **46** (1996), no. 1, p. 33-62.

[7] ———, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study, xii+227 pages.

[8] T. Sano, "A generalization of Darmon's conjecture for Euler systems for general p-adic representations", *J. Number Theory* **144** (2014), p. 281-324.

[9] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progress in Mathematics, vol. 47, Birkhäuser Boston, Inc., Boston, MA, 1984, Lecture notes edited by Dominique Bernardi and Norbert Schappacher, 143 pages.

[10] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math. (2)* **141** (1995), no. 3, p. 443-551.

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

Karl Rubin
Department of Mathematics
UC Irvine
Irvine, CA 92697, USA
E-mail: krubin@math.uci.edu