CONTROLLING SELMER GROUPS IN THE HIGHER CORE RANK CASE

BARRY MAZUR AND KARL RUBIN

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.

CONTENTS

Introduction 2

Part 1. Cohomology groups and Selmer structures 4
  1. Local cohomology groups 4
  2. Global cohomology groups and Selmer structures 5
  3. Selmer structures and the core rank 7
  4. Running hypotheses 8
  5. Examples 9

Part 2. Stark systems and the structure of Selmer groups 13
  6. Stark systems 13
  7. Stark systems over discrete valuation rings 15
  8. Structure of the dual Selmer group 17

Part 3. Kolyvagin systems 19
  9. Sheaves and monodromy 19
  10. Kolyvagin systems and the Selmer sheaf 20
  11. Stub Kolyvagin systems 22
  12. Kolyvagin systems and Stark systems 24
  13. Stub Kolyvagin systems and the dual Selmer group 25
  14. Proof of Theorem 11.6 27

Appendix A. Some exterior algebra 29

References 32
Introduction

Let $K$ be a number field and $G_K := \text{Gal}(\bar{K}/K)$ 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 $T^* := \text{Hom}(T, \mu_\infty)$ be its Cartier dual.

A cohomology class $c$ in $H^1(G_K, T)$ provides (after localization and cup-product) a linear functional $L_{c,v}$ on $H^1(G_K_v, T^*)$ for any place $v$ of $K$. Thanks to the duality theorems of class field theory, these $L_{c,v}$, when summed over all places $v$ of $K$, give a linear functional $L_c$ 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 3.3 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

$$r = \sum_{v | \infty} \text{corank} H^0(G_K_v, T^*).$$

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 $d[K:Q]$.

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 [MR1]) 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 [S]. There is a third type, Euler systems (see for example [PR2] or [Ru2]), which we do not deal with in this paper. When $r = 1$, Euler systems provide the crucial link ([MR1 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 [MR2].
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 6.10 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 8.9 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 [MR1, 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 I (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 [MR1] were restricted to the case where the base field $K$ is $\mathbb{Q}$. In many cases the proofs for general $K$ are the same, and in those cases we will feel free to use results from [MR1] without further comment.

**Notation.** Fix a rational prime $p$. Throughout this paper, $R$ will denote a complete, noetherian, local principal ideal domain with finite residue field of characteristic $p$. Let $\mathfrak{m}$ denote the maximal ideal of $R$. The basic cases to keep in mind are $R = \mathbb{Z}/p^n\mathbb{Z}$ or $R = \mathbb{Z}_p$.

If $K$ is a field, $\bar{K}$ will denote a fixed separable closure of $K$ and $G_K := \text{Gal}(\bar{K}/K)$. 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 $G_K \to \text{Aut}(A)$.
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, $\mu_n$ 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 $K$, $F$ its residue field, $K^ur \subset \bar{K}$ the maximal unramified subfield of $\bar{K}$, and $\mathcal{I}$ the inertia group $\text{Gal}(\bar{K}/K^ur)$, so $G_F = G_K/\mathcal{I} = \text{Gal}(K^ur/K)$.

Fix an $R$-module $T$ endowed with a continuous $G_K$-action. By $H^*(K,T) := H^*(G_K,T)$ we mean cohomology 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

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

One can similarly propagate the local condition $\mathcal{F}$ canonically to arbitrary subquotients of $T$, and if $R \rightarrow R'$ 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

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

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

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

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

**Lemma 1.3.** (i) The composition

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

is an isomorphism, so there is a canonical splitting

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

There are canonical functorial isomorphisms

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

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

**Proof.** Assertion (i) is [MRT1, Lemma 1.2.4]. The rest is well known; see for example [MRT1, Lemma 1.2.1].
Definition 1.4. Suppose that $T$ is free of finite rank as an $R$-module, and that $\det(1 - Fr \mid T) = 0$. Define $P(x) \in R[x]$ by
$$P(x) := \det(1 - Fr x \mid T).$$
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, $P(Fr^{-1})$ annihilates $T$, so $Q(Fr^{-1})T \subset T^{Fr=1}$.
We define the finite-singular comparison map $\phi^s$ on $T$ to be the composition, using the isomorphisms of Lemma [M1][ii,iii],
$$H^1_f(K,T) \xrightarrow{\sim} T/(Fr - 1)T \xrightarrow{Q(Fr^{-1})} T^{Fr=1} \xrightarrow{\sim} H^1_tr(K,T) \otimes \Gal(L/K).$$

Lemma 1.5. Suppose that $T$ is free of finite rank over $R$, and that $T/(Fr - 1)T$ is a free $R$-module of rank one. Then $\det(1 - Fr \mid T) = 0$ and the map
$$\phi^s : H^1_f(K,T) \rightarrow H^1_tr(K,T) \otimes \Gal(L/K)$$
of Definition [L2] is an isomorphism. In particular both $H^1_f(K,T)$ and $H^1_tr(K,T)$ are free of rank one over $R$.

Proof. This is [M1] Lemma 1.2.3].

Definition 1.6. Define the dual of $T$ to be the $R[[G_K]]$-module
$$T^* := \Hom(T, \mu_{p^\infty}).$$
We have the (perfect) local Tate cup product pairing
$$\langle , \rangle : H^1(K,T) \times H^1(K,T^*) \rightarrow H^2(K, \mu_{p^\infty}) \xrightarrow{\sim} \Q_p/\Z_p.$$
A local condition $\mathcal{F}$ for $T$ determines a local condition $\mathcal{F}^*$ for $T^*$, by taking $H^1_f(K,T^*)$ to be the orthogonal complement of $H^1_f(K,T)$ under the Tate pairing $\langle , \rangle$.

Proposition 1.7. With notation as above, we have:
(i) $H^1_f(K,T)$ and $H^1_f(K,T^*)$ are orthogonal complements under $\langle , \rangle$.
(ii) $H^1_tr(K,T)$ and $H^1_tr(K,T^*)$ are orthogonal complements under $\langle , \rangle$.

Proof. The first assertion is (for example) Theorem I.2.6 of [Mi]. Both assertions are [M1] 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 $\overline{K} \subset C$ be the algebraic closure of $K$ in $C$, and for each prime $\mathfrak{q}$ of $K$ fix an algebraic closure $\overline{K}_\mathfrak{q}$ of $K_\mathfrak{q}$ containing $\overline{K}$. This determines a choice of extension of $\mathfrak{q}$ to $\overline{K}$.
Let $D_\mathfrak{q} := \Gal(\overline{K}_\mathfrak{q}/K_\mathfrak{q})$, which we identify with a closed subgroup of $G_K := \Gal(K/K)$. In other words $D_\mathfrak{q}$ is a particular decomposition group at $\mathfrak{q}$ in $G_K$, and $H^1(D_\mathfrak{q}, T) = H^1(K_\mathfrak{q}, T)$. Let $I_\mathfrak{q} \subset D_\mathfrak{q}$ be the inertia group, and $Fr_\mathfrak{q} \in D_\mathfrak{q}/I_\mathfrak{q}$ the Frobenius element. If $T$ is unramified at $\mathfrak{q}$, then $D_\mathfrak{q}/I_\mathfrak{q}$ acts on $T$, and hence so does $Fr_\mathfrak{q}$. If we choose a different decomposition group at $\mathfrak{q}$, then the action of $Fr_\mathfrak{q}$ changes by conjugation in $G_K$. We will write $\text{loc}_\mathfrak{q}$ for the localization map $H^1(K,T) \rightarrow H^1(K_\mathfrak{q}, T)$.
If \( q \) is a prime of \( K \), let \( K(q) \) denote the \( p \)-part of the ray class field of \( K \) modulo \( q \) (i.e., the maximal \( p \)-power extension of \( K \) in the ray class field), and \( K(q)_q \) the completion of \( K(q) \) at the chosen prime above \( q \). If \( q \) is principal then \( K(q)_q/K_q \) is cyclic and totally tamely ramified.

If \( q \) is principal, \( T \) is unramified at \( q \), and \( [K(q)_q : K_q]T = 0 \), the transverse submodule of \( H^1(K_q, T) \) is the submodule

\[
H^1_{tr}(K_q, T) := H^1_{K(q)_q} - H^1_{K(q)_q} \] (\( q \rightarrow T \)) = \ker \left[ H^1(K_q, T) \to H^1(K(q)_q, T) \right]

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 \( q \in \Sigma(\mathcal{F}) \) (including archimedean places), a local condition (in the sense of Definition 1.1) on \( T \) over \( K_q \), i.e., a choice of \( R \)-submodule \( H^1_{K_q}(T) \subset H^1(K_q, T) \).

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

\[
H^1(K_{\Sigma(\mathcal{F})}/K, T) \to \bigoplus_{q \in \Sigma(\mathcal{F})} \left( H^1(K_q, T)/H^1_{K_q}(K_q, T) \right)
\]

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 \( q \) belong to \( H^1_{K_q}(K_q, T) \) for every \( q \in \Sigma(\mathcal{F}) \).

For examples of Selmer structures see [MR1]. 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 \( R \), \( q \nmid p \infty \) is prime, and \( T \) is unramified at \( q \). If \( q \) is not principal, let \( I_q := R \). If \( q \) is principal, let \( I_q \subset R \) be the largest power of \( m \) (i.e., \( m^k \) with \( k \geq 0 \) maximal) such that \( [K(q)_q : K_q]R \subset I_q \) and \( T/(Fr - 1)T + I_qT \) is free of rank one over \( R/I_q \).

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

\[
\mathcal{P}_k = \{ q \in \mathcal{P} : I_q \subset m^k \}
\]

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 \( n \in \mathcal{N} \), \( n \neq 1 \), define

\[
I_n := \sum_{q|n} I_q \subset R.
\]

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

- \( \Sigma(\mathcal{F}_a^b(n)) := \Sigma(\mathcal{F}) \cup \{ q : q | abn \} \),
Definition 2.5. The \( m \) every \( q \) dividing \( \mathcal{F} \) as in (2.4) \( 0 \)

\[ \text{If } m \rightarrow 0 \] (2.4)

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

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

\[ \text{For example, we will be especially interested in Selmer groups of the form} \]

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

\[ (2.4) \quad 0 \rightarrow H^1_{2m}(K, T) \rightarrow H^1_{2n}(K, T) \rightarrow \bigoplus_{q \mid n/m} H^1(K_q, T)/H^1_{1}(K_q, T). \]

**Definition 2.5.** The dual of \( T \) is the \( R[[G_K]] \)-module \( T^* := \text{Hom}(T, \mu_{p^\infty}) \). For every \( q \) we have the local Tate pairing

\[ \langle \cdot, \cdot \rangle_q : H^1(K_q, T) \times H^1(K_q, T^*) \rightarrow Q_p/\mathbb{Z}_p \]

as in [10].

Just as every local condition on \( T \) determines a local condition on \( T^* \) (Definition [1], a Selmer structure \( \mathcal{F} \) for \( T \) determines a Selmer structure \( \mathcal{F}^* \) for \( T^* \). Namely, take \( \Sigma(\mathcal{F}^*) := \Sigma(\mathcal{F}) \), and for \( q \in \Sigma(\mathcal{F}) \) take \( H^1_{2q}(K_q, T^*) \) to be the local condition induced by \( \mathcal{F} \), i.e., the orthogonal complement of \( H^1_{2q}(K_q, T) \) under \( \langle \cdot, \cdot \rangle_q \).

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 \( q \in \Sigma(\mathcal{F}) \), the local condition \( \mathcal{F} \) at \( q \) is “cartesian on the category of quotients of \( T \)” as defined in [MRI] Definition 1.1.4.

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

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

If \( n \in \mathcal{N} \) and \( I_n = 0 \) then:

(i) the exact sequence

\[ 0 \rightarrow T/m^i T \rightarrow T/m^{k-i} T \rightarrow 0 \]
induces an isomorphism \( H^1_{\mathcal{F}(n)}(K, T/m^nT) \xrightarrow{\sim} H^1_{\mathcal{F}(n)}(K, T)[m^n] \) and an exact sequence

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

(ii) the inclusion \( T^*[m^n] \hookrightarrow T^* \) induces an isomorphism

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

(iii) there is a unique integer \( r \), independent of \( n \), such that there is a non-canonical isomorphism

\[
H^1_{\mathcal{F}(n)}(K, T) \cong H^1_{\mathcal{F}(n)*}(K, T^*) \oplus R^r \quad \text{if} \quad r \geq 0,
\]

\[
H^1_{\mathcal{F}(n)}(K, T) \oplus R^{-r} \cong H^1_{\mathcal{F}(n)*}(K, T^*) \quad \text{if} \quad r \leq 0.
\]

Proof. These assertions are [MR1, Lemma 3.5.4], [MR1, Lemma 3.5.3], and [MR1, 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 \((T/m^kT, \mathcal{F})\) 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 \( n \in \mathcal{N} \), let \( \nu(n) \) denote the number of primes dividing \( n \).

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

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

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

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

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

Proof. The first isomorphism is just Proposition 3.3 (iii). For (ii), observe that the Selmer structure \( \mathcal{F}^n \) is cartesian by [MR1, Lemma 3.7.1(i)], so applying Proposition 3.3 (iii) to \((T, \mathcal{F}^n)\) we have \( H^1_{\mathcal{F}^n}(K, T) \cong H^1_{\mathcal{F}(n)*}(K, T^*) \oplus R^{\chi(T, \mathcal{F}^n)} \). To complete the proof of (ii) we need only show that \( \chi(T, \mathcal{F}^n) = \chi(T)+\nu(n) \), and this follows without difficulty from Poitou-Tate global duality (see for example [MR1, 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
\[
\mathcal{P}(L, \tau) := \{ \text{primes } q \notin \Sigma(F) : q \text{ is unramified in } L/K \}
\]
and \( \text{Fr}_q \) is conjugate to \( \tau \) in \( \text{Gal}(L/K) \).

Fix Selmer data \((T, \mathcal{F}, \mathcal{P}, r)\) as in Definition 4.1. Let \( \bar{T} = T/mT \), so \( \bar{T}^* = T^*[m] \).
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 \( \mathcal{H}_M := \mathcal{H}(\mu_M, (O_K^*)^{1/M}) \). Let \( k \) denote the residue field \( R/m \).
In order to obtain the strongest results, we will usually make the following additional assumptions.

\begin{enumerate}[(H.1)]
\item \( T^{G_K} = (T^*)^{G_K} = 0 \) and \( T \) is an absolutely irreducible \( k[[G_K]] \)-module,
\item there is a \( \tau \in \text{Gal}(K/\mathcal{H}_M) \) 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 \( \mathcal{P}(L, \tau) \subset \mathcal{P} \),
\item \( H^1(\mathcal{H}_M(T)/K, T/mT) = H^1(\mathcal{H}_M(T)/K, T^*[m]) = 0 \),
\item either \( T \not\cong T^* \) as \( k[[G_K]] \)-modules, or \( p > 3 \),
\item the Selmer structure \( \mathcal{F} \) is cartesian (Definition 3.1),
\item \( r = \chi(T) > 0 \), where \( \chi(T) \) is the core rank of \( T \).
(Only) when \( R \) is artinian, we will also sometimes assume
\item \( I_q = 0 \) for every \( q \in \mathcal{P} \).
\end{enumerate}

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 \( R/m^k \) and \( T \) by \( T/m^k \), 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 with is a large selection of primes \( q \) such that \( T/(\text{Fr}_q - 1, m^k) \) 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 \( \text{Hom}(G_{\mathcal{H}_M(T)}, T) \). Assumptions \((H.1) \) and \((H.4) \) then allow us to satisfy various Cebotarev conditions simultaneously.

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

Proof. Since \( \text{Fr}_q \) fixes \( \mathcal{H} \), \( q \) is principal. By class field theory we have
\[
\text{Gal}(K(q)_q/K_q) \cong (O_K/q)^\times /\text{image}(O_K^\times).
\]
Since \( \tau \) acts trivially on \( \mu_M \), so does \( \text{Fr}_q \), so \( |(O_K/q)^\times| \) is cyclic of order divisible by \( M \). Since \( \tau \) acts trivially on \( (O_K^\times)^{1/M} \), so does \( \text{Fr}_q \), so the reduction of \( O_K^\times \) is contained in \( ((O_K/q)^\times)^M \). By \((4.6) \) we conclude that \( [K(q)_q : K_q] \) is divisible by \( M \), so \([K(q)_q : K_q]R = 0 \). We also have that \( T/(\text{Fr}_q - 1)T \cong T/(\tau - 1)T \) is free of rank one over \( R \), so the lemma follows from the definition of \( I_q \).

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 \( \mathcal{F}_{ur} \) on \( T \) by
\[
\Sigma(\mathcal{F}_{ur}) := \{ q : T \text{ is ramified at } q \} \cup \{ p : p | p \} \cup \{ v : v | \infty \},
\]
• if \( q \in \Sigma(\mathcal{F}_{\text{ur}}) \) and \( q \nmid p \infty \) then
  \[
  H^1_{\mathcal{F}_{\text{ur}}}(K_q, T) := \ker[H^1(K_q, T) \to H^1(K_{q^p}, T \otimes \mathbb{Q}_p)],
  \]

• if \( p \mid p \) then define the universal norm subgroup
  \[
  H^1(K_p, T)^{\text{un}} := \cap_{K_p \subset L \subset K_p} \text{Cor}_{L/K_p} H^1(L, T),
  \]
  intersection over all finite unramified extensions \( L \) of \( K_p \). Define
  \[
  H^1_{\mathcal{F}_{\text{ur}}}(K_p, T) := H^1(K_p, T)^{\text{un, sat}},
  \]
  the saturation of \( H^1(K_p, T)^{\text{un}} \) in \( H^1(K_p, T) \), i.e., \( H^1(K_p, T)/H^1_{\mathcal{F}_{\text{ur}}}(K_p, T) \) is \( R \)-torsion-free and \( H^1_{\mathcal{F}_{\text{ur}}}(K_p, T)/H^1(K_p, T)^{\text{un}} \) has finite length,

• if \( v \mid \infty \) then
  \[
  H^1_{\mathcal{F}_{\text{ur}}}(K_v, T) := H^1(K_v, T).
  \]

In other words, \( H^1_{\mathcal{F}_{\text{ur}}}(K, T) \) 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 \( \mathbb{Z}_p \)-extension above \( p \).

Note that the Selmer structure \( \mathcal{F}_{\text{ur}} \) satisfies \([\text{H.5}]\) by Remark \([\text{H.2}]\).

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

**Proof.** By the Lemma in [PK], \([2.1.1] \) (applied to the unramified \( \mathbb{Z}_p \)-extension of \( K_p \)), \( H^1_{\mathcal{F}_{\text{ur}}}(K_p, T^*) \) is the maximal divisible submodule of the image of the (injective) inflation map

\[
H^1(K_p, T^*) \longrightarrow H^1_{\mathcal{F}_{\text{ur}}}(K_p, T^*)
\]

We have

\[
H^1(K_p, T^*)^{\mathcal{F}_{\text{ur}}} \cong (T^*)^{\mathcal{F}_{\text{ur}}} / (\gamma - 1)(T^*)^{\mathcal{F}_{\text{ur}}}
\]

where \( \gamma \) is a topological generator of \( \text{Gal}(K_p^*/K_p) \). Thus we have an exact sequence

\[
0 \longrightarrow H^0(K_p, T^*) \longrightarrow (T^*)^{\mathcal{F}_{\text{ur}}} \xrightarrow{\gamma - 1} (T^*)^{\mathcal{F}_{\text{ur}}} \longrightarrow H^1(K_p, T^*)^{\mathcal{F}_{\text{ur}}} \longrightarrow 0
\]

and the lemma follows. \( \Box \)

**Corollary 5.3.** If \( p \mid p \) and \( H^0(K_p, T^*) \) has finite length, then \( H^1_{\mathcal{F}_{\text{ur}}}(K_p, T) = H^1(K_p, T) \).

**Proof.** By Lemma \([5.2] \) \( H^1_{\mathcal{F}_{\text{ur}}}(K_p, T^*) \) has finite length, so \( H^1(K_p, T)/H^1_{\mathcal{F}_{\text{ur}}}(K_p, T) \) has finite length. But by definition \( H^1(K_p, T)/H^1_{\mathcal{F}_{\text{ur}}}(K_p, T) \) is \( R \)-torsion-free, so \( H^1_{\mathcal{F}_{\text{ur}}}(K_p, T) = H^1(K_p, T) \). \( \Box \)

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

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

**Proof.** For every \( k > 0 \) let \( T_k = T/m^kT \). If \( f, g \) are functions of \( k \in \mathbb{Z}_+ \), 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 \([6.4] \) and Proposition \([6.3](iii) \)), the theorem will follow if we can show that

\[
\text{length}(H^1_{\mathcal{F}_{\text{ur}}}(K, T_k)) - \text{length}(H^1_{\mathcal{F}_{\text{ur}}}(K, T^*_k)) \sim k \sum_{v \mid \infty} \text{corank}_R(H^0(K_v, T^*)).
\]
By [MR1, Proposition 2.3.5] (which is essentially [Wi] Lemma 1.6], for every $k \in \mathbb{Z}^+$

\begin{equation}
\text{length}(H^1_{\mathcal{F}^*}(K, T_k)) - \text{length}(H^1_{\mathcal{F}^*}(K, T_k^*)) = \text{length}(H^0(K, T_k)) - \text{length}(H^0(K, T_k^*)) + \sum_{v \in \Sigma(F)} \left( \text{length}(H^0(K, T_k^*)) - \text{length}(H^1_{\mathcal{F}^*}(K, T_k^*))) \right).
\end{equation}

By hypothesis (H.1), $H^0(K, T_k) = H^0(K, T_k^*) = 0$. If $v \mid \infty$, then $\text{length}(H^0(K, T_k^*)) \sim k \text{ corank}_R(H^0(K, T^*))$, $\text{length}(H^1_{\mathcal{F}^*}(K, T_k^*))) \sim 0$.

Suppose $q \in \Sigma(F)$, $q \nmid \rho \infty$. Let $I_q$ denote an inertia group above $q$ in $G_K$. By [Ru2, Lemma 1.3.5], we have

\[
\text{length}(H^1_{\mathcal{F}^*}(K, T_k^*)) \sim \text{length}((T_k^*)^F_q/(Fr_q - 1)(T_k^*)^F_q).
\]

On the other hand, the exact sequence

\[
0 \to H^0(K, T_k^*) \to (T_k^*)^F_q \xrightarrow{Fr_q - 1} (T_k^*)^F_q \to (T_k^*)^F_q/(Fr_q - 1)(T_k^*)^F_q \to 0
\]

shows that

\[
\text{length}(H^0(K, T_k^*)) = \text{length}((T_k^*)^F_q/(Fr_q - 1)(T_k^*)^F_q).
\]

Thus the term for $v = q$ in (5.6) is bounded independent of $k$.

Now suppose $p \mid p$. By Lemma [5.2] $\text{corank}_R(H^1_{\mathcal{F}^*}(K, T^*)) = \text{corank}_R(H^0(K, T^*))$. By definition $H^1_{\mathcal{F}^*}(K, T_k^*)$ is the inverse image of $H^1_{\mathcal{F}^*}(K, T^*)$ under the natural map $H^1(K, T_k^*) \to H^1(K, T^*)(m_k^\infty)$. A simple exercise shows that the kernel and cokernel of this map have length bounded independent of $k$, so we see that

\[
\text{length}(H^1_{\mathcal{F}^*}(K, T_k^*)) \sim k \text{ corank}_R(H^1_{\mathcal{F}^*}(K, T^*)) = k \text{ corank}_R(H^0(K, T^*)�)
\]

Thus the term for $v = p$ in (5.6) is bounded independent of $k$.

Combining these calculations proves (5.5), and hence the theorem. \hfill \Box

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

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

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

A simple exercise in Galois cohomology (see for example [MR1 §6.1] or [Ru2 §1.6.C]) shows that

\[
H^1(K, T) \cong (E^\times \otimes \mathbb{Z}_p)^\rho
\]

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

\[
H^1(K, q) \cong (E_q^\times \otimes \mathbb{Z}_p)^\rho
\]
where $E_q = E \otimes_K K_q$ is the product of the completions of $E$ above $q$. With these identifications, the unramified Selmer structure of Definition 5.1 is given by

$$H^1_{\text{ur}}(K_q, T) := (O^\times_{E, q} \otimes \mathbb{Z}_p)^p$$

for every $q$, where $O_{E,q}$ is the ring of integers of $E_q$.

Proposition 5.7. Let $\text{Cl}(E)$ denote the ideal class group of $E$. There are natural isomorphisms

$$H^1_{\text{ur}}(K, T) \cong (O^\times_E \otimes \mathbb{Z}_p)^p, \quad H^1_{\text{ur}}(K, T^*) \cong \text{Hom}(\text{Cl}(E)^p, \mathbb{Q}_p/\mathbb{Z}_p)$$

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

$$0 \to (O^\times_E / (O^\times_E)^p)^k \to H^1_{\text{ur}}(K, T / p^k T) \to \text{Cl}(E) / p^k \to 0$$

and an isomorphism

$$H^1_{\text{ur}}(K, T^* / p^k) \cong \text{Hom}(\text{Cl}(E)^p, \mathbb{Z} / p^k \mathbb{Z}).$$

Proof. See for example [MR1] Proposition 6.1.3].

Suppose in addition now that $\rho \neq \omega$, and either $\rho^2 \neq \omega$ or $p > 3$, where $\omega : G_K \to \mathbb{Z}_p^\times$ is the Teichmüller character giving the action of $G_K$ on $\mu_p$. Then conditions (H.1), (H.3), and (H.4) of [11] all hold. By Remark 3.2, the Selmer structure $F_{\text{ur}}$ satisfies (H.5) as well, and condition (H.2) holds with $r = 1$ and $L = E$. Finally, if there is at least one real place $v$ of $K$ such that $\rho$ is trivial on complex conjugation at $v$, then the following corollary shows that condition (H.6) holds.

Corollary 5.8. The core rank $\chi(T, F_{\text{ur}})$ is

$$\chi(T) = \dim_{\mathbb{F}_p} (O^\times_E / (O^\times_E)^p)^p = \text{rank}_{\mathbb{Z}_p} (O^\times_E \otimes \mathbb{Z}_p)^p = |\{\text{archimedean } v : \rho(\sigma_v) = 1\}|$$

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

Proof. The first equality follows from Proposition 5.7 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 [11] Proposition I.3.4].

Thus if $E/K$ is an extension of totally real fields and $\rho \neq 1$, then $\chi(T, F_{\text{ur}}) = [K : Q]$ by Corollary 5.8 and all conditions (H.1) through (H.6) are satisfied.

If $K = Q$, then $\chi(T) = 1$, and a Kolyvagin system (see [10]) can be constructed from the Euler system of cyclotomic units (see [MR1]).

For a general totally real field $K$, if we assume the version of Stark’s Conjecture described in [R1], 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 [8]). For the details and a thorough discussion of this example, see [MR2].

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

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

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

Let $F$ be the Selmer structure on $T$ given by $H^1_{\text{ur}}(K_v, T) = H^1_{\text{ur}}(K_v, T_v)$ for every $v$. Then $F$ is the unramified Selmer structure $F_{\text{ur}}$ given by Definition 5.1 (For $v$
dividing \( p \), this follows from the Lemma in [PR1 §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 [Ru2 §1.6.4]). Hence we have an exact sequence

\[
0 \to H^1_{\mathcal{F}}(K, T^*) \to \text{Sel}_{p^\infty}(\tilde{A}/K) \to \bigoplus_{p \mid p} H^1(K_p, \tilde{A}[p^\infty]).
\]

Suppose now that \( p > 3 \), and that the image of \( G_K \) in \( \text{Aut}(A[p]) \cong \text{GL}_{2d}(\mathbb{F}_p) \) 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 \( \text{GSp}_{2d}(\mathbb{F}_p) \). 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 5.9.** The core rank of \( T \) is given by \( \chi(T) = d [K : Q] \).

**Proof.** By Theorem 5.4, we have

\[
\chi(T) = \sum_{v \mid \infty} \text{corank}_{\mathbb{Z}_p} H^0(K_v, \tilde{A}[p^\infty]).
\]

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

\[
\sum_{v \mid \infty} \text{corank}_{\mathbb{Z}_p} H^0(K_v, \tilde{A}[p^\infty]) = \sum_{v \mid \infty} d [K_v : R] = d [K : Q].
\]

If \( K = Q \) and \( d = 1 \) (i.e., \( A \) is an elliptic curve), then Proposition 5.9 shows that \( \chi(T) = 1 \). In this case Kato has constructed an Euler system for \( T \), from which one can produce a Kolyvagin system ([MR1 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 \( m^k = 0 \) and \( m^{k-1} \neq 0 \). 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., \( I_q = 0 \) for every \( q \in \mathcal{P} \).

Recall that \( \nu(n) \) denotes the number of prime factors of \( n \).

**Definition 6.1.** For every \( n \in \mathcal{N} \), define

\[
W_n := \bigoplus_{\ell \mid n} \text{Hom}(H^1_{\mathcal{F}}(K_{q}, T), R),
\]

\[
Y_n := \wedge^{r+\nu(n)} H^1_{\mathcal{F}}(K, T) \otimes \wedge^{\nu(n)} W_n,
\]

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

Then \( W_n \) is a free \( R \)-module of rank \( \nu(n) \), since each \( H^1_{\mathcal{F}}(K_{q}, T) \) is free of rank one (Lemma 1.5). If we fix an ordering \( n = q_1 \cdots q_{\nu(n)} \) of the primes dividing \( n \), and a generator \( h_i \) of \( \text{Hom}(H^1_{\mathcal{F}}(K_{q_i}, T), R) \) for each \( i \), then \( h_1 \wedge \cdots \wedge h_{\nu(n)} \) is a generator of the free, rank-one \( R \)-module \( \wedge^{\nu(n)} W_n \).

For the structure of \( Y_n \) when \( r \) is the core rank of \( T \), see Lemma 6.9 below.
Definition 6.2. For every \( q \in \mathcal{P} \), define the transverse localization map
\[
\text{loc}^\text{tr}_q : H^1(K, T) \xrightarrow{\text{loc}_q} H^1(K_q, T) \to H^1_{\text{tr}}(K_q, T),
\]
where the second map is projection (using the direct sum decomposition of Lemma 1.3(i)) with kernel \( H^1_{\text{tr}}(K_q, T) \). If \( n \in \mathcal{N} \) and \( q \mid n \), then
\[
\text{ker}(\text{loc}^\text{tr}_q|_{H^1_{\text{tr}}(K, T)}) = H^1_{\text{tr}/n}(K, T).
\]
In exactly the same way, we can define a map \( \text{loc}^\text{tr}_q \) by using the finite projection and the isomorphism \( \phi^\text{loc}_q \) of Definition 6.4.
\[
\text{loc}^\text{tr}_q : H^1(K, T) \xrightarrow{\text{loc}_q} H^1(K_q, T) \to H^1_{\text{tr}}(K_q, T) \sim H^1_{\text{tr}/n}(K, T).
\]

Definition 6.5. Suppose \( n \in \mathcal{N} \) and \( m \mid n \). By (6.3) we have an exact sequence
\[
0 \to H^1_{\text{tr}/m}(K, T) \to H^1_{\text{tr}/n}(K, T) \to \bigoplus_{q \mid n/m} H^1_{\text{tr}}(K_q, T)
\]
and it follows that the square
\[
\begin{array}{c}
H^1_{\text{tr}/m}(K, T) \\
\oplus \text{loc}^\text{tr}_q
\end{array}
\begin{array}{c}
H^1_{\text{tr}/n}(K, T) \\
\oplus \text{loc}^\text{tr}_q
\end{array}
\]
is cartesian. Let
\[
\Psi_{n, m} : Y_n \to Y_m
\]
be the map of Proposition A.3(i) attached to this diagram.

Concretely, \( \Psi_{n, m} \) is given as follows. Fix a factorization \( n = q_1 \cdots q_t \), with \( m = q_1 \cdots q_s \), and a generator \( h_i \) of \( \text{Hom}(H^1_{\text{tr}}(K_{q_i}, T), R) \) for every \( i \). Let \( n_i = \prod_{j < i} q_j \). These choices lead to a map
\[
h_{s+1} \circ \text{loc}^\text{tr}_{q_{s+1}} \circ \cdots \circ h_t \circ \text{loc}^\text{tr}_{q_t} : H^1_{\text{tr}/n}(K, T) \to \wedge^r H^1_{\text{tr}/m}(K, T)
\]
(where \( h_i \circ \text{loc}^\text{tr}_{q_i} : \wedge^i H^1_{\text{tr}/n_i}(K, T) \to \wedge^{i-1} H^1_{\text{tr}/n_{i-1}}(K, T) \) is given by Proposition A.1) and an isomorphism \( \wedge^r(n)W_n \cong \wedge^r(m)W_m \) given by \( h_1 \wedge \cdots \wedge h_t \). The tensor product of these two maps is the map \( \Psi_{n, m} : Y_n \to Y_m \), and is independent of the choices made.

Proposition 6.7. Suppose \( n \in \mathcal{N} \), \( n' \mid n \), and \( n'' \mid n' \). Then \( \Psi_{n'', n'} \circ \Psi_{n, n''} = \Psi_{n, n'} \).

Proof. This is Proposition A.3(i). \( \square \)

Definition 6.8. Thanks to Proposition 6.7, we can define the \( R \)-module \( \text{SS}_r(T) = \text{SS}_r(T, \mathcal{F}, \mathcal{P}) \) of Stark systems of rank \( r \) to be the inverse limit
\[
\text{SS}_r(T) := \lim_{\substack{\rightarrow \\\\\\n \in \mathcal{N} \\\\\\n}} Y_n
\]
with respect to the maps \( \Psi_{n, m} \).
We call these collections Stark systems because a fundamental example is given by elements predicted by a generalized Stark conjecture \[ MR2, Ru1 \].

Let \( Y'_n = m^{\text{length}(H^1_{(r^*),n}(K,T^*))}Y_n \).

**Lemma 6.9.** Suppose that hypotheses (H.1) through (H.7) of \( \ref{section} \) are satisfied, so in particular \( r \) is the core rank of \( T \). Then:

1. \( Y'_n \) is a cyclic \( R \)-module of length \( \max\{k - \text{length}(H^1_{(r^*),n}(K,T^*)), 0\} \).
2. There are \( n \in \mathcal{N} \) such that \( H^1_{(r^*),n}(K,T^*) = 0 \).
3. If \( H^1_{(r^*),n}(K,T^*) = 0 \) then \( Y_n \) is free of rank one over \( R \).
4. If \( H^1_{(r^*),n}(K,T^*) = 0 \) and \( m \mid n \), then \( \Psi_{n,m}(Y_n) = Y'_m \).

**Proof.** Assertions (i) and (iii) follow directly from Corollary \[ 3.5(iv) \]. Since \( H^1_{(r^*),n}(K,T^*) \) is finite, we can choose generators \( c_1, \ldots, c_t \) of \( H^1_{(r^*),n}(K,T^*)[m] \). For each \( i \), use \[ MR1 \] Proposition 3.6.1 to choose \( q_i \in \mathcal{N} \) such that \( \text{loc}_{q_i}(c_i) \neq 0 \), and let \( n = \prod q_i \). Then \( H^1_{(r^*),n}(K,T^*) = 0 \), so (ii) holds.

Proposition \[ A.3(ii) \] applied to the diagram \[ 6.9 \] shows that

\[
\Psi_{n,m}(Y_n) = m^{\text{length}(H^1_{(r^*),m}(K,T)) - (r + \nu(m))k}Y_m.
\]

Corollary \[ 3.5(ii) \] shows that

\[
\text{length}(H^1_{(r^*),m}(K,T)) - (r + \nu(m))k = \text{length}(H^1_{(r^*),m}(K,T^*))
\]

which proves (iv). \( \square \)

**Theorem 6.10.** Suppose that hypotheses (H.1) through (H.7) of \( \ref{section} \) are satisfied. Then the \( R \)-module \( \text{SS}_r(T) \) is free of rank one, and for every \( n \in \mathcal{N} \), the image of the projection map \( \text{SS}_r(T) \to Y_n \) is \( Y'_n \).

**Proof.** Using Lemma \[ 6.9(ii) \], choose an \( d \in \mathcal{N} \) such that \( H^1_{(r^*),d}(K,T^*) = 0 \). Then \( H^1_{(r^*),n}(K,T) = 0 \) for every \( n \in \mathcal{N} \) divisible by \( d \). Now the theorem follows from Lemma \[ 6.9(iv) \]. \( \square \)

7. Stark systems over discrete valuation rings

For this section we assume that \( R \) is a discrete valuation ring, and we fix Selmer data \( (T, F, P, r) \) as in Definition \[ 1.1 \]. We assume throughout this section that hypotheses (H.1) through (H.6) of \( \ref{section} \) are satisfied. For \( k > 0 \) recall from Definition \[ 2.2 \] that

\[
P_k := \{ q \in P : I_q \in m^k \},
\]

and \( \mathcal{N}_k \) is the set of squarefree products of primes in \( P_k \). By Remark \[ 1.3 \] the Selmer data \( (T/m^kT, F, P_k, r) \) satisfies (H.1) through (H.7) over the ring \( R/m^k \).

In this section we will define the module \( \text{SS}_r(T) \) of Stark systems of rank \( r \) over \( T \), and use the results of \[ 3.5 \] about \( \text{SS}_r(T/m^kT) \) to study \( \text{SS}_r(T) \).

**Definition 7.1.** For every \( n \in \mathcal{N}_k \), define

\[
W_n := \bigoplus_{q \in \mathcal{N}_k} \text{Hom}(H^1_{(r^*),n}(K_q, T/I_nT), R/I_n),
\]

\[
Y_n := \wedge^{r + \nu(n)} H^1_{(r^*),n}(K, T/I_nT) \otimes \wedge^{\nu(n)} W_n,
\]

\[
Y'_n := m^{\text{length}(H^1_{(r^*),n}(K,T^* | I_n))}Y_n.
\]
A Stark system of rank r for T (more precisely, for \((T, \mathcal{F}, \mathcal{P})\)) is a collection \(\{\epsilon_n \in Y_n : n \in \mathcal{N}\}\) such that if \(n \in \mathcal{N}\) and \(m \nmid n\), then
\[
\Psi_{n,m}(\epsilon_n) = \overline{\epsilon_m}
\]
where \(\overline{\epsilon_m}\) is the image of \(\epsilon_m\) in \(Y_m \otimes R/I_n\), and \(\Psi_{n,m} : Y_n \to Y_m \otimes R/I_n\) is the map of Definition 6.5 applied to \(T/I_n T\) and \(R/I_n\). Denote by \(SS_r(T) = SS_r(T, \mathcal{F}, \mathcal{P})\) the \(R\)-module of Stark systems for \(T\).

**Lemma 7.2.** If \(j \leq k\), then the projection map \(T/m^k T \to T/m^j T\) and restriction to \(P_k\) induce a surjection and an isomorphism, respectively
\[
\begin{align*}
SS_r(T/m^k T, P_k) &\longrightarrow SS_r(T/m^j T, P_k) \\
\sim &\longrightarrow SS_r(T/m^j T, P_j)
\end{align*}
\]

Proof. Let \(n \in \mathcal{N}_k\) be such that \(H^1_{(\mathcal{F}, \mathcal{P})_n}(K, T^* m) = 0\). Then by Theorem 6.10 projecting to \(Y_n\) gives a commutative diagram with vertical isomorphisms
\[
\begin{align*}
SS_r(T/m^k T, P_k) &\longrightarrow SS_r(T/m^j T, P_k) \\
\sim &\longrightarrow SS_r(T/m^j T, P_j) \\
Y_n \otimes R/m^k &\longrightarrow Y_n \otimes R/m^j \\
&\cong Y_n \otimes R/m^j
\end{align*}
\]
Since the bottom maps are a surjection and an isomorphism, so are the top ones. \(\square\)

**Proposition 7.3.** The natural maps \(T \to T/m^k\) and \(P_k \hookrightarrow \mathcal{P}\) induce an isomorphism
\[
SS_r(T, \mathcal{P}) \xrightarrow{\sim} \varinjlim SS_r(T/m^k T, P_k)
\]
where the inverse limit is with respect to the maps of Lemma 7.2.

Proof. Suppose \(\epsilon \in SS_r(T)\) is nonzero. Then we can find an \(n\) such that \(\epsilon_n \neq 0\) in \(Y_n\). If \(n \neq 1\) then \(I_n \neq 0\), and we let \(k\) be such that \(m^k = I_n\). If \(n = 1\) choose \(k\) so that \(\epsilon_1 \neq 0\) in \(\wedge^r H^1_{\mathcal{F}, \mathcal{P}}(K, T/m^k T)\). In either case \(I_n \subset m^k\), and the image of \(\epsilon\) in \(SS_r(T/m^k T, P_k)\) is nonzero. Thus the map in the proposition is injective.

Now suppose \(\{\epsilon^{(k)}\} \in \varinjlim SS_r(T/m^k T, P_k)\). If \(n \in \mathcal{N}\) and \(n \neq 1\), let \(j\) be such that \(I_n = m^j\) and define
\[
\epsilon_n := \epsilon_n^{(j)} \in Y_n.
\]
If \(n = 1\), define
\[
\epsilon_1 = \lim_{k \to \infty} \epsilon^{(k)}_1 \in \lim_{k \to \infty} \wedge^r H^1_{\mathcal{F}, \mathcal{P}}(K, T/m^k T) = \wedge^r H^1_{\mathcal{F}, \mathcal{P}}(K, T) = Y_1.
\]
It is straightforward to verify that this defines an element \(\epsilon \in SS_r(T, \mathcal{P})\) that maps to \(\epsilon^{(k)} \in SS_r(T/m^k T, P_k)\) for every \(k\). Thus the map in the proposition is surjective as well. \(\square\)

**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 \(r\), \(SS_r(T, \mathcal{P})\), is free of rank one, generated by Stark system \(\epsilon\) whose image in \(SS_r(T/m^k T, \mathcal{P})\) is nonzero. The map \(SS_r(T, \mathcal{P}) \to SS_r(T/m^k T, \mathcal{P})\) is surjective for every \(k\).

Proof. By Theorem 6.10 \(SS_r(T/m^k T, \mathcal{P})\) is free of rank one over \(R/m^k\) for every \(k\). The maps \(SS_r(T/m^{k+1} T, \mathcal{P}_{k+1}) \to SS_r(T/m^k T, P_k)\) are surjective by Lemma 7.2, so the theorem follows from Proposition 7.3. \(\square\)
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 \( k := \text{length}(R) \), so \( k \) is finite in the artinian case and \( k = \infty \) in the discrete valuation ring case.

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

**Definition 8.1.** Define functions \( \mu, \lambda, \varphi \in \text{Maps}(\mathcal{N}, \mathbb{Z}_{\geq 0} \cup \{\infty\}) \)

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

and if \( e \in \text{SS}_r(T) \) is a Stark system
- \( \varphi(e) = \max\{j : \epsilon_n \in m^j Y_n\} \).

Define \( \partial : \text{Maps}(\mathcal{N}, \mathbb{Z}_{\geq 0} \cup \{\infty\}) \rightarrow \text{Maps}(\mathbb{Z}_{\geq 0}, \mathbb{Z}_{\geq 0} \cup \{\infty\}) \) by

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

**Definition 8.2.** The order of vanishing of a nonzero Stark system \( e \in \text{SS}_r(T) \) is

\[
\text{ord}(e) := \min\{\nu(n) : n \in \mathcal{N}, \epsilon_n \neq 0\} = \min\{i : \partial \varphi(i) \neq \infty\}.
\]

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

\[
d_\epsilon(i) := \partial \varphi(i) - \partial \varphi(i + 1), \quad i \geq \text{ord}(\epsilon).
\]

Note that \( \partial \varphi(i) = \infty \) if \( i < \text{ord}(\epsilon) \); Theorems \( \text{S.6} \) and \( \text{S.9} \) below show that the converse is true as well, so the \( d_\epsilon(i) \) are well-defined and finite.

**Proposition 8.3.** Suppose \( R \) is artinian, and \( H^1_{\mathcal{F}, *}(K, T^*) \cong \bigoplus_{i \geq 1} R/\mathfrak{m}^{e_i} \) 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 \( n \in \mathcal{N} \) and \( \nu(n) = t \). Consider the map

\[
H^1_{\mathcal{F}, n}(K, T^*) \longrightarrow \bigoplus_{q \mid n} H^1_{\mathcal{F}, q}(K_q, T^*).
\]

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 \( \sum_{i \leq t} e_i \), so the kernel has length at least \( \sum_{i > t} e_i \). But by definition this kernel is \( H^1_{\mathcal{F}, n}(K, T^*) \), which is contained in \( H^1_{\mathcal{F}, n}(K, T^*) \), so

\[
(8.4) \quad \lambda(n) \geq \mu(n) \geq \sum_{i > t} e_i.
\]

We will prove by induction on \( t \) that \( n \in \mathcal{N} \) can be chosen so that \( \nu(n) = t \) and \( H^1_{\mathcal{F}, n}(K, T^*) \cong \bigoplus_{i > t} R/\mathfrak{m}^{e_i} \). For such an \( n \) equality holds in \( \text{S.3} \), and the lemma follows. When \( t = 0 \) we can just take \( n = 1 \).

Suppose we have an \( n \) with \( \nu(n) = t - 1 \) and \( H^1_{\mathcal{F}, n}(K, T^*) \cong \bigoplus_{i > t - 1} R/\mathfrak{m}^{e_i} \). Since \( \chi(T) > 0 \), Corollary \( \text{S.5} \) shows that \( \mathfrak{m}^{k-1} H^1_{\mathcal{F}, n}(K, T) \neq 0 \). Fix a nonzero element \( c \in \mathfrak{m}^{k-1} H^1_{\mathcal{F}, n}(K, T) \subset H^1_{\mathcal{F}, n}(K, T)[\mathfrak{m}] \). If \( e_t > 0 \) then choose a nonzero element \( c' \in \mathfrak{m}^{e_t-1} H^1_{\mathcal{F}, n}(K, T^*) \subset H^1_{\mathcal{F}, n}(K, T^*)[\mathfrak{m}] \).
we can use the Cebotarev theorem to choose a prime $q \in \mathcal{P}$ such that the localization $\text{loc}_q(c) \neq 0$ and, if $\epsilon_q > 0$, such that $\text{loc}_q(c') \neq 0$ as well.

Since $H^1_{\mathfrak{F}}(K, T)$ is free of rank one over $R$, and (by our choice of $q$) the localization of $m^{k-1}H^1_{\mathfrak{F}_n}(K, T)$ at $q$ is nonzero, it follows that the localization map $H^1_{\mathfrak{F}_n}(K, T) \to H^1_{\mathfrak{F}_q}(K, T)$ is surjective. Similarly, we have that $H^1_{\mathfrak{F}_n^*(K, T^*)}$ has exponent $m^{e_1}$, and if $e_1 > 0$ then the localization of $m^{e_1-1}H^1_{\mathfrak{F}_n^*}(K, T^*)$ at $q$ is nonzero, so

$$H^1_{\mathfrak{F}_n^*}(K, T^*)/H^1_{\mathfrak{F}_q^*}(K, T^*) \cong \text{loc}_q(H^1_{\mathfrak{F}_n^*}(K, T^*)) \cong R/m^{e_1}$$

and therefore $H^1_{\mathfrak{F}_n^*}(K, T^*) \cong \bigoplus_{i \geq i_1} R/m^{e_i}$. By [MR1, Theorem 4.1.7(ii)] we have $H^1_{\mathfrak{F}_n}(K, T) = H^1_{\mathfrak{F}_n^*}(K, T^*)$, so $nq \in \mathcal{N}$ has the desired property. □

**Proposition 8.5.** Suppose $R$ is artinian of length $k$, and $c \in \text{SS}_r(T)$. Fix $s \geq 0$ such that $c$ generates $m^s \text{SS}_r(T)$, and nonnegative integers $e_1 \geq e_2 \geq \cdots$ such that

$$H^1_{\mathfrak{F}_r^*}(K, T^*) \cong \bigoplus_{i \geq 1} R/m^{e_i}.$$

Then for every $t \geq 0$,

$$\partial \varphi_c(t) = \left\{ \begin{array}{ll}
\sum_{i > t} e_i & \text{if } s + \sum_{i > t} e_i < k,
\infty & \text{if } s + \sum_{i > t} e_i \geq k.
\end{array} \right.$$

**Proof.** It is enough to prove the proposition when $s = 0$, and the general case will follow. So we may assume that $c$ generates $\text{SS}_r(T)$. By Theorem 6.10 and Lemma 6.9(i), we have that $\epsilon_n$ generates $Y' = m^\mu Y$, which is cyclic of length $\text{max}\{k - \mu(n), 0\}$. Hence $\epsilon_n \in m^\mu Y$, and $\epsilon_n \in m^{\mu(n)+1} Y$ if and only if $\mu(n) \geq k$. Therefore

$$\partial \varphi_c(t) = \left\{ \begin{array}{ll}
\partial \mu(t) & \text{if } \partial \mu(t) < k,
\infty & \text{if } \partial \mu(t) \geq k.
\end{array} \right.$$

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

**Theorem 8.6.** Suppose $R$ is artinian, $c \in \text{SS}_r(T)$, and $c_1 \neq 0$. Then

$$\partial \varphi_c(0) \geq \partial \varphi_c(1) \geq \partial \varphi_c(2) \geq \cdots,$$

$$d_c(0) \geq d_c(1) \geq d_c(2) \geq \cdots \geq 0,$$

and

$$H^1_{\mathfrak{F}_r^*}(K, T^*) \cong \bigoplus_{i \geq 0} R/m^{d_{c_i}},$$

**Proof.** Let $s$ be such that $c$ generates $m^s \text{SS}_r(T)$. If $c_1 \neq 0$ then $\partial \varphi_c(0) < k$, so in Proposition 8.5 we have $\partial \varphi_c(t) = s + \sum_{i > t} e_i$ 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

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

Proposition 8.7. Suppose $R$ is a discrete valuation ring, and $\epsilon \in \text{SS}_r(T)$ generates $m^r \text{SS}_r(T)$. Let $a := \text{corank}_R(H^1_{T^*}(K, T^*))$ and write
\[ H^1_{T^*}(K, T^*)/(H^1_{T^*}(K, T^*))_{\text{div}} \cong \bigoplus_{i \geq a} R/m^i \]
with $a_1 + 1 \geq a_2 + 2 \geq \cdots$. Then
\[
\partial \varphi_\epsilon(t) = \begin{cases} 
\infty & \text{if } t < a, \\
s + \sum_{i > t} e_i & \text{if } t \geq a.
\end{cases}
\]

Proof. Let $e_1 = \cdots = e_a := \infty$. Since
\[ H^1_{T^*}(K, T^*) = \lim_{k \to \infty} H^1_{T^*}(K, T^*[m^k]), \]
Proposition 8.5(ii) applied to all the $T/m^kT$ shows that for every $k \in \mathbb{Z}^+$ we have
\[ (8.8) \quad H^1_{T^*}(K, T^*[m^k]) = H^1_{T^*}(K, T^*[m^k]) \cong \bigoplus_{i \geq 1} R/m^i, \]
For every $k \geq 0$ let $\epsilon^{(k)}$ denote the image of $\epsilon$ in $\text{SS}_r(T/m^kT, T)$. Fix $s \geq 0$ such that $\epsilon$ generates $m^s \text{SS}_r(T)$. Then by Theorem 7.4, $\epsilon^{(k)}$ generates $m^s \text{SS}_r(T/m^kT)$ for every $k$.

Fix $t$, and choose $n \in \mathcal{N}$ with $\nu(n) = t$. Let $k$ be such that $I_n = m^k$. By (8.8) and Proposition 8.5, we have that $\epsilon^{(k)} = 0$ if $t < a$, and $\epsilon^{(k)} \in m^{s+\sum_{i > t} e_i} Y_n$ if $t > a$. But $\epsilon^{(k)} = \epsilon_n \in Y_n$, so we conclude that $\partial \varphi_\epsilon(t) = \infty$ if $t < a$, and $\partial \varphi_\epsilon(t) \geq s + \sum_{i > t} e_i$ if $t \geq a$.

Now suppose $t \geq a$, and fix $k > s + \sum_{i > t} e_i$. By Proposition 8.5, we can find $n \in \mathcal{N}$ with $I_n \subseteq m^k$ such that $\epsilon^{(k)} \notin m^{s+1+\sum_{i > t} e_i} Y_n$. Since $\epsilon^{(k)}$ is the image of $\epsilon_n$, we have that $\epsilon_n \notin m^{s+1+\sum_{i > t} e_i} Y_n$. This shows that $\partial \varphi_\epsilon(t) \leq s + \sum_{i > t} e_i$, and the proof is complete.

Theorem 8.9. Suppose $R$ is a discrete valuation ring, $\epsilon \in \text{SS}_r(T)$ and $\epsilon \neq 0$. Then:
(i) the sequence $\partial \varphi_\epsilon(t)$ is nonincreasing, finite for $t \geq \text{ord}(\epsilon)$, and nonnegative,
(ii) the sequence $d_\epsilon(i)$ is nonincreasing, finite for $i \geq \text{ord}(\epsilon)$, and nonnegative,
(iii) $\text{ord}(\epsilon)$ and the $d_\epsilon(i)$ are independent of the choice of nonzero $\epsilon \in \text{SS}_r(T)$,
(iv) $\text{corank}_R(H^1_{T^*}(K, T^*)) = \text{ord}(\epsilon)$,
(v) $H^1_{T^*}(K, T^*)/(H^1_{T^*}(K, T^*))_{\text{div}} \cong \bigoplus_{i \geq \text{ord}(\epsilon)} R/m^i d_\epsilon(i)$,
(vi) $\text{length}_R(H^1_{T^*}(K, T^*)/(H^1_{T^*}(K, T^*))_{\text{div}}) = \text{ord}(\epsilon) - \partial \varphi_\epsilon(\infty)$, where $\partial \varphi_\epsilon(\infty) := \lim_{t \to \infty} \partial \varphi_\epsilon(t)$
(vii) $\epsilon$ is primitive if and only if $\partial^{(\infty)}(\epsilon) = 0$,
(viii) $\text{length}(H^1_{T^*}(K, T^*))$ is finite if and only if $\epsilon_1 \neq 0$,
(ix) $\text{length}(H^1_{T^*}(K, T^*)) \leq \partial \varphi_\epsilon(0) = \max\{s : \epsilon_1 \in m^s \wedge H^1_{T^*}(K, T^*)\}$, with equality if and only if $\epsilon$ is primitive.

Proof. The theorem follows directly from Proposition 8.7.

Part 3. Kolyvagin systems

9. Sheaves and monodromy

In this section we recall some concepts and definitions from [MR1].
Definition 9.1. If $X$ is a graph, a sheaf $S$ (of $R$-modules) on $X$ is a rule assigning:

- to each vertex $v$ of $X$, an $R$-module $S(v)$ (the stalk of $X$ at $v$),
- to each edge $e$ of $X$, an $R$-module $S(e)$,
- to each pair $(e,v)$ where $v$ is an endpoint of the edge $e$, an $R$-module map $\psi^v_e : S(v) \to S(e)$.

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

Definition 9.2. We say that a sheaf $S$ on a graph $X$ is \textit{locally cyclic} if all the $R$-modules $S(v),S(e)$ are cyclic and all the maps $\psi^v_e$ are surjective.

If $S$ is locally cyclic then a \textit{surjective path} (relative to $S$) 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 $\psi^{e_i}_{v_i+1}$ is an isomorphism. We say that the vertex $v$ is a \textit{hub} of $S$ if for every vertex $w$ there is an $S$-surjective path from $v$ to $w$.

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

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

since all the inverted maps are isomorphisms. We will say that $S$ has \textit{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 $\psi_w \circ \psi_P = \psi_{w'} \circ \psi_{P'} \in \text{Hom}(S(v),S(w))$. In particular for every pair $v,w$ of vertices and every pair $P,P'$ of surjective paths from $v$ to $w$, we require that $\psi_P = \psi_{P'} \in \text{Hom}(S(v),S(w))$.

Proposition 9.3. Suppose $S$ is locally cyclic and $v$ is a hub of $S$.

(i) The map $f_v : \Gamma(S) \to S(v)$ defined by $\kappa \mapsto \kappa_v$ is injective, and is surjective if and only if $S$ has trivial monodromy.

(ii) If $\kappa \in \Gamma(S)$, and if $u$ is a vertex such that $\kappa_u \neq 0$ and $\kappa_u$ generates $m^iS(u)$ for some $i \in \mathbb{Z}^+$, then $\kappa_u$ generates $m^iS(w)$ for every vertex $w$.

Proof. This is [MRT] Proposition 3.4.4].

Definition 9.4. A global section $\kappa \in \Gamma(S)$ will be called \textit{primitive} if for every vertex $v$, $\kappa(v) \in S(v)$ is a generator of the $R$-module $S(v)$.

It follows from Proposition 9.3 that a locally cyclic sheaf $S$ with a hub has a primitive global section if and only if $S$ has trivial monodromy.

10. Kolyvagin systems and the Selmer sheaf

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

Definition 10.1. For every $n \in N$, define

$$
G_n := \bigotimes_{q|n} \text{Gal}(K(q)/K_q).
$$

Each $\text{Gal}(K(q)/K_q)$ is cyclic with order contained in $I_n$, so $G_n \otimes (R/I_n)$ is free of rank one over $R/I_n$. 


If \( q \) is a prime dividing \( n \), then \( (T/I_nT)/(Fr_q - 1)(T/I_nT) \) is free of rank one over \( R/I_n \), so we can apply the results of \( \text{[1]} \) to \( H^1(K_q, T/I_nT) \). In particular we will write

\[
\varphi^q_n : H^1(K_q, T/I_nT) \longrightarrow H^1_{tr}(K_q, T/I_nT) \otimes G_q
\]

for the finite-singular isomorphism of Definition \( \text{[1.8]} \) applied to \( K_q \).

If \( q \) is a prime, \( nq \in \mathcal{N} \), and \( r \geq 1 \), then we can compare \( \wedge^r H^1_{\mathcal{F}(n)}(K, T/I_nT) \otimes G_n \) and \( \wedge^r H^1_{\mathcal{F}(nq)}(K, T/I_{nq}T) \otimes G_{nq} \) using the exterior algebra of Appendix \( \text{[A]} \). Namely, applying Proposition \( \text{[A.1]} \) with the localization maps of Definition \( \text{[6.2]} \)

\[
\begin{align*}
\text{loc}^r_q : H^1_{\mathcal{F}(n)}(K, T/I_{nq}T) & \longrightarrow H^1_{\mathcal{F}(nq)}(K, T/I_{nq}T) \\
\text{loc}^r_{nq} : H^1_{\mathcal{F}(nq)}(K, T/I_{nq}T) & \longrightarrow H^1_{\mathcal{F}(n)}(K, T/I_{nq}T)
\end{align*}
\]

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

\[
\begin{array}{c}
\text{loc}^r_q \otimes 1 \\
H^1_{tr}(K_q, T/I_{nq}T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}(n)}(K, T/I_{nq}T)) \otimes G_{nq} \\
\text{loc}^r_{nq} \otimes 1 \\
(\wedge^r H^1_{\mathcal{F}(nq)}(K, T/I_{nq}T)) \otimes G_{nq}
\end{array}
\]

\[(10.2)\]

**Definition 10.3.** Define a graph \( \mathcal{X} := \mathcal{X}(P) \) by taking the set of vertices of \( \mathcal{X} \) to be \( \mathcal{N} := \mathcal{N}(P) \) (Definition \( \text{[2.2]} \)), and whenever \( n, nq \in \mathcal{N} \) (with \( q \) prime) we join \( n \) and \( nq \) by an edge.

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

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

and if \( e \) is the edge joining \( n \) and \( nq \) define

- \( S(e) := H^1_{tr}(K_q, T/I_{nq}T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}(n)}(K, T/I_{nq}T)) \otimes G_{nq} \),
- \( \psi^q_n : S(n) \rightarrow S(e) \) is the upper map of \( \text{(10.2)} \),
- \( \psi^q_{nq} : S(nq) \rightarrow S(e) \) is the lower map of \( \text{(10.2)} \).

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

**Definition 10.4.** A **Kolyvagin system** for \( (T, F, P, r) \) (or simply a Kolyvagin system of rank \( r \) for \( T \), if \( F \) and \( P \) are fixed) is a global section of the Selmer sheaf \( S \).

We write \( KS_r(T, F, P) \), or simply \( KS_r(T) \) when there is no risk of confusion, for the \( R \)-module of Kolyvagin systems \( \Gamma(S) \).

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

\[ \{ \kappa_n \in (\wedge^r H^1_{\mathcal{F}(n)}(K, T/I_nT)) \otimes G_n : n \in \mathcal{N} \} \]

such that if \( q \) is prime and \( nq \in \mathcal{N} \), the images of \( \kappa_n \) and \( \kappa_{nq} \) coincide in the diagram \( \text{(10.2)} \).

**Remark 10.5.** The definition of Kolyvagin system given in \( \text{[MR1]} \) 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 $(T, F, P, r)$ as in Definition 11.1 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 $n \in N$ we defined

\[ \lambda(n) := \text{length}_R(H^1_{F(n)}(K, T^*)) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}. \]

We say that a vertex $n \in N$ is a core vertex if $\lambda(n) = 0$.

**Proposition 11.1.** The following are equivalent:

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

**Proof.** We have (i) $\iff$ (ii) by Corollary 3.3 and (i) $\iff$ (iv) by Proposition 11.2. It is easy to see that (ii) $\iff$ (iii). \qed

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

\[ \psi_n^e(m^{\lambda(n)}S(n)) = \psi_{nq}^e(m^{\lambda(nq)}S(nq)) \subset S(e). \]

**Proof.** By Proposition 4.3(ii) and Definition 10.3 of $\psi_n^e$ and $\psi_{nq}^e$, we have

\[ \psi_n^e(S(n)) = \phi_q^{e_0}(\text{loc}_q(H^1_{F(n)}(K, T))) \otimes H^1_{F(n)}(K, T) \otimes G_n, \]

\[ \psi_{nq}^e(S(nq)) = \text{loc}_q(H^1_{F(nq)}(K, T)) \otimes H^1_{F(nq)}(K, T) \otimes G_{nq}. \]

By [MR1] Lemma 4.1.7, global duality shows that

\[ m^{\lambda(n)}\psi_n^e(\text{loc}_q(H^1_{F(n)}(K, T))) = m^{\lambda(nq)}\text{loc}_q(H^1_{F(nq)}(K, T)) \otimes G_q \]

and the proposition follows. \qed

We define a subsheaf $S'$ of the Selmer sheaf $S$ as follows.

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

- $S'(n) := m^{\lambda(n)}S(n) = m^{\lambda(n)}(\wedge^r H^1_{F(n)}(K, T)) \otimes G_n \subset S(n)$ if $n \in N$,
- $S'(e)$ is the image of $S'(n)$ in $S(e)$ under the vertex-to-edge map of $S$, if $n$ 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 $S$.

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

**Remark 11.5.** It is shown in [MR1] Theorem 4.4.1 that when the core rank $\chi(T) = 1$, we have $\text{KS}'_s(T) = \text{KS}'_s(T)$. In other words, in that case for every Kolyvagin system $\kappa \in \text{KS}_r(T)$ and $n \in N$, we have $\kappa_n \in m^{\lambda(n)}H^1_{F(n)}(K, T) \otimes G_n$.

**Theorem 11.6.** (i) There are core vertices.
(ii) Suppose \( n, n' \) are core vertices. Then there is a path

\[
n = n_0 \xrightarrow{e_1} n_1 \xrightarrow{e_2} \cdots \xrightarrow{e_l} n_l = n'
\]

in \( \mathcal{X} \) such that every \( n_i \) is a core vertex and all of the maps \( \psi_{n_i}^{e_i+1} \) and \( \psi_{n_i}^{e_i} \) are isomorphisms.

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

Theorem \ref{thm:kernel} will be proved in \cite{14}. In the remainder of this section we derive some consequences of it.

\begin{theorem}
(i) The module \( \text{KS}'(T) \) of stub Kolyvagin systems is free of rank one over \( R \), and for every core vertex \( n \) the specialization map

\[
\text{KS}'(T) \longrightarrow S'(n) = (\wedge^r H^1\{T\}(K,T)) \otimes G_n
\]

given by \( \kappa \mapsto \kappa_n \) is an isomorphism.

(ii) There is a Kolyvagin system \( \kappa \in \text{KS}'(T) \) such that \( \kappa_n \) generates \( S'(n) \) for every \( n \in N \).

(iii) The locally cyclic sheaf \( S' \) has trivial monodromy.
\end{theorem}

\begin{proof}
This follows from Proposition \ref{prop:base} using Theorem \ref{thm:kernel}(i,iii).
\end{proof}

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

\begin{theorem}
Suppose that \( R \) is a discrete valuation ring, and hypotheses \ref{hyp:R} through \ref{hyp:G} are satisfied for the Selmer data \((T, F, P, r)\). For \( k > 0 \) let \( P_k \subset P \) be as in Definition \ref{def:projection}.

The natural maps \( T \to T/m^k \) and \( P_k \to P \) induce an isomorphism

\[
\text{KS}'_r(T, P) \xrightarrow{\sim} \varprojlim \text{KS}'_r(T/m^kT, P_k).
\]

The \( R \)-module \( \text{KS}'_r(T, P) \), is free of rank one, generated by a Kolyvagin system \( \kappa \) whose image in \( \text{KS}'_r(T/mT) \) is nonzero. The maps \( \text{KS}'_r(T, P) \to \text{KS}'_r(T/m^k, P_k) \) are surjective.
\end{theorem}

\begin{proof}
This can be proved easily directly from Theorem \ref{thm:kernel} as in the proofs of Proposition \ref{prop:base} and Theorem \ref{thm:properties} for Stark systems. See also \cite{MR1}, Proposition 5.2.9.
\end{proof}

\begin{remark}
When \( r = \chi(T) > 1 \), it is not generally true that \( \text{KS}'_r(T) = \text{KS}_r(T) \). For example, suppose \( R \) is principal artinian of length \( k > 1 \), and suppose \( m \in N \) is such that \( H^1\{m\}(K, T) \cong R' \oplus (R/m)^r \), with corresponding basis \( c_1, \ldots, c_r, d_1, \ldots, d_r \). Let \( g_m \) be a generator of \( G_m \).

For every \( q \in P \) and every \( i \), \( \text{loc}_q(d_i) \) is killed by \( m \), so it is divisible by \( m^{k-1} \) in the free \( R \)-module \( H^1(K_n, T) \). It follows that if we define \( \kappa := \{\kappa_n\} \) where

\[
\kappa_n := \begin{cases} (d_1 \wedge \cdots \wedge d_r) \otimes g_m & \text{if } n = m, \\ 0 & \text{if } n \neq m, \end{cases}
\]

then \( \kappa \) is a Kolyvagin system, but \( \kappa_m \notin S'(m) \) so \( \kappa \notin \text{KS}'_r(T) \).
\end{remark}
12. Kolyvagin systems and Stark systems

Suppose that $R$ is a principal artinian ring, and fix Selmer data $(T, F, P, r)$ as in Definition 6.4, such that $I_q = 0$ for every $q \in P$. Recall the $R$ module $Y_n$ of Definition 6.2 and let $\text{loc}_q^\ast: H^1 (K, T) \to H^1_{\text{tr}} (K, T) \otimes G_q$ and $\text{loc}_q^r: H^1 (K, T) \to H^1_{\text{tr}} (K, T)$ be the maps of Definition 6.2.

**Definition 12.1.** Suppose $n \in \mathcal{N}$. By (6.4) we have an exact sequence

$$0 \to H^1_{F(n)} (K, T) \to H^1_{\text{tr}} (K, T) \oplus \bigoplus_{q \mid n} H^1_{\text{tr}} (K_q, T) \otimes G_q$$

and it follows that the square

$$\begin{array}{ccc}
H^1_{F(n)} (K, T) & \to & H^1_{\text{tr}} (K, T) \\
\downarrow & & \downarrow \\
0 & \to & \bigoplus_{q \mid n} H^1_{\text{tr}} (K_q, T) \otimes G_q
\end{array}$$

is cartesian. Proposition 4.3(i,iv) attaches to this diagram a map

$$\wedge^{r+\nu(n)} H^1_{F(n)} (K, T) \otimes \wedge^{\nu(n)} \text{Hom}(\bigoplus_{q \mid n} H^1_{\text{tr}} (K_q, T) \otimes G_q, R) \to \wedge^r H^1_{F(n)} (K, T).$$

Tensoring both sides with $G_n$ defines a map

$$\Pi_n : Y_n \to \wedge^r H^1_{F(n)} (K, T) \otimes G_n.$$

See the proof of Proposition 12.3 below for an explicit description of the map $\Pi_n$. Recall that if $m \mid n \in \mathcal{N}$, then $\Psi_{n, m} : Y_n \to Y_m$ 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 $H^1_{(F^*)^n} (K, T^*) = 0$ and $m \mid n$, then

$$(\Pi_m \circ \Psi_{n, m})(Y_n) = m^{\text{length}(H^1_{F^*(m)} (K, T^*))} S(m) = S'(m).$$

**Proof.** If $H^1_{(F^*)^n} (K, T^*) = 0$ then $H^1_{F^*n}(K, T)$ is free of rank $r + \nu(n)$ over $R$ by Corollary 5.5(ii). By (6.3) and (6.4) we have

$$(\cap_{q \mid m} \ker(\text{loc}_q^f | H^1_{F(n)} (K, T))) \cap (\cap_{q \mid (n/m)} \ker(\text{loc}_q^r | H^1_{F^*(n/m)} (K, T))) = H^1_{F(n)} (K, T).$$

Now the lemma follows from Proposition 4.3(ii,iii) applied to the cartesian square

$$\begin{array}{ccc}
H^1_{F(m)} (K, T) & \to & H^1_{F(n)} (K, T) \\
\downarrow & & \downarrow \\
0 & \to & \bigoplus_{q \mid m} \text{loc}_q^f \oplus_{q \mid n/(n/m)} \text{loc}_q^r \\
& & \bigoplus_{q \mid n} H^1_{\text{tr}} (K_q, T) \otimes G_q \oplus H^1_{\text{tr}} (K_q, T)
\end{array}$$

□

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

(i) $\Pi(\epsilon) \in \text{KS}_s(T)$.

(ii) If hypotheses (H.1) through (H.7) of §4 hold, then $\Pi(\epsilon) \in \text{KS}'_s(T)$. 
Corollary 13.1. Suppose for this section that $R$ is a principal artinian local ring or a discrete valuation ring. We let $k := \text{length}(R)$, so $k$ is finite in the artinian case and $k = \infty$ in the discrete valuation ring case.

Fix Selmer data $(T, F, P, r)$ 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 Section 8 for Stark systems. We will say that a stub Kolyvagin system $\kappa$ is primitive if it is primitive as a global section of the stub Selmer sheaf $S'$ (Definition 9.3), i.e., if $\kappa$ generates the $R$-module $\text{KS}^r_n(T)$, or equivalently, if $\kappa_n$ generates $\mathfrak{m}^n(\wedge^n H^1_{F(n)}(K,T)) \otimes G_n$ for every $n \in \mathcal{N}$.

Corollary 13.1. Suppose $R$ is a principal artinian ring of length $k$, and $\kappa \in \text{KS}^r_n(T)$.

(i) If $\kappa_1 \neq 0$ then 
\[\text{length}(H^1_{F(n)}(K,T^*)) \leq k - \text{length}(R\kappa_1) = \max\{i : \kappa_1 \in \mathfrak{m}^i \wedge^n H^1_{F(n)}(K,T)\} \].

(ii) If $\kappa$ is primitive and $\kappa_1 \neq 0$, then equality holds in (i).
(iii) If $\kappa$ is primitive and $\kappa_1 = 0$, then $\text{length}(H^1_\kappa(K, T^*)) \geq k$.

**Proof.** By Corollary 3.3(iii), $S'(1) = m^{\lambda(1)} \cap^r H^1_\kappa(K, T)$ is a cyclic $R$-module of length $\text{max}(0, k - \text{length}(H^1_\kappa(K, T^*)))$. Since $\kappa_1 \in S'(1)$ by definition, (i) follows. If $\kappa$ is primitive, then $\kappa_1$ generates $S'(1)$, which proves (ii) and (iii).

The following definition is the analogue for Kolyvagin systems of Definitions 8.4 and 8.2 for Stark systems.

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

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

We also define the sequence of elementary divisors

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

**Proposition 13.3.** Suppose that $\kappa \in \text{KS}_\epsilon(T)$, $\epsilon \in \text{SS}_\tau(T)$, and $\kappa = \Pi(\epsilon)$. Then $\text{ord}(\kappa) = \text{ord}(\epsilon)$, $\partial\varphi_\kappa(i) = \partial\varphi_\epsilon(i)$ for every $i$, and $d_\kappa(i) = d_\epsilon(i)$ for every $i$.

**Proof.** Suppose first that $R$ is artinian of length $k$. Since $\Pi$ is an isomorphism (Theorem 12.4), we may assume without loss of generality that $\kappa$ and $\epsilon$ generate $\text{KS}_\epsilon(T)$ and $\text{SS}_\tau(T)$, respectively. Recall that $\mu(n) := \text{length}(H^1_{(\epsilon_*)}^1(K, T^*))$.

For every $n \in \mathcal{N}$, Theorem 11.7(ii) shows that $\kappa_n$ generates $m^{\lambda(n)}S(n)$, and Theorem 6.10 shows that $\epsilon_n$ generates $m^{\mu(n)}Y_n$. Thus

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

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 8.7. □

**Theorem 13.4.** Suppose $R$ is a discrete valuation ring, $\kappa \in \text{KS}_\epsilon(T)$ and $\kappa \neq 0$. Then:

(i) the sequence $\partial\varphi_\kappa(t)$ is nonincreasing, and finite for $t \geq \text{ord}(\kappa)$,
(ii) the sequence $d_\kappa(i)$ is nonincreasing, nonnegative, and finite for $i \geq \text{ord}(\kappa)$,
(iii) $\text{ord}(\kappa)$ and the $d_\kappa(i)$ are independent of the choice of nonzero $\kappa \in \text{KS}_\epsilon(T)$,
(iv) $\text{corank}_R(H^1_\kappa(K, T^*)) = \text{ord}(\kappa)$,
(v) $H^1_\kappa(K, T^*)/(H^1_\kappa(K, T^*))_{\text{div}} \cong \oplus_{i \geq \text{ord}(\kappa)} R/m^d_\kappa(i)$,
(vi) $\text{length}_R(H^1_\kappa(K, T^*)/(H^1_\kappa(K, T^*))_{\text{div}}) = \partial\varphi_\kappa(\text{ord}(\kappa)) - \partial\varphi_\kappa(\infty)$, where $\partial\varphi_\kappa(\infty) := \lim_{t \to \infty} \partial\varphi_\kappa(t)$.
(vii) $\kappa$ is primitive if and only if $\partial\varphi_\kappa(\infty) = 0$,
(viii) $\text{length}(H^1_\kappa(K, T^*))$ is finite if and only if $\kappa_1 \neq 0$,
(ix) $\text{length}(H^1_\kappa(K, T^*)) \leq \partial\varphi_\kappa(0) = \max\{s : \kappa_1 \in m^s \cap^r H^1_\kappa(K, T)\}$, with equality if and only if $\kappa$ is primitive.

**Proof.** By Theorem 12.4, there is a (unique) $\epsilon \in \text{SS}_\tau(T)$ such that $\Pi(\epsilon) = \kappa$. By Proposition 13.3, all the invariants of Definition 13.2 attached to $\kappa$ are equal to the corresponding invariants of $\epsilon$. Now the theorem follows from Theorem 8.9. □
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 that $r = \chi(T)$, the core rank of $T$.

**Lemma 14.1.** The sheaf $S'$ is locally cyclic.

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

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

(i) $\text{loc}_n : H^1_{\mathcal{F}(n)}(K,T)[m] \to H^1_{\mathcal{T}}(K_q,T)$ is nonzero,

(ii) $nq$ is a core vertex and both maps $\psi^n_e : S(n) \to S(e)$, $\psi^n_{nq} : S(nq) \to S(e)$ are isomorphisms.

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

Further, since $\text{loc}_q : H^1_{\mathcal{F}(n)}(K,T) \to H^1_{\mathcal{T}}(K_q,T)$ is surjective, and $H^1_{\mathcal{T}}(K_q,T)$ is free of rank one over $R$, and $H^1_{\mathcal{T}}(K_q,T^*) = 0$, [MR1] Lemma 4.1.6 shows that $nq$ is a core vertex and $\text{loc}_n : H^1_{\mathcal{F}(n)}(K,T) \to H^1_{\mathcal{T}}(K_q,T)$ is surjective. Now Proposition A.1 shows that that $\psi^n_{nq}$ is an isomorphism. Thus (ii) holds.

Conversely, if $\psi^n_e$ is an isomorphism then Proposition A.1 shows that the map $\text{loc}_q : H^1_{\mathcal{F}(n)}(K,T) \to H^1_{\mathcal{T}}(K_q,T)$ is surjective, and since $H^1_{\mathcal{T}}(K_q,T)$ is free of rank one over $R$ it follows that $\text{loc}_q$ is not identically zero on $H^1_{\mathcal{F}(n)}(K,T)[m]$. Thus (ii) implies (i). \hfill \Box

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

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

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

**Proof.** By [MR1] Proposition 3.6.1 we can use the Cebotarev theorem to choose a prime $q \in \mathcal{P}$ such that the localization maps

$$m^{k-1}H^1_{\mathcal{F}(n)}(K,T) \to H^1_{\mathcal{T}}(K_q,T), \quad H^1_{\mathcal{F}(n)^+}(K,T^+)[m] \to H^1_{\mathcal{T}}(K_q,T^+)$$

are both nonzero. (Note that $m^{k-1}H^1_{\mathcal{F}(n)}(K,T) \neq 0$ by Corollary 8.3(iii).) Then by Poitou-Tate global duality (see for example [MR1] Lemma 4.1.7(iv)), we have $\bar{\lambda}(nq) < \bar{\lambda}(n)$. Further, we have that localization $H^1_{\mathcal{F}(n)}(K,T) \to H^1_{\mathcal{T}}(K_q,T)$ is surjective, so by Proposition A.1(ii)

$$\text{loc}_q : \wedge^r H^1_{\mathcal{F}(n)}(K,T) \longrightarrow H^1_{\mathcal{T}}(K_q,T) \otimes (\wedge^{r-1} H^1_{\mathcal{F}(n)}(K,T))$$

are both nonzero.
is surjective as well. Since $S'(e)$ is defined to be the image of
\[ S'(n) := m^{λ(n)}(\wedge^r H^1_{Fq}(K, T)) \otimes G_n \]
under the upper maps of (10.2), we deduce that
\[ S'(e) = m^{λ(n)}H^1_{tr}(K_q, T) \otimes (\wedge^{r-1} H^1_{Fq}(n, K, T)) \otimes G_{aq}. \]
Thus
\[ \text{length}_R(S'(e)) \geq k - λ(n) = \text{length}_R(S'(n)), \]
the equality by Corollary 3.5 iii). Since the map $S'(n) \to S'(e)$ is surjective by definition, it must be an isomorphism. □

**Theorem 14.4.** Suppose $n, n'$ are core vertices. Then there is a path
\[ n = n_0 \xrightarrow{e_1} n_1 \xrightarrow{e_2} \cdots \xrightarrow{e_t} n_t = n' \]
in $X$ such that every $n_i$ is a core vertex and all of the maps $ψ_{n_i}^{e_t+1}$ and $ψ_{n_i}^{e_t}$ are isomorphisms.

**Proof.** When $χ(T) = 1$, this is [MR1 Theorem 4.3.12]. The general case can be proved in the same way, but instead we will prove it here by induction on $r := χ(T)$.

Denote by $F$ the induced Selmer structure on $T$. By Proposition 3.3 and the definition of core vertices we see that the Selmer sheaves $S_{(T, F, P)}$ and $S_{(F, T, P)}$ have the same core vertices and the same core rank $r$ (see also [MR1 Theorem 4.1.3]).

Since $r > 0$, we can fix nonzero classes $c \in H^1_{F(n)}(K, T)$ and $c' \in H^1_{F(n)}(K, T)$. By [MR1 Proposition 3.6.1], we can use the Cebotarev theorem to choose $q \in P$, not dividing $n$, such that the localizations $c_q$ and $c'_q$ are both nonzero.

Note that the Selmer triple $(\bar{T}, \bar{F}, P - \{q\})$ 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 $R/m$). By our choice of $q$, both localization maps
\[ \text{loc}_q : H^1_{F(n)}(K, T) \to H^1_{F(n)}(K_q, T), \quad \text{loc}_q : H^1_{F(n)}(K, T) \to H^1_{F(n)}(K_q, T) \]
are nonzero, and $H^1_{F(n)}(K_q, T)$ is a one-dimensional $R/m$-vector space, so both maps are surjective. Since $n$ and $n'$ are core vertices for $(\bar{T}, \bar{F})$, it follows that
\[ \dim_{R/m} H^1_{Fq(n)}(K, \bar{T}) = \dim_{R/m} H^1_{Fq(n')} (K, \bar{T}) = r - 1 \]
and (by Poitou-Tate global duality, see for example [MR1 Theorem 2.3.4]) that
\[ H^1_{Fq(n)}(K, \bar{T}^*) = H^1_{Fq(n')}(K, \bar{T}^*) = 0. \]

In particular we deduce that $χ(\bar{T}, Fq) = r - 1$, and that $n, n'$ are core vertices for the sheaf $S_{\bar{T}, Fq}$. By our induction hypotheses we conclude that there is a path
\[ n = n_0, n_1, \ldots, n_t = n' \]
in $X$ such that every $n_i$ is prime to $q$, every $n_i$ is a core vertex for $S_{\bar{T}, Fq}$, and every vertex-to-edge map (for $S_{\bar{T}, Fq}$) along the path is an isomorphism. We will show that every $n_i$ is a core vertex for $S_{T, F}$, and every vertex-to-edge map (for $S_{T, F}$) along the path is an isomorphism. This will prove the theorem.

Fix $i$, $0 \leq i \leq t$. The exact sequence
\[ 0 \to H^1_{Fq(n_i)}(K, \bar{T}) \to H^1_{Fq(n_i)}(K, \bar{T}) \xrightarrow{\text{loc}_q} H^1_{Fq(n_i)}(K_q, T) \]
shows that $\dim_{R/m} H^1_{Fq(n_i)}(K, T) \leq r$. Then Corollary 3.5 i) (applied to $\bar{T}, \bar{F}$, and $R/m$) shows that $n_i$ is a core vertex of $S_{\bar{T}, \bar{F}}$, and hence is a core vertex of $S_{T, F}$. 


Further, suppose \( l \) is a prime such that \( n_{l+1} = n_l \), and let \( e \) be the edge joining those two vertices. By assumption, the maps \( S_{\bar{F}, \bar{q}}(n_l) \rightarrow S_{\bar{F}, \bar{q}}(e) \) and \( S_{\bar{F}, \bar{q}}(n_l) \rightarrow S_{\bar{F}, \bar{q}}(\bar{e}) \) are isomorphisms, so by Lemma 14.2 the localization map \( H^1_{\bar{F}, \bar{q}}(n_l)(K, \bar{T}) \rightarrow H^1_{\bar{F}, \bar{q}}(K, \bar{T}) \) is nonzero. But
\[
H^1_{\bar{F}, \bar{q}}(n_l)(K, \bar{T}) \subset H^1_{\bar{F}, \bar{q}}(K, \bar{T}) = H^1_{\bar{F}, \bar{q}}(K, T)[m],
\]
so \( \text{loc}_1 : H^1_{\bar{F}, \bar{q}}(K, T)[m] \rightarrow H^1_{\bar{F}, \bar{q}}(K, T) \) is nonzero, so by Lemma 14.2 both of the maps \( \psi^e_{n_l} \) and \( \psi^e_{n_{l+1}} \) are isomorphisms. This completes the proof. □

Corollary 14.5. There are core vertices. More precisely:

(i) for every \( n \in \mathcal{N} \) there is an \( n' \in \mathcal{N} \) prime to \( n \), with \( nn' \) is a core vertex,

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

Proof. Choose \( n \in \mathcal{N} \). For every \( n' \in \mathcal{N} \) prime to \( n \), global duality (see for example [MR1] Lemma 4.1.7(i)) shows that
\[
\tilde{\lambda}(nn') \geq \tilde{\lambda}(n) - \nu(n').
\]

Applying Proposition 14.3, we can construct \( n = n_0, n_1, n_2, \ldots \in \mathcal{N} \) inductively, with \( n_{i+1} = n_i q_i \) for some prime \( q_i \in \mathcal{N} \) and \( \lambda(n_{i+1}) < \lambda(n_i) \), until we reach \( n_d \in \mathcal{N} \) with \( \lambda(n_d) = 0 \). Then \( H^1_{\bar{F}(n_d)^*}(K, T^*)[m] = H^1_{\bar{F}(n_d)^*}(K, T^*) = 0 \), so \( n_d \) is a core vertex. Setting \( n' := n_d/n \) we have
\[
\nu(n') = d \leq \lambda(n) = \dim_{R/m} H^1_{\bar{F}(n_d^*)}(K, T^*)[m].
\]
By (14.6), since \( \tilde{\lambda}(nn') = 0 \) we have \( \nu(n') \geq \tilde{\lambda}(n) \), and so \( \nu(n') = \tilde{\lambda}(n) \). This proves (i), and applying (i) with \( n = 1 \) and (14.6) proves (ii). □

Proof of Theorem 11.7. Theorem 11.9(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 14.4, we need only show that every core vertex is a hub of \( \mathcal{S}' \).

Fix a core vertex \( n_0 \), and let \( n \in \mathcal{N} \) be any other vertex. We will show by induction on \( \tilde{\lambda}(n) \) that there is an \( \mathcal{S}' \)-surjective path from \( n_0 \) to \( n \).

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

Now suppose \( \tilde{\lambda}(n) > 0 \). Use Proposition 14.3 to find \( q \in \mathcal{P} \) not dividing \( n \) such that \( \tilde{\lambda}(nq) < \tilde{\lambda}(n) \) and \( \psi^e_n : \mathcal{S}'(n) \rightarrow \mathcal{S}'(e) \) is an isomorphism, where \( e \) is the edge joining \( n \) and \( nq \). By induction there is an \( \mathcal{S}' \)-surjective path from \( n_0 \) to \( nq \), and if we adjoin to that path the edge \( e \), we get an \( \mathcal{S}' \)-surjective path from \( n_0 \) to \( n \). □

Appendix A. Some exterior algebra

Suppose for this appendix that \( R \) is a local principal ideal ring with maximal ideal \( m \).

Proposition A.1. Suppose \( 0 \rightarrow N \rightarrow M \xrightarrow{\psi} C \) 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

\[\text{dim}_{R/m} \hat{\psi}(nn') = \tilde{\lambda}(n). \]
Proposition A.3. \(\psi\) modules \(\hookrightarrow\) with maps induced by the inclusions
\[\psi(M) \otimes \wedge^{r-1}N \to C \otimes \wedge^{r-1}M\]
is given by
\[m_1 \wedge \cdots \wedge m_r \mapsto \sum_{i=1}^{r} (-1)^{i+1}(m_i) \otimes (m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \cdots \wedge m_r),\]

(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 \(\psi\) is surjective.

\[\text{Proof.}\]
Since \(R\) is principal, we can “diagonalize” \(\psi\) 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 \(\hat{\psi}_0 : \wedge^r M \to \psi(M) \otimes \wedge^{r-1}M\). Consider the diagram

\[
\begin{array}{ccc}
\wedge^r M & \xrightarrow{\hat{\psi}_0} & \psi(M) \otimes \wedge^{r-1}M \\
& \downarrow{\eta_1} & \downarrow{\eta_2} \\
\psi(M) \otimes \wedge^{r-1}N & \to & C \otimes \wedge^{r-1}N
\end{array}
\]

with maps induced by the inclusions \(\psi \to C\) and \(N \hookrightarrow M\). We will show that
image\((\hat{\psi}_0)\) \(\subset\) 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 image\((\hat{\psi}_0)\) \(\subset\) 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 \(I\psi(M) = 0\),
\[
\ker(\eta_1) = \ker(\psi(M) \otimes Im \otimes \wedge^{r-2}N_0) \to \psi(M) \otimes Rm \otimes \wedge^{r-2}N_0
\]
\[= \psi(M) \otimes Im \otimes \wedge^{r-2}N_0.\]

We further have
\[
(\text{A.2}) \quad \eta_2(\psi(M) \otimes Im \otimes \wedge^{r-2}N_0) = 0.
\]

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.2)
\[
\eta_2(\psi(M) \otimes \wedge^{r-1}N) = \eta_2(\psi(M) \otimes \wedge^{r-1}N_0)
\]
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 \(M^* := \text{Hom}(M, R)\).

**Proposition A.3.** Suppose \(R\) is artinian and there is a cartesian diagram of \(R\)-modules
\[
\begin{array}{ccc}
M_1 & \xrightarrow{h} & M_2 \\
\downarrow & & \downarrow \\
C_1 & \xrightarrow{\bar{h}} & C_2
\end{array}
\]
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 \( s_i = \text{rank}_R(C_i) \). There is a canonical \( R \)-module homomorphism

\[
\wedge^{r+s_2}M_2 \otimes \wedge^{s_2}C_2^* \rightarrow \wedge^{r+s_1}M_1 \otimes \wedge^{s_1}C_1^*
\]

defined as follows. If \( m \in \wedge^{r+s_2}M_2, \psi_1, \ldots, \psi_{s_2} \) is a basis of \( C_2^* \) such that \( \psi_{s_1+1}, \ldots, \psi_{s_2} \) is a basis of \( (C_2/C_1)^* \), 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 \( \psi_i \).

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

\[
m^{\text{length}(M_1)-(r+s_1)} \rightarrow \wedge^{r+s_1}M_1 \otimes \wedge^{s_1}C_1^*.
\]

(iii) If

\[
\begin{array}{ccc}
M_2 & \rightarrow & M_3 \\
\downarrow & & \downarrow \\
C_2 & \rightarrow & C_3
\end{array}
\]

is another such cartesian square, then the triangle

\[
\begin{array}{ccc}
\wedge^{r+s_2}M_3 \otimes \wedge^{s_2}C_3^* & \rightarrow & \wedge^{r+s_1}M_1 \otimes \wedge^{s_1}C_1^* \\
\downarrow & \swarrow & \downarrow \\
\wedge^{r+s_2}M_2 \otimes \wedge^{s_2}C_2^*
\end{array}
\]

induced by the maps of (i) commutes.

(iv) Suppose there is an exact sequence \( 0 \rightarrow M_1 \rightarrow M_2 \rightarrow C \), 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 \( \wedge^{r+s}M_2 \otimes \wedge^sC^* \rightarrow \wedge^rM_1 \).

**Proof.** Since the square is cartesian, and by our choice of the \( \psi_i \), we have

\[
\text{ker}(\oplus_{i=1}^{s_2} h_i) = h^{-1}(C_1) = M_1.
\]

Applying Proposition [A.1] repeatedly shows that the map defined in (i) takes values in \( \wedge^{r+s_1}M_1 \otimes \wedge^{s_1}C_1^* \). It is straightforward to check that this map is independent of the choice of the \( \psi_i \). 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 \( C_2^* \) 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 \( h_{s_1+j} = \sum a_{ij} \eta_i \). Let \( N := \bigcap_{i=1}^{s_1} \ker(\eta_i) \). Then \( N \) is free over \( R \) of rank \( r + s_1 \), and we have a split exact sequence of free modules

\[
0 \rightarrow N \rightarrow M_2 \overset{\oplus_{i \leq s_1} \eta_i}{\rightarrow} R^s \rightarrow 0.
\]

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

We also have

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

and \( N \subset M_1 \) by (A.4). Since \( N \) is free, there is a noncanonical splitting

\[
M_1 \cong N \oplus M_1/N,
\]
so the map 
\[ m^{\text{length}(M_1/N)} \wedge r+s_1 N \longrightarrow m^{\text{length}(M_1/N)} \wedge r+s_1 M_1 \]
induced by the inclusion \( N \hookrightarrow M_1 \) is surjective. Finally, 
\[ \det(A)R = m^{\text{length}(M_1/N)} = m^{\text{length}(M_1)-(r+s_1)\text{length}(R)}, \]
and combining these facts proves (ii).

Assertion (iii) follows from the independence of the choice of the \( \psi_i \). Choose a basis \( \psi_1, \ldots, \psi_s \) of \( \mathbb{C}^3 \) such that \( \psi_{s_1+1}, \ldots, \psi_{s_3} \) is a basis of \( (C_3/C_1)^* \) and \( \psi_{s_2+1}, \ldots, \psi_{s_3} \) is a basis of \( (C_3/C_2)^* \). Then \( \psi_{s_1+1}|C_2, \ldots, \psi_{s_2}|C_2 \) is a basis of \( (C_2/C_1)^* \), and (iii) just reduces to the statement that
\[ (\hat{\psi}_{s_1+1} \circ \cdots \circ \hat{\psi}_{s_2}) \circ (\hat{\psi}_{s_2+1} \circ \cdots \circ \hat{\psi}_{s_3}) = (\hat{\psi}_{s_1+1} \circ \cdots \circ \hat{\psi}_{s_3}) \].

\[ \square \]

**Erratum to [MR1].** We thank Clément Gomez for pointing out an error in the statement of [MR1, Lemma 2.1.4]. The correct statement (which is all that was used elsewhere in [MR1]) should be:

**Lemma 2.1.4.** If \( (T/mT)^{G_\mathbb{Q}} = 0 \) then \( (T/IT)^{G_\mathbb{Q}} = 0 \) for every ideal \( I \) of \( R \).

**References**

[MR1] B. Mazur, K. Rubin, Kolyvagin systems. *Memoirs of the Amer. Math. Soc.* **799** (2004).
[MR2] B. Mazur, K. Rubin, Refined class number formulas for \( G_m \). To appear. [http://math.uci.edu/~krubin/preprints/generaldc.pdf](http://math.uci.edu/~krubin/preprints/generaldc.pdf)
[Mi] J.S. Milne, Arithmetic duality theorems. *Perspectives in Math.* **1**, Orlando: Academic Press (1986).
[PR1] B. Perrin-Riou, Théorie d’Iwasawa et hauteurs \( p \)-adiques. *Invent. Math.* **109** (1992) 137–185.
[PR2] B. Perrin-Riou, Systèmes d’Euler \( p \)-adiques et théorie d’Iwasawa. *Ann. Inst. Fourier (Grenoble)* **48** (1998) 1231–1307.
[Ru1] K. Rubin, A Stark conjecture “over \( \mathbb{Z} \)” for abelian \( L \)-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)* **46** (1996) 33–62.
[Ru2] K. Rubin, Euler Systems. *Annals of Math. Studies* **147**, Princeton: Princeton University Press (2000).
[S] T. Sano, A generalization of Darmon’s conjecture for Euler systems for general \( p \)-adic representations. To appear.
[T] J. Tate, Les Conjectures de Stark sur les Fonctions L d’Artin en \( s = 0 \). *Prog. in Math.* **47**, Birkhäuser, Boston-Basel-Stuttgart (1984).
[W] A. Wiles, Modular elliptic curves and Fermat’s Last Theorem. *Annals of Math.* **141** (1995) 443–551.

**Department of Mathematics, Harvard University, Cambridge, MA 02138 USA**

*E-mail address: mazur@math.harvard.edu*

**Department of Mathematics, UC Irvine, Irvine, CA 92697 USA**

*E-mail address: krubin@math.uci.edu*