Euler systems

Karl Rubin

Author address:

Department of Mathematics
Stanford University
Stanford, CA 94305-2125
USA

E-mail address: `rubin@math.stanford.edu`

Contents

Introduction

History. In 1986, Francisco Thaine [**Th**] discovered a remarkable method to bound ideal class groups of real abelian extensions of $\mathbf{Q}$. Namely, if F is such a field, he used cyclotomic units in fields $F(\boldsymbol{\mu}_\ell)$, for a large class of rational primes ℓ, to construct explicitly a large collection of principal ideals of F. His construction produced enough principal ideals to bound the exponent of the different Galois-eigencomponents of the ideal class group of F, in terms of the cyclotomic units of F. Thaine's results were already known (as a Corollary of the proof by Mazur and Wiles [**MW**] of Iwasawa's "Main Conjecture") but Thaine's proof was very much simpler. The author [**Ru1**] was able to apply Thaine's method essentially unchanged to bound ideal class groups of abelian extensions of imaginary quadratic fields in terms of elliptic units, with important consequences for the arithmetic of elliptic curves with complex multiplication.

Shortly after this, Kolyvagin [**Ko1**] discovered independently a similar remarkable method, in his case to bound the Selmer group of an elliptic curve. Suppose E is a modular elliptic curve over $\mathbf{Q}$, with sign $+1$ in the functional equation of its L-function. Kolyvagin's method used Heegner points on E over anticyclotomic extensions of prime conductor of an imaginary quadratic field K (in place of cyclotomic units in abelian extensions of $\mathbf{Q}$) to construct cohomology classes over K (in place of principal ideals). He used these cohomology classes, along with duality theorems from Galois cohomology, to bound the exponent of the Selmer group of E over $\mathbf{Q}$. The overall structure of his proof was very similar to that of Thaine.

Inspired by Thaine's work and his own, Kolyvagin then made another fundamental advance. In his paper [**Ko2**] he introduced what he called "Euler systems." In Thaine's setting (the Euler system of cyclotomic units) Kolyvagin showed how to use cyclotomic units in fields $F(\boldsymbol{\mu}_r)$, for a large class of integers r (no longer just primes), to bound the *orders* of the different Galois-eigencomponents of the ideal class group of F, rather than just their exponents. Similarly, by using a larger collection of Heegner points in the situation described above, Kolyvagin was able to give a bound for the order of the Selmer group of E. Thanks to the theorem of Gross and Zagier [**GZ**], which links Heegner points with the L-function of E, Kolyvagin's bound is closely related to the order predicted by the Birch and Swinnerton-Dyer conjecture.

This book. This book describes a general theory of Euler systems for p-adic representations. We start with a finite-dimensional p-adic representation T of the Galois group of a number field K. (Thaine's situation is the case where T is $\varprojlim \boldsymbol{\mu}_{p^n}$ twisted by an even Dirichlet character, and Kolyvagin's is the case where T is the

Tate module of a modular elliptic curve.) We define an Euler system for T to be a collection of cohomology classes in $\mathbf{c}_F \in H^1(F,T)$, for a family of abelian extensions F of K, with properties relating $\mathbf{c}_{F'}$ and $\mathbf{c}_F$ when $F \subset F'$. Our main results show how the existence of an Euler system leads to bounds on the orders of Selmer groups attached to the Galois module $\mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty})$, bounds which depend only on the given Euler system.

The proofs of these theorems in this general setting parallel closely (with some additional complications) Kolyvagin's original proof. Results similar to ours have recently been obtained independently by Kato [**Ka2**] and Perrin-Riou [**PR5**].

What we do *not* do here is construct new Euler systems. This is the deepest and most difficult part of the theory. Since Kolyvagin's introduction of the concept of an Euler system there have been very few new Euler systems found, but each has been extremely important. Kato [**Ka3**] has constructed a new Euler system for a modular elliptic curve over $\mathbf{Q}$, very different from Kolyvagin's system of Heegner points (see Chapter III §5). Flach [**Fl**] has used a collection of cohomology classes (but not a complete Euler system in our sense) to bound the exponent but not the order of the Selmer group of the symmetric square of a modular elliptic curve.

One common feature of all the Euler systems mentioned above is that they are closely related to special values of L-functions (and thereby to p-adic L-functions). An important benefit of this connection is that the bounds on Selmer groups that come out of the theory are then linked to L-values. Such bounds then provide evidence for the Bloch-Kato conjectures [**BK**], which predict the orders of these Selmer groups in terms of L-values.

Our definition of Euler system says nothing about L-values. If there is an Euler system for T then there is a whole family of them (for example, the collection of Euler system cohomology classes is a $\mathbf{Z}_p$-module, as well as a $\mathrm{Gal}(\bar{K}/K)$-module). If one multiplies an Euler system by p, one gets a new Euler system but a worse bound on the associated Selmer groups. The philosophy underlying this book, although it is explicitly discussed only in Chapter VIII, is that under certain circumstances, not only should there exist an Euler system for T, but there should exist a "best possible" Euler system, which will be related to (and contain all the information in) the p-adic L-function attached to T.

A remark about generality. It is difficult to formulate the "most general" definition of an Euler system, and we do not attempt to do this here. The difficulty is partly due to the fact that the number of examples on which to base a generalization is quite small. In the end, we choose a definition which does not cover the case of Kolyvagin's Heegner points, because to use a more inclusive definition would introduce too many difficulties. (In Chapter IX we discuss possible modifications of our definition, including one which does include the case of Heegner points.) On the other hand, we do allow the base field K to be an arbitrary number field, instead of requiring $K = \mathbf{Q}$. Although this adds a layer of notation to all proofs, it does not significantly increase the difficulty. A reader wishing to restrict to the simplest (and most interesting) case $K = \mathbf{Q}$ should feel free to do so.

Organization. In Chapter I we introduce the local and global cohomology groups, and state the duality theorems, which will be required to state and prove our main results. Chapter II contains the definition of an Euler system, followed by the statements of our main theorems bounding the Selmer group of $\mathrm{Hom}(T, \boldsymbol{\mu}_{p^\infty})$ over the base field K (§2) and over $\mathbf{Z}_p^d$-extensions K_∞ of K (§3).

Chapter III contains sample applications of the theorems of Chapter II. We apply those theorems to three different Euler systems: the first constructed from cyclotomic units, to study ideal class groups of real abelian fields (§III.2); the second constructed from Stickelberger elements, to study the minus part of ideal class groups of abelian fields (§III.4); and the third constructed by Kato from Beilinson elements in the K-theory of modular curves, to study the Selmer groups of modular elliptic curves (§III.5).

The proofs of the theorems of Chapter II are given in Chapters IV through VII. In Chapter IV we give Kolyvagin's "derivative" construction, taking the Euler system cohomology classes defined over abelian extensions of K and using them to produce cohomology classes over K itself. We then analyze the localizations of these derived classes, information which is crucial to the proofs of our main theorems. In Chapter V we bound the Selmer group over K by using the derived classes of Chapter IV and global duality. Bounding the Selmer group over K_∞ is similar but more difficult; this is accomplished in Chapter VII after a digression in Chapter VI which is used to reduce the proof to a simpler setting.

In Chapter VIII we discuss the conjectural connection between Euler systems and p-adic L-functions. This connection relies heavily on conjectures of Perrin-Riou [**PR4**]. Assuming a strong version of Perrin-Riou's conjectures, and subject to some hypotheses on the representation T, we show that there is an Euler system for T which is closely related to the p-adic L-function.

Chapter IX discusses possible variants of our definition of Euler systems.

Finally, there is some material which is used in the text, but which is outside our main themes. Rather than interrupt the exposition with this material, we include it in four appendices.

Notation. Equations are numbered consecutively within each chapter. Theorem 4.2 means the theorem numbered 4.2 in section 4 of the current chapter, while Lemma III.2.6 means Lemma 2.6 of Chapter III (and similarly for definitions, etc.). The chapters are numbered I through IX, and the appendices are A through D.

If F is a field, $\bar{F}$ will denote a fixed separable closure of F and $G_F = \mathrm{Gal}(\bar{F}/F)$. (All fields we deal with will be perfect, so we may as well assume that $\bar{F}$ is an algebraic closure of F.) Also F^{ab} will denote the maximal abelian extension of F, and if F is a local field F^{ur} will denote the maximal unramified extension of F. If F is a global field and Σ is a set of places of F, F_Σ will be the maximal extension of F which is unramified outside Σ. If $K \subset F$ is an extension of fields, we will write $K \subset_{\mathrm{f}} F$ to indicate that $[F : K]$ is finite.

If F is a field and B is a G_F-module, $F(B)$ will denote the fixed field of the kernel of the map $G_F \to \mathrm{Aut}(B)$, the smallest extension of F whose absolute Galois group acts trivially on B.

If $\mathcal{O}$ is a ring and B is an $\mathcal{O}$-module then $\mathrm{Ann}_{\mathcal{O}}(B) \subset \mathcal{O}$ will denote the annihilator of B in $\mathcal{O}$. If $M \in \mathcal{O}$ then B_M will denote the kernel of multiplication by M on B, and similarly if M is an ideal. If B is a free $\mathcal{O}$-module and τ is an $\mathcal{O}$-linear endomorphism of B, we will write

$$P(\tau|B;x) = \det(1-\tau x|B) \in \mathcal{O}[x],$$

the determinant of $1-\tau x$ acting on B.

The Galois module of n-th roots of unity will be denoted by $\boldsymbol{\mu}_n$.

If p is a fixed rational prime and F is a field of characteristic different from p, the cyclotomic character $\varepsilon_{\mathrm{cyc}} : G_F \to \mathbf{Z}_p^\times$ is the character giving the action of G_F on $\boldsymbol{\mu}_{p^\infty}$, and the Teichmüller character $\omega : G_F \to (\mathbf{Z}_p^\times)_{\mathrm{tors}}$ is the character giving the action of G_F on $\boldsymbol{\mu}_p$ (if p is odd) or $\boldsymbol{\mu}_4$ (if $p=2$). Hence ω has order at most $p-1$ or 2, respectively (with equality if $F=\mathbf{Q}$) and $\langle\varepsilon\rangle = \omega^{-1}\varepsilon_{\mathrm{cyc}}$ takes values in $1+p\mathbf{Z}_p$ (resp. $1+4\mathbf{Z}_2$).

If B is an abelian group, B_{div} will denote the maximal divisible subgroup of B. If p is a fixed rational prime, we define the p-adic completion of B to be the double dual

$$B\hat{} = \mathrm{Hom}(\mathrm{Hom}(B, \mathbf{Q}_p/\mathbf{Z}_p), \mathbf{Q}_p/\mathbf{Z}_p)$$

(where Hom always denotes continuous homomorphisms if the groups involved comes with topologies). For example, if B is a $\mathbf{Z}_p$-module then $B\hat{} = B$; if B is a finitely generated abelian group then $B\hat{} = B \otimes_{\mathbf{Z}} \mathbf{Z}_p$. In general $B\hat{}$ is a $\mathbf{Z}_p$ module and there is a canonical map from B to $B\hat{}$. If τ is an endomorphism of B then we will often write $B^{\tau=0}$ for the kernel of τ, $B^{\tau=1}$ for the subgroup fixed by τ, etc.

Most of these notations will be recalled when they first occur.

Acknowledgments. This book is an outgrowth of the Hermann Weyl lectures I gave at the Institute for Advanced Study in October, 1995. Some of the work and writing work was done while I was in residence at the Institute for Advanced Study and the Institut des Hautes Etudes Scientifiques. I would like to thank both the IAS and the IHES for their hospitality and financial support, and the NSF for additional financial support.

I am indebted to many people for numerous helpful conversations, especially Avner Ash, Ralph Greenberg, Barry Mazur, Bernadette Perrin-Riou, Alice Silverberg, and Warren Sinnott. I would also like to thank Tom Weston and Christophe Cornut for their careful reading of the manuscript and their comments, and the audiences of graduate courses I gave at Ohio State University and Stanford University for their patience as I was developing this material. Finally, special thanks go to Victor Kolyvagin and Francisco Thaine for their pioneering work.

CHAPTER I

Galois cohomology of p-adic representations

In this chapter we introduce our basic objects of study: p-adic Galois representations, their cohomology groups, and especially Selmer groups.

We begin by recalling basic facts about cohomology groups associated to p-adic representations, material which is mostly well-known but included here for completeness.

A Selmer group is a subgroup of a global cohomology group determined by "local conditions". In §3 we discuss these local conditions, special subgroups of the local cohomology groups. In §4 we state without proof the results we need concerning the Tate pairing on local cohomology groups, and we study how our special subgroups behave with respect to this pairing.

In §5 and §6 we define the Selmer group and give the basic examples of ideal class groups and Selmer groups of elliptic curves and abelian varieties. Then in §7, using our local orthogonality results from §4 and Poitou-Tate duality of global cohomology groups, we derive our main tool (Theorem 7.3) for bounding the size of Selmer groups.

1. p-adic representations

DEFINITION 1.1. Suppose K is a field, p is a rational prime, and $\mathcal{O}$ is the ring of integers of a finite extension Φ of $\mathbf{Q}_p$. A *p-adic representation* of $G_K = \mathrm{Gal}(\bar{K}/K)$, with coefficients in $\mathcal{O}$, is a free $\mathcal{O}$-module T of finite rank with a continuous, $\mathcal{O}$-linear action of G_K.

Let $\mathbf{D}$ denote the divisible module $\Phi/\mathcal{O}$. For a p-adic representation T, we also define

$$\begin{aligned} V &= T \otimes_{\mathcal{O}} \Phi, \\ W &= V/T = T \otimes_{\mathcal{O}} \mathbf{D}, \\ W_M &= M^{-1}T/T \subset W \quad \text{for } M \in \mathcal{O}, M \neq 0, \end{aligned}$$

so W_M is the M-torsion in W. Note that T determines V and W, and W determines $T = \varprojlim W_M$ and V, but in general there may be different $\mathcal{O}$-modules T giving rise to the same vector space V.

EXAMPLE 1.2. Suppose $\rho : G_K \to \mathcal{O}^\times$ is a character (continuous, but not necessarily of finite order). Then we can take $T = \mathcal{O}_\rho$, where $\mathcal{O}_\rho$ is a free, rank-one $\mathcal{O}$-module on which G_K acts via ρ. Clearly every one-dimensional representation arises in this way. When ρ is the trivial character we get $T \cong \mathcal{O}$, and when $\mathcal{O} = \mathbf{Z}_p$

and ρ is the cyclotomic character

$$\varepsilon_{\mathrm{cyc}} : G_K \to \mathrm{Aut}(\boldsymbol{\mu}_{p^\infty}) \xrightarrow{\sim} \mathbf{Z}_p^\times$$

we get

$$T \cong \mathbf{Z}_p(1) = \varprojlim_n \boldsymbol{\mu}_{p^n},$$
$$V \cong \mathbf{Q}_p(1) = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \varprojlim_n \boldsymbol{\mu}_{p^n},$$
$$W \cong (\mathbf{Q}_p/\mathbf{Z}_p)(1) = \boldsymbol{\mu}_{p^\infty}.$$

For general $\mathcal{O}$ we also write $\mathcal{O}(1) = \mathcal{O} \otimes \mathbf{Z}_p(1)$, $\Phi(1) = \Phi \otimes \mathbf{Q}_p(1)$, and $\mathbf{D}(1) = \mathbf{D} \otimes \mathbf{Z}_p(1)$.

Definition 1.3. If T is a p-adic representation of G_K then so is the dual representation

$$T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1)).$$

We will also write

$$V^* = \mathrm{Hom}_{\mathcal{O}}(V, \Phi(1)) = \mathrm{Hom}_{\mathcal{O}}(T, \Phi(1)) = T^* \otimes_{\mathcal{O}} \Phi,$$
$$W^* = V^*/T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathbf{D}(1)).$$

Example 1.4. If $\rho : G_K \to \mathcal{O}^\times$ is a continuous character as in Example 1.2 and $T = \mathcal{O}_\rho$, then $T^* = \mathcal{O}_{\rho^{-1}\varepsilon_{\mathrm{cyc}}}$.

Example 1.5. Suppose A is an abelian variety defined over K, and p is a prime different from the characteristic of K. Then we can take $\mathcal{O}$ to be $\mathbf{Z}_p$ and T to be the p-adic Tate module of A,

$$T_p(A) = \varprojlim_n A_{p^n}$$

where A_{p^n} denotes the p^n-torsion in $A(\bar{K})$, and we have $\mathrm{rank}_{\mathbf{Z}_p} T = 2\dim(A)$. If A and A' are isogenous, the corresponding Tate modules $T = T_p(A)$ and $T' = T_p(A')$ need not be isomorphic (as G_K-modules), but the corresponding vector spaces V and V' are isomorphic.

If the endomorphism algebra of A over K contains the ring of integers $\mathcal{O}_F$ of a number field F, and $\mathfrak{p}$ is a prime of F above p, we can also take $\Phi = F_{\mathfrak{p}}$, the completion of F at $\mathfrak{p}$, and

$$T = T_{\mathfrak{p}}(A) = \varprojlim_n A_{\mathfrak{p}^n}$$

which has rank $2\dim(A)/[F : \mathbf{Q}]$ over the ring of integers $\mathcal{O}$ of Φ. If A is an elliptic curve with complex multiplication by $F \subset K$, this is another source of important one-dimensional representations.

2. Galois cohomology

Suppose K is a field. If B is a commutative topological group with a continuous action of G_K, we have the continuous cohomology groups

$$H^i(K, B) = H^i(G_K, B),$$

and if the action of G_K factors through the Galois group $\mathrm{Gal}(K'/K)$ for some extension K' of K, we also write

$$H^i(K'/K, B) = H^i(\mathrm{Gal}(K'/K), B)$$

See Appendix B for the basic facts which we will need about continuous cohomology groups.

EXAMPLE 2.1. We have

$$H^1(K, \mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(G_K, \mathbf{Q}_p/\mathbf{Z}_p), \qquad H^1(K, \mathbf{Z}_p) = \mathrm{Hom}(G_K, \mathbf{Z}_p),$$

and by Kummer theory and Proposition B.2.3, respectively

$$\begin{aligned} H^1(K, \boldsymbol{\mu}_{p^\infty}) &= K^\times \otimes (\mathbf{Q}_p/\mathbf{Z}_p), \\ H^1(K, \mathbf{Z}_p(1)) &= \varprojlim_n H^1(K, \boldsymbol{\mu}_{p^n}) = \varprojlim_n K^\times/(K^\times)^{p^n} = K^\times \hat{\otimes} \mathbf{Z}_p, \end{aligned}$$

where $\hat{\otimes}$ denotes the (p-adically) completed tensor product.

Suppose T is a p-adic representation of G_K with coefficients in $\mathcal{O}$ as in §1, and $M \in \mathcal{O}$ is nonzero. Recall that $V = T \otimes \Phi$ and $W = V/T$. We will frequently make use of the following three exact sequences.

$$0 \longrightarrow W_M \longrightarrow W \xrightarrow{M} W \longrightarrow 0 \tag{1}$$

$$\begin{tikzcd} 0 \arrow[r] & T \arrow[r, "M"] \arrow[d, equal] & T \arrow[r, "M^{-1}"] \arrow[d, "M^{-1}"] & W_M \arrow[r] \arrow[d] & 0, \\ 0 \arrow[r] & T \arrow[r] & V \arrow[r] & W \arrow[r] & 0. \end{tikzcd} \tag{2}$$

LEMMA 2.2. *Suppose $M \in \mathcal{O}$ is nonzero.*

(i) *The sequence* (1) *induces an exact sequence*

$$0 \longrightarrow W^{G_K}/MW^{G_K} \longrightarrow H^1(K, W_M) \longrightarrow H^1(K, W)_M \longrightarrow 0.$$

(ii) *The bottom row of* (2) *induces an exact sequence*

$$V^{G_K} \longrightarrow W^{G_K} \longrightarrow H^1(K, T)_{\mathrm{tors}} \longrightarrow 0.$$

(iii) *The kernel of the map*

$$H^1(K, T) \longrightarrow H^1(K, W)$$

induced by $T \twoheadrightarrow T/MT \xrightarrow{\sim} W_M \hookrightarrow W$ is

$$MH^1(K, T) + H^1(K, T)_{\mathrm{tors}}.$$

PROOF. Assertions (i) and (ii) are clear, once we show that the kernel of the natural map $H^1(K, T) \to H^1(K, V)$ is $H^1(K, T)_{\mathrm{tors}}$. But this is immediate from Proposition B.2.4, which says that the map $H^1(K, T) \to H^1(K, V)$ induces an isomorphism $H^1(K, V) \cong H^1(K, T) \otimes \mathbf{Q}_p$.

The diagram (2) induces an exact commutative diagram

$$\begin{tikzcd} H^1(K,T) \arrow[r, "M"] \arrow[d, equal] & H^1(K,T) \arrow[r] \arrow[d, "\phi_1"] & H^1(K,W_M) \arrow[d] \\ H^1(K,T) \arrow[r, "\phi_2"] & H^1(K,V) \arrow[r, "\phi_3"] & H^1(K,W) \end{tikzcd}$$

with ϕ_1 induced by $M^{-1} : T \to V$. Since

$$\ker(\phi_3) = \phi_2(H^1(K,T)) = \phi_1(MH^1(K,T)),$$

we see that

$$\ker(\phi_3 \circ \phi_1) = MH^1(K,T) + \ker(\phi_1) = MH^1(K,T) + H^1(K,T)_{\text{tors}}$$

which proves (iii). □

3. Local cohomology groups

3.1. Unramified local cohomology. Suppose for this section that K is a finite extension of $\mathbf{Q}_\ell$ for some rational prime ℓ. Let $\mathcal{I}$ denote the inertia subgroup of G_K, let $K^{\text{ur}} = \bar{K}^{\mathcal{I}}$ be the maximal unramified extension of K, and let $\text{Fr} \in \text{Gal}(K^{\text{ur}}/K)$ denote the Frobenius automorphism.

Definition 3.1. Suppose B is a G_K-module. We say that B is unramified if $\mathcal{I}$ acts trivially on B. We define the subgroup of unramified cohomology classes $H^1_{\text{ur}}(K,B) \subset H^1(K,B)$ by

$$H^1_{\text{ur}}(K,B) = \ker(H^1(K,B) \to H^1(\mathcal{I},B)).$$

Note that if T is as in §1,

$$T \text{ is unramified} \Leftrightarrow V \text{ is unramified} \Leftrightarrow W \text{ is unramified}$$

and if the residue characteristic ℓ is different from p, then this is equivalent to T^*, V^*, and/or W^* being unramified.

Lemma 3.2. *Suppose B is a G_K module which is either a finitely generated $\mathbf{Z}_p$-module, or a finite dimensional $\mathbf{Q}_p$-vector space, or a discrete torsion $\mathbf{Z}_p$-module.*

(i) $H^1_{\text{ur}}(K,B) \cong H^1(K^{\text{ur}}/K, B^{\mathcal{I}}) \cong B^{\mathcal{I}}/(\text{Fr}-1)B^{\mathcal{I}}$.

(ii) *If the residue characteristic ℓ of K is different from p, then*

$$H^1(K,B)/H^1_{\text{ur}}(K,B) \cong H^1(\mathcal{I},B)^{\text{Fr}=1}.$$

Proof. The first isomorphism of (i) follows from the inflation-restriction exact sequence (Proposition B.2.5(i)). The second isomorphism of (i) (induced by the map on cocycles $c \mapsto c(\text{Fr})$) is Lemma B.2.8.

The hypotheses on B guarantee (see Propositions B.2.5(ii) and B.2.7) that we have a Hochschild-Serre spectral sequence

$$0 \longrightarrow H^1(K^{\text{ur}}/K, B^{\mathcal{I}}) \longrightarrow H^1(K,B) \longrightarrow H^1(\mathcal{I},B)^{\text{Fr}=1} \longrightarrow H^2(K^{\text{ur}}/K, B^{\mathcal{I}}).$$

Since $\text{Gal}(K^{\text{ur}}/K)$ has cohomological dimension one, $H^2(K^{\text{ur}}/K, B^{\mathcal{I}}) = 0$ so this proves (ii). □

COROLLARY 3.3. *Suppose $p \neq \ell$ and V is a $\mathbf{Q}_p[G_K]$-module which has finite dimension as a $\mathbf{Q}_p$-vector space.*

(i) $\dim_{\mathbf{Q}_p}(H^1_{\mathrm{ur}}(K,V)) = \dim_{\mathbf{Q}_p}(V^{G_K})$.

(ii) $\dim_{\mathbf{Q}_p}(H^1(K,V)/H^1_{\mathrm{ur}}(K,V)) = \dim_{\mathbf{Q}_p}(H^2(K,V))$.

PROOF. Using Lemma 3.2(i) we have an exact sequence

$$0 \longrightarrow V^{G_K} \longrightarrow V^{\mathcal{I}} \xrightarrow{\mathrm{Fr}-1} V^{\mathcal{I}} \longrightarrow H^1_{\mathrm{ur}}(K,V) \longrightarrow 0$$

which proves (i).

Since $p \neq \ell$, $\mathcal{I}$ has a unique maximal p-divisible subgroup $\mathcal{I}'$ and $\mathcal{I}/\mathcal{I}' \cong \mathbf{Z}_p$ (see [**Fr**] §8 Corollary 3). Thus both $\mathcal{I}$ and $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ have p-cohomological dimension one. It follows that

$$H^m(K^{\mathrm{ur}}/K, H^n(\mathcal{I},V)) = 0$$

if $m > 1$ or $n > 1$. Therefore the Hochschild-Serre spectral sequence (Propositions B.2.5(ii) and B.2.7) shows that

$$H^1(K^{\mathrm{ur}}/K, H^1(\mathcal{I},V)) = H^2(K,V).$$

On the other hand, Lemma 3.2 shows that

$$H^1(K^{\mathrm{ur}}/K, H^1(\mathcal{I},V)) \cong H^1(\mathcal{I},V)/(\mathrm{Fr}-1)H^1(\mathcal{I},V),$$
$$H^1(K,V)/H^1_{\mathrm{ur}}(K,V) \cong H^1(\mathcal{I},V)^{\mathrm{Fr}=1}$$

so there is an exact sequence

$$0 \longrightarrow H^1(K,V)/H^1_{\mathrm{ur}}(K,V) \longrightarrow H^1(\mathcal{I},V) \xrightarrow{\mathrm{Fr}-1} H^1(\mathcal{I},V) \longrightarrow H^2(K,V) \longrightarrow 0.$$

This proves (ii). □

3.2. Special subgroups. Suppose now that K is a finite extension of some $\mathbf{Q}_\ell$, but now we also allow $\ell = \infty$, i.e., $K = \mathbf{R}$ or $\mathbf{C}$. Let T be a p-adic representation of G_K, $V = T \otimes \Phi$ and $W = V/T$ as in §1. Following many authors (for example Bloch and Kato [**BK**] §3, Fontaine and Perrin-Riou [**FPR**] §I.3.3, or Greenberg [**Gr2**]) we define special subgroups $H^1_f(K,\,\cdot\,)$ of certain cohomology groups $H^1(K,\,\cdot\,)$. We assume first that $\ell \neq p, \infty$, and discuss the other cases in Remarks 3.6 and 3.7 below.

DEFINITION 3.4. Suppose $\ell \neq p$, $\ell \neq \infty$, and define the *finite* part of $H^1(K,V)$ by

$$H^1_f(K,V) = H^1_{\mathrm{ur}}(K,V).$$

Define $H^1_f(K,T) \subset H^1(K,T)$ and $H^1_f(K,W) \subset H^1(K,W)$ to be the inverse image and image, respectively, of $H^1_f(K,V)$ under the natural maps

$$H^1(K,T) \longrightarrow H^1(K,V) \longrightarrow H^1(K,W).$$

For every $M \in \mathcal{O}$ define $H^1_f(K,W_M) \subset H^1(K,W_M)$ to be the inverse image of $H^1_f(K,W)$ under the map induced by the inclusion $W_M \hookrightarrow W$.

Finally, for V, T, W, or W_M define the *singular* quotient of $H^1(K,\,\cdot\,)$ by

$$H^1_s(K,\,\cdot\,) = H^1(K,\,\cdot\,)/H^1_f(K,\,\cdot\,)$$

so there are exact sequences

$$0 \longrightarrow H^1_f(K,\,\cdot\,) \longrightarrow H^1(K,\,\cdot\,) \longrightarrow H^1_s(K,\,\cdot\,) \longrightarrow 0.$$

LEMMA 3.5. *Suppose T is as above and $\ell \neq p$, $\ell \neq \infty$. If A is a $\mathbf{Z}_p$-module let A_{div} denote its maximal divisible subgroup.*

(i) $H^1_f(K,W) = H^1_{\mathrm{ur}}(K,W)_{\mathrm{div}}$.

(ii) $H^1_{\mathrm{ur}}(K,T) \subset H^1_f(K,T)$ *with finite index and* $H^1_s(K,T)$ *is torsion-free.*

(iii) *Writing* $\mathcal{W} = W^{\mathcal{I}}/(W^{\mathcal{I}})_{\mathrm{div}}$, *there are natural isomorphisms*

$$H^1_{\mathrm{ur}}(K,W)/H^1_f(K,W) \xrightarrow{\sim} \mathcal{W}/(\mathrm{Fr}-1)\mathcal{W}$$

and

$$H^1_f(K,T)/H^1_{\mathrm{ur}}(K,T) \xrightarrow{\sim} \mathcal{W}^{\mathrm{Fr}=1}.$$

(iv) *If T is unramified then*

$$H^1_f(K,T) = H^1_{\mathrm{ur}}(K,T) \quad \textit{and} \quad H^1_f(K,W) = H^1_{\mathrm{ur}}(K,W).$$

PROOF. It is immediate from the definitions that $H^1_f(K,W)$ is divisible and $H^1_s(K,T)$ is torsion-free. The exact diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\mathrm{ur}}(K,T) & \longrightarrow & H^1(K,T) & \longrightarrow & H^1(\mathcal{I},T) \\
 & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_f(K,V) & \longrightarrow & H^1(K,V) & \longrightarrow & H^1(\mathcal{I},V) \\
 & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_{\mathrm{ur}}(K,W) & \longrightarrow & H^1(K,W) & \longrightarrow & H^1(\mathcal{I},W)
\end{array}$$

shows that $H^1_f(K,W) \subset H^1_{\mathrm{ur}}(K,W)$ and $H^1_{\mathrm{ur}}(K,T) \subset H^1_f(K,T)$. The rest of assertions (i) and (ii) will follow once we prove (iii), since $W^{\mathcal{I}}/(W^{\mathcal{I}})_{\mathrm{div}}$ is finite.

Note that the image of $V^{\mathcal{I}}$ in $W^{\mathcal{I}}$ is $(W^{\mathcal{I}})_{\mathrm{div}}$. Taking $\mathcal{I}$-cohomology and then $\mathrm{Gal}(K^{\mathrm{ur}}/K)$-invariants of the exact sequence $0 \to T \to V \to W \to 0$ gives an exact sequence

$$0 \longrightarrow (W^{\mathcal{I}}/(W^{\mathcal{I}})_{\mathrm{div}})^{\mathrm{Fr}=1} \longrightarrow H^1(\mathcal{I},T)^{\mathrm{Fr}=1} \longrightarrow H^1(\mathcal{I},V)^{\mathrm{Fr}=1}.$$

Therefore using Lemma 3.2 we have

$$\begin{aligned}
H^1_f(K,T)/H^1_{\mathrm{ur}}(K,T) &= \ker(H^1(K,T)/H^1_{\mathrm{ur}}(K,T) \to H^1(K,V)/H^1_{\mathrm{ur}}(K,V)) \\
&= \ker(H^1(\mathcal{I},T)^{\mathrm{Fr}=1} \to H^1(\mathcal{I},V)^{\mathrm{Fr}=1}) \\
&= (W^{\mathcal{I}}/(W^{\mathcal{I}})_{\mathrm{div}})^{\mathrm{Fr}=1}, \\
H^1_{\mathrm{ur}}(K,W)/H^1_f(K,W) &= \mathrm{coker}(H^1_{\mathrm{ur}}(K,V) \to H^1_{\mathrm{ur}}(K,W)) \\
&= \mathrm{coker}(V^{\mathcal{I}}/(\mathrm{Fr}-1)V^{\mathcal{I}} \to W^{\mathcal{I}}/(\mathrm{Fr}-1)W^{\mathcal{I}}) \\
&= W^{\mathcal{I}}/((W^{\mathcal{I}})_{\mathrm{div}} + (\mathrm{Fr}-1)W^{\mathcal{I}}).
\end{aligned}$$

This proves (iii).

If T is unramified then $W^{\mathcal{I}} = W$ is divisible, so (iv) is immediate from (iii). $\square$

REMARK 3.6. When the residue characteristic ℓ is equal to p, the choice of a subspace $H^1_f(K,V)$ is much more subtle. Fortunately, for the purpose of working with Euler systems it is not essential to make such a choice. However, to understand fully the arithmetic significance of the Selmer groups we will define in §5, and to get the most out of the applications of Euler systems in Chapter III, it is necessary to choose a subspace $H^1_f(K,V)$ in the more difficult case $\ell = p$.

In this case, Bloch and Kato define $H^1_f(K,V)$ using the ring B_{cris} defined by Fontaine ([**BK**] §3). Namely, they define

$$H^1_f(K,V) = \ker\left(H^1(K,V) \to H^1(K, V \otimes B_{\mathrm{cris}})\right).$$

For our purposes we will allow an *arbitrary* special subspace of $H^1(K,V)$, which we will still denote by $H^1_f(K,V)$. This notation is not as bad as it may seem: in our applications we will always choose a subspace $H^1_f(K,V)$ which is the same as the one defined by Bloch and Kato, but we need not (and will not) prove they are the same. One could also choose, for example, $H^1_f(K,V) = 0$ or $H^1_f(K,V) = H^1(K,V)$.

Once $H^1_f(K,V)$ is chosen, we define $H^1_f(K,T)$, $H^1_f(K,W)$, and $H^1_f(K,W_M)$ in terms of $H^1_f(K,V)$ exactly as in Definition 3.4.

REMARK 3.7. If $K = \mathbf{R}$ or $\mathbf{C}$ then $H^1(K,V) = 0$, so $H^1_f(K,V) = 0$ and proceeding as above we are led to define

$$\begin{aligned} H^1_f(K,W) &= 0, \\ H^1_f(K,T) &= H^1(K,T), \\ H^1_f(K,W_M) &= \ker(H^1(K,W_M) \to H^1(K,W)) = W^{G_K}/MW^{G_K}. \end{aligned}$$

Note that all of these groups are zero unless $K = \mathbf{R}$ and $p = 2$.

LEMMA 3.8. *Suppose $M \in \mathcal{O}$ is nonzero.*

(i) *$H^1_f(K,W_M)$ is the image of $H^1_f(K,T)$ under the map*

$$H^1(K,T) \longrightarrow H^1(K,W_M)$$

induced by $T \twoheadrightarrow M^{-1}T/T = W_M$.

(ii) *If $\ell \neq p,\infty$ and T is unramified then $H^1_f(K,W_M) = H^1_{\mathrm{ur}}(K,W_M)$.*

PROOF. The diagram (2) gives rise to a commutative diagram with exact rows

$$\begin{tikzcd} H^1(K,T) \arrow[r, "M"] \arrow[d, equal] & H^1(K,T) \arrow[r] \arrow[d, "M^{-1}"] & H^1(K,W_M) \arrow[r] \arrow[d] & H^2(K,T) \arrow[d, equal] \\ H^1(K,T) \arrow[r] & H^1(K,V) \arrow[r] & H^1(K,W) \arrow[r] & H^2(K,T). \end{tikzcd} \tag{3}$$

It is immediate from this diagram and the definitions that the image of $H^1_f(K,T)$ is contained in $H^1_f(K,W_M)$.

Suppose $c_{W_M} \in H^1_f(K,W_M)$. Then the image of c_{W_M} in $H^1(K,W)$ is the image of some $c_V \in H^1_f(K,V)$. Thus (3) shows that c_{W_M} is the image of some $c_T \in H^1(K,T)$, and the image of c_T in $H^1(K,V)$ differs from c_V by an element c' of $H^1(K,T)$. Therefore $c_T - Mc' \in H^1_f(K,T)$ and $c_T - Mc'$ maps to c_{W_M}. This shows that $H^1_f(K,W_M)$ is contained in the image of $H^1_f(K,T)$, and completes the proof of (i).

If $\ell \neq p$ and T is unramified then

$$H^1_f(K, W_M) = \mathrm{image}(H^1_f(K,T)) = \mathrm{image}(H^1_{\mathrm{ur}}(K,T)) \subset H^1_{\mathrm{ur}}(K, W_M)$$

by (i) and Lemma 3.5(iv). Similarly if ι_M is the map $H^1(K, W_M) \to H^1(K, W)$ then Lemma 3.5(iv) shows that

$$H^1_f(K, W_M) = \iota_M^{-1}(H^1_f(K,W)) = \iota_M^{-1}(H^1_{\mathrm{ur}}(K,W)) \supset H^1_{\mathrm{ur}}(K, W_M)$$

which proves (ii). □

REMARK 3.9. We can view W_M either as a subgroup of W or as a quotient of T. Lemma 3.8(i) says that it makes no difference whether we define $H^1_f(K, W_M)$ as the inverse image of $H^1_f(K, W)$ (as we did) or as image of $H^1_f(K,T)$.

COROLLARY 3.10. *There are natural horizontal exact sequences and vertical isomorphisms*

$$\begin{array}{ccccccccc}
0 & \to & H^1_f(K,W) & \longrightarrow & H^1(K,W) & \longrightarrow & H^1_s(K,W) & \to & 0 \\
 & & \| & & \| & & \| & & \\
0 & \to & \varinjlim_M H^1_f(K,W_M) & \longrightarrow & \varinjlim_M H^1(K,W_M) & \longrightarrow & \varinjlim_M H^1_s(K,W_M) & \to & 0 \\
 & & & & & & & & \\
0 & \to & H^1_f(K,T) & \longrightarrow & H^1(K,T) & \longrightarrow & H^1_s(K,T) & \to & 0 \\
 & & \| & & \| & & \| & & \\
0 & \to & \varprojlim_M H^1_f(K,W_M) & \longrightarrow & \varprojlim_M H^1(K,W_M) & \longrightarrow & \varprojlim_M H^1_s(K,W_M) & \to & 0
\end{array}$$

PROOF. The groups inside the inverse limits are finite (Proposition B.2.7(ii)), so the horizontal exact sequences are clear.

The isomorphism $H^1(K,W) = \varinjlim H^1(K,W_M)$ is a basic fact from Galois cohomology, and the isomorphism $H^1_f(K,W) = \varinjlim H^1_f(K,W_M)$ follows immediately from the definition of $H^1_f(K,W_M)$. The isomorphism $H^1_s(K,W) = \varinjlim H^1_s(K,W_M)$ now follows.

The second set of isomorphisms is similar, except that to handle the inverse limits we use Proposition B.2.3 for the center and Lemma 3.8(i) for the right. □

4. Local duality

Suppose that either K is a finite extension of $\mathbf{Q}_\ell$ for some rational prime ℓ or $K = \mathbf{R}$ or $\mathbf{C}$, and T is a p-adic representation of G_K.

THEOREM 4.1 (Local duality). *Suppose that either K is nonarchimedean and $i = 0, 1, 2$, or K is archimedean and $i = 1$. Then the cup product and the local invariant map induce perfect pairings*

$$\begin{array}{ccccccc}
H^i(K,V) & \times & H^{2-i}(K,V^*) & \to & H^2(K,\Phi(1)) & \xrightarrow{\sim} & \Phi \\
H^i(K,W_M) & \times & H^{2-i}(K,W_M^*) & \to & H^2(K,\mathcal{O}(1)/M\mathcal{O}(1)) & \xrightarrow{\sim} & \mathcal{O}/M\mathcal{O} \\
H^i(K,T) & \times & H^{2-i}(K,W^*) & \to & H^2(K,\mathbf{D}(1)) & \xrightarrow{\sim} & \mathbf{D}.
\end{array}$$

PROOF. See for example [**Mi**] Corollary I.2.3 or [**Se2**] §II.5.2 (and use Propositions B.2.3 and B.2.4). □

Without fear of confusion, we will denote all of the pairings of Theorem 4.1 by $\langle\ ,\ \rangle_K$.

PROPOSITION 4.2. *Suppose either K is archimedean, or K is nonarchimedean of residue characteristic $\ell \neq p$. Then $H^1_f(K,V)$ and $H^1_f(K,V^*)$ are orthogonal complements of each other under the pairing $\langle\ ,\ \rangle_K$.*

PROOF. If K is archimedean then all the groups are zero, so there is nothing to prove.

Suppose that K is nonarchimedean of residue characteristic $\ell \neq p$. The pairing

$$\langle\ ,\ \rangle_K : H^1_f(K,V) \times H^1_f(K,V^*) \to \Phi$$

factors through $H^2(K^{\mathrm{ur}}/K, \Phi(1))$, which is 0 since $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ has cohomological dimension 1. Thus $H^1_f(K,V)$ and $H^1_f(K,V^*)$ are orthogonal. Further, Corollary 3.3(i), local duality (Theorem 4.1), and Corollary 3.3(ii), respectively, give the three equalities

$$\begin{aligned}\dim_\Phi(H^1_f(K,V^*)) = \dim_\Phi(H^0(K,V^*)) &= \dim_\Phi(H^2(K,V)) \\ &= \dim_\Phi(H^1(K,V)) - \dim_\Phi(H^1_f(K,V)),\end{aligned}$$

so $H^1_f(K,V)$ and $H^1_f(K,V^*)$ are exact orthogonal complements. □

PROPOSITION 4.3. *Suppose either*

(a) *K is archimedean,*
(b) *K is nonarchimedean of residue characteristic $\ell \neq p$, or*
(c) *K is nonarchimedean of residue characteristic $\ell = p$ and we choose subspaces $H^1_f(K,V)$ and $H^1_f(K,V^*)$ which are orthogonal complements of each other under the pairing $\langle\ ,\ \rangle_K$.*

Then under the pairings $\langle\ ,\ \rangle_K$,

(i) *$H^1_f(K,T)$ and $H^1_f(K,W^*)$ are orthogonal complements of each other,*
(ii) *for every nonzero M in $\mathcal{O}$, $H^1_f(K,W_M)$ and $H^1_f(K,W^*_M)$ are orthogonal complements of each other.*

PROOF. The definition of the local pairings in terms of cup products shows that the diagram

$$\begin{array}{ccccc} H^1(K,V) & \times & H^1(K,V^*) & \longrightarrow & \Phi \\ {\scriptstyle\phi}\uparrow & & \downarrow{\scriptstyle\phi^*} & & \downarrow \\ H^1(K,T) & \times & H^1(K,W^*) & \longrightarrow & \mathbf{D}. \end{array}$$

"commutes", in the sense that if $c \in H^1(K,T)$ and $d \in H^1(K,V^*)$, then

$$\langle \phi(c), d\rangle_K = \langle c, \phi^*(d)\rangle_K \in \mathbf{D}.$$

By Proposition 4.2, $H^1_f(K,V)$ and $H^1_f(K,V^*)$ are orthogonal complements of each other in all cases. Thus if we write $\cdot^\perp$ to denote the orthogonal complement, then since $H^1_f(K, W^*) = \phi^*(H^1_f(K, V^*))$,

$$H^1_f(K, W^*)^\perp = \phi^{-1}(H^1_f(K, V^*)^\perp) = \phi^{-1}(H^1_f(K, V)) = H^1_f(K, T).$$

This proves (i), and the proof of (ii) is similar, using (i), the diagram

$$\begin{array}{ccccc} H^1(K,T) & \times & H^1(K,W^*) & \longrightarrow & \mathbf{D} \\ \downarrow & & \uparrow & & \uparrow \\ H^1(K,W_M) & \times & H^1(K,W_M^*) & \longrightarrow & \mathcal{O}/M\mathcal{O} \end{array}$$

and Lemma 3.8(i). □

Definition 4.4. If the residue characteristic ℓ of K is different from p, then there is an exact sequence

$$0 \longrightarrow \mathcal{I}' \longrightarrow \mathcal{I} \longrightarrow \mathbf{Z}_p \longrightarrow 0$$

where $\mathcal{I}'$ has trivial pro-p-part (see **[Fr]** §8 Corollary 3). It follows that if M is a power of p then $\mathcal{I}$ has a unique subgroup of index M (the inverse image of $M\mathbf{Z}_p$), and by slight abuse of notation we denote this subgroup by $\mathcal{I}^M$.

There is a natural action of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ on the cyclic group $\mathcal{I}/\mathcal{I}^M$. The next lemma is essentially Exercice 2, §IV.2 of **[Se3]**.

Lemma 4.5. *Suppose $\ell \neq p$ and M is a power of p. Then there is a canonical isomorphism of* $\mathrm{Gal}(K^{\mathrm{ur}}/K)$*-modules*

$$\mathcal{I}/\mathcal{I}^M \xrightarrow{\sim} \boldsymbol{\mu}_M.$$

Proof. We have isomorphisms

$$\mathrm{Hom}(\mathcal{I}/\mathcal{I}^M, \boldsymbol{\mu}_M) = \mathrm{Hom}(\mathcal{I}, \boldsymbol{\mu}_M) \xrightarrow{\sim} (K^{\mathrm{ur}})^\times/((K^{\mathrm{ur}})^\times)^M \xrightarrow{\sim} \mathbf{Z}/M\mathbf{Z},$$

given by Kummer theory and (on the right) by the valuation map (the unit group of the ring of integers of K^{ur} is p-divisible). The inverse image of 1 under this composition is the desired isomorphism.

More concretely, the isomorphism is given by

$$\sigma \mapsto (\lambda^{1/M})^\sigma/(\lambda^{1/M})$$

where λ is any uniformizing parameter of K. □

Definition 4.6. If $M \in \mathcal{O}$ is nonzero, we let $\bar{M} \in \mathbf{Z}^+$ denote the smallest power of p which is divisible by M.

Lemma 4.7. *Suppose the residue characteristic ℓ is different from p, T is unramified, $M \in \mathcal{O}$ is nonzero, and $\boldsymbol{\mu}_{\bar{M}} \subset K$. Fix a generator ζ of $\boldsymbol{\mu}_{\bar{M}}$ and let $\sigma_\zeta \in \mathcal{I}/\mathcal{I}^{\bar{M}}$ be the inverse image of ζ under the isomorphism of Lemma* 4.5.

(i) *Evaluating cocycles on* Fr *and σ_ζ induces isomorphisms*

$$H^1_f(K, W_M) \xrightarrow{\sim} W_M/(\mathrm{Fr}-1)W_M, \quad H^1_s(K, W_M) \xrightarrow{\sim} W_M^{\mathrm{Fr}=1},$$

respectively.

(ii) *With an appropriate choice of sign on the right, the diagram*

$$\begin{array}{ccccc} H^1_f(K,W_M^*) & \times & H^1_s(K,W_M) & \longrightarrow & \mathcal{O}/M\mathcal{O} \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \pm 1\otimes\zeta} \\ W_M^*/(\mathrm{Fr}-1)W_M^* & \times & (W_M)^{\mathrm{Fr}=1} & \longrightarrow & \mathcal{O}(1)/M\mathcal{O}(1) \end{array}$$

commutes, where the first two vertical maps are the isomorphisms of (i), the upper pairing is the paring of Theorem 4.1 *and the lower pairing is the natural one.*

Proof. The first assertion of (i) is just a restatement of Lemma 3.2(i), since by Lemma 3.8(ii), $H^1_f(K,W_M) = H^1_{\mathrm{ur}}(K,W_M)$. Similarly, Lemma 3.2(ii) shows that

$$H^1_s(K,W_M) = H^1(K,W_M)/H^1_{\mathrm{ur}}(K,W_M) \cong H^1(\mathcal{I},W_M)^{\mathrm{Fr}=1}.$$

Lemma 4.5 shows that $\mathcal{I}/\mathcal{I}^{\bar{M}} \cong \boldsymbol{\mu}_{\bar{M}}$, and we have assumed that G_K acts trivially on $\boldsymbol{\mu}_{\bar{M}}$, so we conclude that

$$H^1_s(K,W_M) \cong \mathrm{Hom}(\mathcal{I}/\mathcal{I}^{\bar{M}},W_M)^{\mathrm{Fr}=1} \cong \mathrm{Hom}(\boldsymbol{\mu}_{\bar{M}},W_M^{\mathrm{Fr}=1}).$$

Our choice of generator of $\boldsymbol{\mu}_{\bar{M}}$ now completes the proof of (i).

Assertion (ii) can be extracted Chapter I of [**Mi**], especially Proposition 0.14, Examples 0.8 and 1.6, and Theorem 2.6. □

5. Global cohomology groups

Suppose for this section that K is a number field, T is a p-adic representation of G_K, and V and W are defined in terms of T as in §1. We assume in addition that T is unramified outside a finite set of primes of K. (As usual, we say that T is unramified at a place v if the inertia group of v acts trivially on T.) We write K_v for the completion of K at a place v, and for all primes v dividing p we fix a subspace $H^1_f(K_v,V)$ of $H^1(K_v,V)$.

For every place v of K there is a canonical restriction map $H^1(K,\cdot) \to H^1(K_v,\cdot)$, which we will denote either by $c \mapsto \mathrm{res}_v(c)$ or simply $c \mapsto c_v$.

If Σ is a finite set of places of K we write K_Σ for the maximal extension of K unramified outside Σ.

Definition 5.1. Suppose Σ is a finite set of places of K. We define some *Selmer groups* corresponding to Σ as follows. Recall that

$$H^1_s(K_v,W) = H^1(K_v,W)/H^1_f(K_v,W).$$

First, define

$$\mathcal{S}_\Sigma(K,W) \subset \mathcal{S}^\Sigma(K,W) \subset H^1(K,W)$$

by

$$\mathcal{S}^\Sigma(K,W) = \ker\Big(H^1(K,W) \to \bigoplus_{v\notin\Sigma} H^1_s(K_v,W)\Big),$$

$$\mathcal{S}_\Sigma(K,W) = \ker\Big(\mathcal{S}^\Sigma(K,W) \to \bigoplus_{v\in\Sigma} H^1(K_v,W)\Big)$$

(Note that $c \in H^1(K,W)$ restricts to zero in all but finitely many $H^1_s(K_v,W)$ because T is ramified at only finitely many primes.) In other words, $\mathcal{S}^\Sigma(K,W)$ consists of all classes $c \in H^1(K,W)$ satisfying the local conditions

- $c_v \in H^1_f(K_v,W)$ if $v \notin \Sigma$,
- no restriction for $v \in \Sigma$,

and $\mathcal{S}_\Sigma(K,W)$ has the additional restrictions

- $c_v = 0$ if $v \in \Sigma$.

When $\Sigma = \emptyset$ is the empty set we write

$$\mathcal{S}(K,W) = \mathcal{S}^\emptyset(K,W) = \mathcal{S}_\emptyset(K,W).$$

Similarly, we define $\mathcal{S}_\Sigma(K,T) \subset \mathcal{S}^\Sigma(K,T) \subset H^1(K,T)$ by

$$\mathcal{S}^\Sigma(K,T) = \ker\Big(H^1(K,T) \to \prod_{v \notin \Sigma} H^1_s(K_v,T)\Big),$$
$$\mathcal{S}_\Sigma(K,T) = \ker\Big(\mathcal{S}^\Sigma(K,T) \to \bigoplus_{v \in \Sigma} H^1(K_v,T)\Big)$$

and likewise for $\mathcal{S}_\Sigma(K,W_M) \subset \mathcal{S}^\Sigma(K,W_M) \subset H^1(K,W_M)$ for every nonzero M in $\mathcal{O}$.

REMARK 5.2. If Σ contains all primes above p, then the Selmer groups $\mathcal{S}^\Sigma$ and $\mathcal{S}_\Sigma$ are independent of the choice of subspaces $H^1_f(K_v,V)$ for v dividing p.

LEMMA 5.3. *Suppose Σ contains all infinite places, all primes above p, and all primes of K where T is ramified. If $A = T$, W, or W_M with $M \in \mathcal{O}$, then*

$$\mathcal{S}^\Sigma(K,A) = H^1(K_\Sigma/K,A).$$

PROOF. By Lemmas 3.5(iv) and 3.8(ii), $H^1_f(K_v,A) = H^1_{\mathrm{ur}}(K_v,A)$ for $v \notin \Sigma$, so (writing $\mathcal{I}_v$ for an inertia group above v)

$$\begin{aligned}\mathcal{S}^\Sigma(K,A) &= \ker\Big(H^1(K,A) \to \prod_{v \notin \Sigma} \mathrm{Hom}(\mathcal{I}_v,A)\Big)\\ &= \ker\Big(H^1(K,A) \to H^1(K_\Sigma,A)\Big) = H^1(K_\Sigma/K,A).\end{aligned}$$ □

LEMMA 5.4. *If $M \in \mathcal{O}$ is nonzero and Σ is a finite set of primes of K, then the natural map $\iota_M : H^1(K,W_M) \to H^1(K,W)$ induces a surjection*

$$\mathcal{S}^\Sigma(K,W_M) \twoheadrightarrow \mathcal{S}^\Sigma(K,W)_M$$

PROOF. By Lemma 2.2(i), $\iota_M(H^1(K,W_M)) = H^1(K,W)_M$. From the definition of $H^1_f(K_v,W_M)$ it is clear that $\iota_M^{-1}(\mathcal{S}^\Sigma(K,W)_M) = \mathcal{S}^\Sigma(K,W_M)$. This proves the lemma. □

REMARK 5.5. Lemma 5.4 need *not* be true if we replace $\mathcal{S}^\Sigma$ by $\mathcal{S}_\Sigma$, because it may not be the case that $\iota_M^{-1}(\mathcal{S}_\Sigma(K,W)_M) \subset \mathcal{S}_\Sigma(K,W_M)$.

PROPOSITION 5.6. *Suppose Σ is a finite set of primes of K.*

(i) $\mathcal{S}^\Sigma(K,T) = \varprojlim_M \mathcal{S}^\Sigma(K,W_M)$ *and* $\mathcal{S}_\Sigma(K,T) = \varprojlim_M \mathcal{S}_\Sigma(K,W_M)$,

(ii) $\mathcal{S}^\Sigma(K,W) = \varinjlim_M \mathcal{S}^\Sigma(K,W_M)$ *and* $\mathcal{S}_\Sigma(K,W) = \varinjlim_M \mathcal{S}_\Sigma(K,W_M)$.

PROOF. We have $H^1(K,W) = \varinjlim H^1(K,W_M)$, and by Proposition B.2.3, $H^1(K,T) = \varprojlim H^1(K,W_M)$. Corollary 3.10 shows that all the local conditions behave well under inverse and direct limits, and the proposition follows. □

LEMMA 5.7. *Suppose $M \in \mathcal{O}$ is nonzero and Σ is a finite set of primes of K.*

(i) *$\mathcal{S}^\Sigma(K,W_M)$ is finite.*
(ii) *$\mathcal{S}^\Sigma(K,T)$ is a finitely-generated $\mathcal{O}$-module.*
(iii) *The Pontryagin dual of $\mathcal{S}^\Sigma(K,W)$ is a finitely-generated $\mathcal{O}$-module.*

PROOF. Without loss of generality we may enlarge Σ if necessary so that Σ contains all infinite places, all primes above p, and all primes where T is ramified. Then by Lemma 5.3, if A is W_M, T, or W we have $\mathcal{S}^\Sigma(K,A) = H^1(K_\Sigma/K,A)$. As is well known (see Proposition B.2.7) these groups have the desired properties. □

6. Examples of Selmer groups

Again for this section K will denote a number field.

6.1. Ideal class groups I. Suppose $\mathcal{O} = \mathbf{Z}_p$ and $T = \mathbf{Z}_p$ with trivial G_K-action. For every prime v of K not dividing p, Lemma 3.5(iv) shows that

$$H^1_f(K_v,\mathbf{Q}_p/\mathbf{Z}_p) = H^1_{\mathrm{ur}}(K_v,\mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v),\mathbf{Q}_p/\mathbf{Z}_p).$$

If Σ is a set of places of K containing all primes above p, it follows easily that

$$\begin{aligned} H^1(K,\mathbf{Q}_p/\mathbf{Z}_p) &= \mathrm{Hom}(G_K,\mathbf{Q}_p/\mathbf{Z}_p),\\ \mathcal{S}^\Sigma(K,\mathbf{Q}_p/\mathbf{Z}_p) &= \mathrm{Hom}(\mathrm{Gal}(K_\Sigma/K),\mathbf{Q}_p/\mathbf{Z}_p),\\ \mathcal{S}_\Sigma(K,\mathbf{Q}_p/\mathbf{Z}_p) &= \mathrm{Hom}(\mathrm{Gal}(H_{K,\Sigma}/K),\mathbf{Q}_p/\mathbf{Z}_p)\end{aligned}$$

where $H_{K,\Sigma}$ is the maximal everywhere-unramified abelian extension of K in which all places in Σ split completely. Thus by class field theory, writing $A_{K,\Sigma}$ for the quotient of the ideal class group of K by the subgroup generated by the classes of primes in Σ,

$$\mathcal{S}_\Sigma(K,\mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(A_{K,\Sigma},\mathbf{Q}_p/\mathbf{Z}_p).$$

With an appropriate choice of $H^1_f(K_v,\mathbf{Q}_p)$ for primes v dividing p, Proposition 6.1 below will show that

$$\mathcal{S}(K,\mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(A_K,\mathbf{Q}_p/\mathbf{Z}_p) \tag{4}$$

where A_K is the ideal class group of K.

6.2. Ideal class groups II. More generally, suppose that $\chi : G_K \to \mathcal{O}^\times$ is a character of finite, prime-to-p, order, and let $T = \mathcal{O}_\chi$, a free rank-one $\mathcal{O}$-module with G_K acting via χ. Let L be an abelian extension of K of degree prime to p such that χ factors through $\Delta = \mathrm{Gal}(L/K)$. Write $\mathbf{D}_\chi = \mathbf{D} \otimes \mathcal{O}_\chi$ and $\Phi_\chi = \Phi \otimes \mathcal{O}_\chi$.

Suppose v is a place of K, and if w is a place of L above v let D_w and $\mathcal{I}_w$ denote a decomposition group and inertia group of w, respectively, in G_K. The restriction map gives isomorphisms (Corollary B.5.3(ii))

$$H^1(K_v,V) \cong (\oplus_{w|v}\mathrm{Hom}(D_w,V))^\Delta = (\oplus_{w|v}\mathrm{Hom}(D_w,\Phi_\chi))^\Delta \tag{5}$$

and if $v \nmid p$ this identifies

$$H^1_f(K_v,V) = H^1_{\mathrm{ur}}(K_v,V) = (\oplus_{w|v}\mathrm{Hom}(D_w/\mathcal{I}_w,V))^{\Delta} \tag{6}$$

If $v \mid p$ we take (6) as the definition of $H^1_f(K_v,V)$ as well; this agrees with the Bloch-Kato definition of H^1_f in this case.

Let A_L denote the ideal class group of L. When $L=K$ the following proposition reduces to (4).

PROPOSITION 6.1. $\mathcal{S}(K,W) \cong \mathrm{Hom}(A_L,\mathbf{D}_\chi)^\Delta$.

PROOF. Since $[L:K]$ is prime to p, the restriction map

$$H^1(K,W) \longrightarrow H^1(L,W)^\Delta = \mathrm{Hom}(G_L,\mathbf{D}_\chi)^\Delta$$

is an isomorphism. Exactly as in (5) and (6), for every v

$$\begin{array}{ccc} H^1(K_v,W) & \xrightarrow{\sim} & (\oplus_{w|v}\mathrm{Hom}(D_w,W))^\Delta \\ \cup & & \cup \\ H^1_f(K_v,W) & \xrightarrow{\sim} & (\oplus_{w|v}(\mathrm{Hom}(D_w/\mathcal{I}_w,W))^\Delta)_{\mathrm{div}}. \end{array}$$

Since each $D_w/\mathcal{I}_w$ is torsion-free, $\oplus_{w|v}\mathrm{Hom}(D_w/\mathcal{I}_w,W)$ is divisible. Since Δ has order prime to p,

$$(\oplus_{w|v}\mathrm{Hom}(D_w/\mathcal{I}_w,W))^\Delta = \Big(|\Delta|^{-1}\sum_{\delta\in\Delta}\delta\Big)(\oplus_{w|v}\mathrm{Hom}(D_w/\mathcal{I}_w,W))$$

is divisible and so $H^1_f(K_v,W) = (\oplus_{w|v}\mathrm{Hom}(D_w/\mathcal{I}_w,W))^\Delta$. Therefore, if H_L is the Hilbert class field of L,

$$\begin{aligned} \mathcal{S}(K,W) &\cong \{\phi \in \mathrm{Hom}(G_L,\mathbf{D}_\chi)^\Delta : \phi(\mathcal{I}_w)=0 \text{ for every } w\} \\ &= \mathrm{Hom}(\mathrm{Gal}(H_L/L),\mathbf{D}_\chi)^\Delta = \mathrm{Hom}(A_L,\mathbf{D}_\chi)^\Delta. \end{aligned}$$ □

6.3. Global units and ideal class groups. Let χ, $T=\mathcal{O}_\chi$, L, A_L, and $\Delta=\mathrm{Gal}(L/K)$ be as in §6.2. Then $T^* = \mathcal{O}_{\chi^{-1}\varepsilon_{\mathrm{cyc}}}$, i.e., T^* is a free rank-one $\mathcal{O}$ module on which G_K acts via $\chi^{-1}\varepsilon_{\mathrm{cyc}}$, where $\varepsilon_{\mathrm{cyc}}$ denotes the cyclotomic character. In particular G_L acts on T^* by the cyclotomic character.

DEFINITION 6.2. Suppose B is a $\mathbf{Z}[\Delta]$-module. We define the *p-adic completion* of B to be the double dual

$$B\hat{} = \mathrm{Hom}(\mathrm{Hom}(B,\mathbf{Q}_p/\mathbf{Z}_p),\mathbf{Q}_p/\mathbf{Z}_p)$$

(with continuous homomorphisms, when B comes with a topology). For example, if B is a $\mathbf{Z}_p$-module then $B\hat{} = B$; if B is a finitely generated abelian group then $B\hat{} = B\otimes_{\mathbf{Z}}\mathbf{Z}_p$. In general $B\hat{}$ is a $\mathbf{Z}_p$ module and there is a canonical map from B to $B\hat{}$.

Define the *χ-component* of B

$$B^\chi = \{b \in B\hat{}\otimes_{\mathbf{Z}_p}\mathcal{O} : \gamma b = \chi(\gamma)b \text{ for every } \gamma\in\Delta\}$$

We fix once and for all an $\mathcal{O}$-generator of $\mathcal{O}_{\chi^{-1}}$, and with this choice we get an isomorphism

$$B^\chi = (B\hat{}\otimes\mathcal{O}_{\chi^{-1}})^\Delta.$$

Since $[L:K]$ is prime to p, taking χ-components is an exact functor and

$$B^{\hat{}} \otimes_{\mathbf{Z}_p} \mathcal{O} = \oplus_\chi B^\chi.$$

Suppose v is a place of K, and let $U_{L,v}$ denote the local units of $L \otimes K_v = \prod_{w|v} L_w$. (That is, $U_{L,v} = \prod_{w|v} \mathcal{O}_w^\times$ where $\mathcal{O}_w$ is the ring of integers of L_w.) The restriction map (Corollary B.5.3(ii)) and Kummer theory (Example 2.1) give isomorphisms

$$\begin{aligned} H^1(K_v, V^*) &\cong (\oplus_{w|v} H^1(L_w, V^*))^\Delta \\ &= (\oplus_{w|v} H^1(L_w, \mathbf{Q}_p(1)) \otimes \Phi_{\chi^{-1}})^\Delta \cong ((L \otimes K_v)^\times)^\chi \otimes \Phi. \end{aligned}$$

If $v \nmid p$ then with this identification one can check that

$$\begin{array}{ccc} H^1(K_v, V^*) & \xrightarrow{\sim} & ((L \otimes K_v)^\times)^\chi \otimes \Phi \\ \cup & & \cup \\ H^1_f(K_v, V^*) & \xrightarrow{\sim} & U^\chi_{L,v} \otimes \Phi. \end{array} \tag{7}$$

If $v \mid p$ we take the bottom row of (7) as the definition of $H^1_f(K_v, V^*)$ as well; this agrees with the Bloch-Kato definition of H^1_f in this case. Combining (5) and (6) with the identifications

$$\oplus_{w|v} D_w \cong (L \otimes K_v)^\times, \qquad \oplus_{w|v} \mathcal{I}_w \cong U_{L,v}$$

of local class field theory gives a similar diagram

$$\begin{array}{ccc} H^1(K_v, V) & \xrightarrow{\sim} & \mathrm{Hom}(((L \otimes K_v)^\times)^\chi, \Phi) \\ \cup & & \cup \\ H^1_f(K_v, V) & \xrightarrow{\sim} & \mathrm{Hom}(((L \otimes K_v)^\times)^\chi / U^\chi_{L,v}, \Phi). \end{array} \tag{8}$$

The local pairing $\langle\ ,\ \rangle_v$ is the natural one induced by the identifications of (7) and (8), and so $H^1_f(K_v, V^*)$ and $H^1_f(K_v, V)$ are orthogonal complements.

Let $\mathcal{O}_L$ denote the ring of integers of L.

Proposition 6.3. (i) *There is a natural isomorphism*

$$H^1(K, W^*) \xrightarrow{\sim} (L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi.$$

(ii) *There is an exact sequence*

$$0 \longrightarrow (\mathcal{O}_L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi \longrightarrow \mathcal{S}(K, W^*) \longrightarrow A^\chi_L \longrightarrow 0.$$

Proof. Since $[L:K]$ is prime to p, the restriction map

$$\begin{aligned} H^1(K, W^*) \xrightarrow{\mathrm{res}_{L/K}} H^1(L, W^*)^\Delta &= (H^1(L, \boldsymbol{\mu}_{p^\infty}) \otimes \mathcal{O}_{\chi^{-1}})^\Delta \\ &\cong H^1(L, \boldsymbol{\mu}_{p^\infty})^\chi \cong (L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi. \end{aligned}$$

is an isomorphism, which gives (i). It follows easily from (7) that for every v there is an isomorphism, compatible with (i),

$$H^1_f(K_v, W^*) \xrightarrow{\sim} U^\chi_{L,v} \otimes \mathbf{Q}_p/\mathbf{Z}_p.$$

Therefore if we define

$$X_L = \{y \otimes p^{-n} \in L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p : \mathrm{ord}_w(y) \equiv 0 \pmod{p^n} \text{ for every place } w \text{ of } L\},$$

then

$$\mathrm{res}_{L/K}(\mathcal{S}(K, W^*)) \cong X_L^\chi.$$

Suppose $x \in X_L$ is represented by $y \otimes p^{-n}$ with $y \in L^\times$. Then the principal fractional ideal $y\mathcal{O}_L$ is of the form $\mathfrak{a}^{p^n}$ for some fractional ideal $\mathfrak{a}$. This map $x \mapsto \mathfrak{a}$ induces a well defined surjection from X_L to the p-part $A_L^{(p)}$ of the ideal class group of L. Thus there is an exact sequence

$$0 \longrightarrow \mathcal{O}_L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow X_L \longrightarrow A_L^{(p)} \longrightarrow 0,$$

and taking χ-components gives the exact sequence of the proposition. □

Let Σ_p denote the set of primes of K above p.

COROLLARY 6.4. *If Leopoldt's conjecture holds for L then* $\mathcal{S}_{\Sigma_p}(K, W^*)$ *is finite.*

PROOF. Leopoldt's conjecture for L is the assertion that the p-adic completion of $\mathcal{O}_L^\times$ injects into $(L \otimes \mathbf{Q}_p)^\times$. This implies that the map

$$(\mathcal{O}_L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi \longrightarrow ((L \otimes \mathbf{Q}_p)^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi \cong \oplus_{v|p} H^1(K_v, W^*)$$

has finite kernel, so the corollary follows from Proposition 6.3(ii) and the finiteness of the ideal class group. □

COROLLARY 6.5. *With notation as above, suppose that* $K = \mathbf{Q}$*. If* χ *is odd (i.e.,* χ *sends complex conjugation to* -1*) then* $\mathcal{S}(\mathbf{Q}, W^*) \cong A_L^\chi$.

PROOF. Since χ is odd, $(\mathcal{O}_L^\times)^\chi$ is finite and so $(\mathcal{O}_L^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi = 0$. Thus the corollary follows immediately from Proposition 6.3(ii). □

6.4. Abelian varieties. Let A be an abelian variety defined over K and $T = T_p(A)$ the p-adic Tate module of A as in Example 1.5. (See for example [**Si**] for the basic facts in the special case of elliptic curves.) Then

$$V = V_p(A) = T_p(A) \otimes \mathbf{Q}_p, \qquad W = V_p(A)/T_p(A) = A_{p^\infty},$$

where A_{p^∞} is the p-power torsion in $A(\bar{K})$.

For every place v of K there is a natural injective Kummer map

$$A(K_v)\hat{}\otimes_{\mathbf{Z}_p} \mathbf{Q}_p \hookrightarrow H^1(K_v, V_p(A)) \tag{9}$$

where $A(K_v)\hat{}$ denotes the p-adic completion of $A(K_v)$. If v is a prime of K above p we define $H^1_f(K_v, V_p(A))$ to be the image of this map. This definition agrees with the Bloch-Kato definition of H^1_f.

REMARK 6.6. Let A^* denote the dual abelian variety of A. Then $V_p(A)^* = V_p(A^*)$, and if we define the $H^1_f(K_v, V_p(A^*))$ in the same way then $H^1_f(K_v, V_p(A))$ and $H^1_f(K_v, V_p(A^*))$ are orthogonal complements of each other under the local pairing $\langle\ ,\ \rangle_{K_v}$.

Note that if we fix a polarization of A, then the Weil pairing gives an isomorphism $V_p(A^*) \cong V_p(A)$, and this isomorphism identifies $H^1_f(K_v, V_p(A))$ and $H^1_f(K_v, V_p(A^*))$.

PROPOSITION 6.7. *The Selmer group $\mathcal{S}(K, A_{p^\infty})$ is the usual p-power Selmer group attached to the abelian variety A, sitting in an exact sequence*

$$0 \longrightarrow A(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathcal{S}(K, A_{p^\infty}) \longrightarrow Ш(A_{/K})_{p^\infty} \longrightarrow 0$$

where $Ш(A_{/K})_{p^\infty}$ denotes the p-part of the Tate-Shafarevich group of A over K.

PROOF. Suppose $v \nmid p$. If ℓ is the rational prime below p, then $A(K_v)$ has a subgroup of finite index which is a pro-ℓ group, so the p-adic completion $A(K_v)\hat{}$ is finite. Also in this case $H^1_f(K_v, V_p(A)) = 0$ by Corollary 3.3(i) and Remark 3.7. Therefore for every v (including those above p), $H^1_f(K_v, V_p(A))$ is the image of the map (9). It follows that for every v, $H^1_f(K_v, A_{p^\infty})$ is the image of $A(K_v)\hat{} \otimes \mathbf{Q}_p/\mathbf{Z}_p$ under the corresponding Kummer map, and so the definition of $\mathcal{S}(K, A_{p^\infty})$ coincides with the classical definition of the Selmer group of A. □

7. Global duality

As in §5 we suppose that K is a number field and T is a p-adic representation of G_K ramified at only finitely many primes of K. For all primes v dividing p we also fix special subspaces $H^1_f(K_v, V) \subset H^1(K_v, V)$ and $H^1_f(K_v, V^*) \subset H^1(K_v, V^*)$ which are orthogonal complements under the pairing $\langle\ ,\ \rangle_{K_v}$ of Theorem 4.1. We will also denote this pairing by $\langle\ ,\ \rangle_v$

REMARK 7.1. If the representation V is potentially semistable (see [**FPR**] §I.2) at a place v dividing p, then the Bloch-Kato subspaces $H^1_f(K_v, V)$ and $H^1_f(K_v, V^*)$ are orthogonal complements (see [**FPR**] Proposition I.3.3.9(iii) or [**BK**] Proposition 3.8).

DEFINITION 7.2. If $\Sigma_0 \subset \Sigma$ are finite sets of places of K we will write

$$\begin{array}{rrcl}
\mathrm{loc}_\Sigma : & H^1(K, W_M) & \longrightarrow & \bigoplus_{v\in\Sigma} H^1(K_v, W_M) \\
\mathrm{loc}^s_{\Sigma,\Sigma_0} : & \mathcal{S}^\Sigma(K, W_M) & \longrightarrow & \bigoplus_{v\in\Sigma-\Sigma_0} H^1_s(K_v, W_M) \\
\mathrm{loc}^f_{\Sigma,\Sigma_0} : & \mathcal{S}_{\Sigma_0}(K, W_M) & \longrightarrow & \bigoplus_{v\in\Sigma-\Sigma_0} H^1_f(K_v, W_M)
\end{array}$$

for the respective localization maps.

THEOREM 7.3 (Poitou-Tate duality). *Suppose $M \in \mathcal{O}$ is nonzero and $\Sigma_0 \subset \Sigma$ are finite sets of places of K.*

(i) *There are exact sequences*

$$0 \longrightarrow \mathcal{S}^{\Sigma_0}(K, W_M) \longrightarrow \mathcal{S}^\Sigma(K, W_M) \xrightarrow{\mathrm{loc}^s_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma-\Sigma_0} H^1_s(K_v, W_M),$$

$$0 \longrightarrow \mathcal{S}_\Sigma(K, W^*_M) \longrightarrow \mathcal{S}_{\Sigma_0}(K, W^*_M) \xrightarrow{\mathrm{loc}^f_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma-\Sigma_0} H^1_f(K_v, W^*_M).$$

(ii) *The images $\mathrm{loc}^s_{\Sigma,\Sigma_0}(\mathcal{S}^\Sigma(K, W_M))$ and $\mathrm{loc}^f_{\Sigma,\Sigma_0}(\mathcal{S}_{\Sigma_0}(K, W^*_M))$ are orthogonal complements of each other with respect to the pairing $\sum_{v\in\Sigma-\Sigma_0}\langle\ ,\ \rangle_v$.*

(iii) *There is an isomorphism*

$$\mathcal{S}_{\Sigma_0}(K, W_M^*)/\mathcal{S}_\Sigma(K, W_M^*) \xrightarrow{\sim} \mathrm{Hom}_\mathcal{O}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma,\Sigma_0}), \mathcal{O}/M\mathcal{O}).$$

PROOF. Assertion (i) is immediate from the definitions of the Selmer groups involved.

For (ii), recall that by Theorem 4.1 and Proposition 4.3(ii), $\langle\ ,\ \rangle_v$ induces a non-degenerate pairing on $H^1_s(K_v, W_M) \times H^1_f(K_v, W_M^*)$. Suppose first that Σ contains all infinite places, all primes above p, and all primes where T is ramified, so that $\mathcal{S}^\Sigma(K, W_M) = H^1(K_\Sigma/K, W_M)$ and $\mathcal{S}^\Sigma(K, W_M^*) = H^1(K_\Sigma/K, W_M^*)$ by Lemma 5.3. Under these conditions, a part of the Poitou-Tate duality exact sequence ([**Mi**] Theorem I.4.10 or [**T1**] Theorem 3.1) gives

$$\mathcal{S}^\Sigma(K, W_M) \xrightarrow{\mathrm{loc}_\Sigma} \bigoplus_{v\in\Sigma} H^1(K_v, W_M) \xrightarrow{\mathrm{loc}_\Sigma^\vee} \mathcal{S}^\Sigma(K, W_M^*)^\vee \tag{10}$$

where $\mathcal{S}^\Sigma(K, W_M^*)^\vee = \mathrm{Hom}(\mathcal{S}^\Sigma(K, W_M^*), \mathcal{O}/M\mathcal{O})$ and the maps are induced by localization and the local pairings between $H^1(K_v, W_M)$ and $H^1(K_v, W_M^*)$. Using Proposition 4.3(ii), we can combine (10) and (i) to produce a new exact sequence

$$\begin{aligned} 0 \longrightarrow \mathcal{S}^{\Sigma_0}(K, W_M) \longrightarrow \mathcal{S}^\Sigma(K, W_M) &\xrightarrow{\mathrm{loc}^s_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma-\Sigma_0} H^1_s(K_v, W_M) \\ &\xrightarrow{{\mathrm{loc}^f_{\Sigma,\Sigma_0}}^\vee} \mathcal{S}_{\Sigma_0}(K, W_M^*)^\vee \longrightarrow \mathcal{S}_\Sigma(K, W_M^*)^\vee \longrightarrow 0. \end{aligned} \tag{11}$$

The exactness in the center proves (ii) in this case. (To see the exactness in the center, note that the dual of the tautological exact sequence

$$\begin{aligned} 0 \longrightarrow \mathcal{S}_{\Sigma_0}(K, W_M^*) &\longrightarrow \mathcal{S}^\Sigma(K, W_M^*) \\ &\xrightarrow{\mathrm{loc}_{\Sigma_0} \oplus \mathrm{loc}^s_{\Sigma-\Sigma_0}} \bigoplus_{v\in\Sigma_0} H^1(K_v, W_M^*) \bigoplus_{v\in\Sigma-\Sigma_0} H^1_s(K_v, W_M^*) \end{aligned}$$

is

$$\begin{aligned} &\bigoplus_{v\in\Sigma_0} H^1(K_v, W_M) \bigoplus_{v\in\Sigma-\Sigma_0} H^1_f(K_v, W_M) \\ &\qquad \xrightarrow{(\mathrm{loc}_{\Sigma_0} \oplus \mathrm{loc}^s_{\Sigma-\Sigma_0})^\vee} \mathcal{S}^\Sigma(K, W_M^*)^\vee \longrightarrow \mathcal{S}_{\Sigma_0}(K, W_M^*)^\vee \longrightarrow 0. \end{aligned}$$

Splicing this together with (10) and

$$\begin{aligned} 0 \longrightarrow &\bigoplus_{v\in\Sigma_0} H^1(K_v, W_M) \bigoplus_{v\in\Sigma-\Sigma_0} H^1_f(K_v, W_M) \\ &\longrightarrow \bigoplus_{v\in\Sigma} H^1(K_v, W_M) \longrightarrow \bigoplus_{v\in\Sigma-\Sigma_0} H^1_s(K_v, W_M) \longrightarrow 0 \end{aligned}$$

gives (11).)

Now suppose Σ is arbitrary, and let Σ' be a finite set of places containing Σ, all infinite places, all primes above p, and all primes where T is ramified. Then the argument above applies to the pairs $\Sigma \subset \Sigma'$ and to $\Sigma_0 \subset \Sigma'$, so we have a diagram

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
\mathcal{S}^{\Sigma'}(K,W_M)/\mathcal{S}^{\Sigma_0}(K,W_M) \arrow[r] \arrow[d, "\mathrm{loc}^s_{\Sigma',\Sigma_0}"'] & \mathcal{S}^{\Sigma'}(K,W_M)/\mathcal{S}^{\Sigma}(K,W_M) \arrow[d, "\mathrm{loc}^s_{\Sigma',\Sigma}"'] \\
\bigoplus_{v\in\Sigma'-\Sigma_0} H^1_s(K_v,W_M) \arrow[r] \arrow[d, "(\mathrm{loc}^f_{\Sigma',\Sigma_0})^\vee"'] & \bigoplus_{v\in\Sigma'-\Sigma} H^1_s(K_v,W_M) \arrow[d, "(\mathrm{loc}^f_{\Sigma',\Sigma})^\vee"'] \\
(\mathcal{S}_{\Sigma_0}(K,W_M^*)/\mathcal{S}_{\Sigma'}(K,W_M^*))^\vee \arrow[r] \arrow[d] & (\mathcal{S}_{\Sigma}(K,W_M^*)/\mathcal{S}_{\Sigma'}(K,W_M^*))^\vee \arrow[d] \\
0 & 0
\end{tikzcd}$$

with surjective horizontal maps. The Snake Lemma gives an exact sequence of kernels of the horizontal maps

$$0 \longrightarrow \mathcal{S}^{\Sigma}(K,W_M)/\mathcal{S}^{\Sigma_0}(K,W_M) \xrightarrow{\mathrm{loc}^s_{\Sigma,\Sigma_0}} \oplus_{v\in\Sigma-\Sigma_0} H^1_s(K_v,W_M)$$
$$\xrightarrow{(\mathrm{loc}^f_{\Sigma,\Sigma})^\vee} (\mathcal{S}_{\Sigma_0}(K,W_M^*)/\mathcal{S}_{\Sigma}(K,W_M^*))^\vee \longrightarrow 0$$

and the exactness in the center proves (ii) for $\Sigma_0 \subset \Sigma$. Assertion (iii) is just a restatement of (ii). □

REMARK 7.4. Theorem 7.3 will be applied with Σ_0 equal to the empty set or the set of primes dividing p, and with Σ large enough so that $\mathcal{S}_\Sigma(K,W_M^*)=0$. In that situation, it follows from Theorem 7.3(iii) that

$$|\mathcal{S}_{\Sigma_0}(K,W_M^*)| = |\mathrm{coker}(\mathrm{loc}^s_{\Sigma,\Sigma_0})|.$$

Thus if one can produce "enough" cohomology classes in $\mathcal{S}^\Sigma(K,W_M)$, one obtains a good bound on the size of $\mathcal{S}_{\Sigma_0}(K,W_M^*)$. The purpose of an Euler system is to construct these classes.

Recall that Σ_p denotes the set of primes of K above p.

COROLLARY 7.5. *There is an isomorphism*

$$\mathcal{S}(K,W^*)/\mathcal{S}_{\Sigma_p}(K,W^*) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma_p}), \mathbf{D})$$

where $\mathrm{loc}^s_{\Sigma_p}$ *is the localization map* $\mathcal{S}^{\Sigma_p}(K,T) \to \prod_{v|p} H^1_s(K_v,T)$.

PROOF. We apply Theorem 7.3(iii) with $\Sigma = \Sigma_p$ and with Σ_0 equal to the empty set, and take the direct limit over M to obtain

$$\varinjlim_M \mathcal{S}(K,W_M^*)/\mathcal{S}_{\Sigma_p}(K,W_M^*) \cong \varinjlim_M \mathrm{Hom}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma_p,M}), \mathcal{O}/M\mathcal{O}).$$

where $\mathrm{loc}^s_{\Sigma_p,M}$ is the localization map $\mathcal{S}^{\Sigma_p}(K,W_M) \to \oplus_{v|p} H^1_s(K_v,W_M)$. By Proposition 5.6(ii),

$$\varinjlim_M \mathcal{S}(K,W_M^*)/\mathcal{S}_{\Sigma_p}(K,W_M^*) = \mathcal{S}(K,W^*)/\mathcal{S}_{\Sigma_p}(K,W^*).$$

By Proposition 5.6(i),

$$\varprojlim_{M} \mathcal{S}^{\Sigma_p}(K, W_M) = \mathcal{S}^{\Sigma_p}(K, T),$$

and by Corollary 3.10,

$$\varprojlim_{M} \oplus_{v|p} H^1_s(K_v, W_M) = \oplus_{v|p} H^1_s(K_v, T).$$

Since all the groups $\mathcal{S}^{\Sigma_p}(K, W_M)$ and $H^1_s(K_v, W_M)$ are finite (Proposition B.2.7(ii) and Lemma 5.7), it follows (Proposition B.1.1) that

$$\varinjlim_{M} \mathrm{Hom}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma_p, M}), \mathcal{O}/M\mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\varprojlim_{M} \mathrm{coker}(\mathrm{loc}^s_{\Sigma_p, M}), \mathbf{D})$$

and that

$$\varprojlim_{M} \mathrm{coker}(\mathrm{loc}^s_{\Sigma_p, M}) = \mathrm{coker}(\mathrm{loc}^s_{\Sigma_p}).$$

This completes the proof. $\square$

CHAPTER II

Euler systems: definition and main results

In this chapter we state our main results. The definition of an Euler system is given in §1, and the theorems applying Euler systems to study Selmer groups over number fields and over $\mathbf{Z}_p^d$-extensions of number fields are given in §2 and §3, respectively. Examples and applications are given in Chapter III; the reader might benefit from following along in those examples while reading this chapter. The proofs, using tools to be developed in Chapter IV, will be given in Chapters V and VII. In Chapter IX we discuss some variants and extensions of the definition of Euler system given below.

For similar results see the papers of Kato [**Ka2**] and Perrin-Riou [**PR5**].

For a first reading, one might want to restrict below to the case $K = \mathbf{Q}$ (so that the group of global units $\mathcal{O}_K^\times$ is finite) and $\mathcal{O} = \mathbf{Z}_p$. This simplifies the notation, while all the main ideas still appear.

1. Euler systems

Fix a number field K, and let $\mathcal{O}_K$ denote the ring of integers of K. Fix also a rational prime p and a p-adic representation T of G_K as in Chapter I §1, with coefficients in the ring of integers $\mathcal{O}$ of some finite extension Φ of $\mathbf{Q}_p$. We assume in addition, as in Chapter I §5, that T is unramified outside a finite set of primes of K.

For every prime $\mathfrak{q}$ of K not dividing p where T is unramified, let $K(\mathfrak{q})$ denote the maximal p-extension of K inside the ray class field of K modulo $\mathfrak{q}$, let $\mathrm{Fr}_\mathfrak{q}$ denote a Frobenius of $\mathfrak{q}$ in G_K, and define

$$P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;x) = \det(1 - \mathrm{Fr}_\mathfrak{q}^{-1}x|T^*) \in \mathcal{O}[x]$$

(the determinant is well-defined because T^* is unramified at $\mathfrak{q}$).

We will write

$$K \subset_{\mathrm{f}} F$$

to indicate that F is a *finite* extension of K.

Definition 1.1. Suppose $\mathcal{K}$ is an (infinite) abelian extension of K and $\mathcal{N}$ is an ideal of K divisible by p and by all primes where T is ramified, such that

(i) $\mathcal{K}$ contains $K(\mathfrak{q})$ for every prime $\mathfrak{q}$ of K not dividing $\mathcal{N}$,

(ii) $\mathcal{K}$ contains an extension K_∞ of K such that
 $\mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^d$ for some $d \geq 1$,
 no (finite) prime of K splits completely in K_∞/K.

A collection of cohomology classes

$$\mathbf{c} = \{\mathbf{c}_F \in H^1(F,T) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$$

is an *Euler system* for $(T,\mathcal{K},\mathcal{N})$ if, whenever $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$,

$$\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \Bigg(\prod_{\mathfrak{q}\in\Sigma(F'/F)} P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})\Bigg)\mathbf{c}_F$$

where $\Sigma(F'/F)$ is the set of (finite) primes of K, not dividing $\mathcal{N}$, which ramify in F' but not in F.

We say a collection $\mathbf{c} = \{\mathbf{c}_F \in H^1(F,T)\}$ is an Euler system for T if $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$ for some choice of $\mathcal{N}$ and $\mathcal{K}$ as above.

If K_∞ is a $\mathbf{Z}_p^d$-extension of K in which no finite prime splits completely, we say a collection $\mathbf{c} = \{\mathbf{c}_F \in H^1(F,T)\}$ is an Euler system for (T,K_∞) if $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$ for some choice of $\mathcal{N}$ and $\mathcal{K}$ containing K_∞ as above.

REMARK 1.2. The condition that no finite prime splits completely in K_∞/K is satisfied, for example, if K_∞ contains the cyclotomic $\mathbf{Z}_p$-extension of K.

In general, since $\mathbf{Z}_p^d$ has no proper finite subgroups, to say that a prime does not split completely in K_∞/K is equivalent to saying that its decomposition group is infinite. See Chapter IX §2 for additional remarks about this assumption.

Note that since we require $\mathcal{N}$ to be divisible by p, no Euler factors at primes dividing p enter our picture. It follows from our definition that the Euler system classes are "universal norms" in the K_∞/K direction, i.e., if $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset F'K_\infty$, then $\Sigma(F'/F)$ is empty so

$$\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \mathbf{c}_F.$$

On the other hand, one might want to include Euler factors for primes where T is ramified. One could easily modify the definition above to take such Euler factors into account. Alternatively, one can choose an ideal $\mathcal{N}'$ prime to p, replace $\mathcal{K}$ by the maximal extension $\mathcal{K}'$ of K in $\mathcal{K}$ which is unramified at the primes dividing $\mathcal{N}'$, and replace $\mathcal{N}$ by $\mathcal{N}\mathcal{N}'$. Then the Euler factors at primes dividing $\mathcal{N}'$ become irrelevant, and no information has been lost when we apply the theorems below (since the conclusions are independent of $\mathcal{K}$ and $\mathcal{N}$).

REMARK 1.3. If $\mathfrak{m}$ is a generalized ideal of K (i.e., $\mathfrak{m}$ can be divisible by archimedean places as well as prime ideals) let $K[\mathfrak{m}]$ denote the ray class field of K modulo $\mathfrak{m}$. Given $\mathcal{K}$ and $\mathcal{N}$ as in the definition above, an Euler system for $(T,\mathcal{K},\mathcal{N})$ is equivalent to a collection $\{\tilde{\mathbf{c}}_{\mathfrak{m}} \in H^1(K[\mathfrak{m}]\cap\mathcal{K},T)\ :\ \text{every } \mathfrak{m}\}$ satisfying

$$\mathrm{Cor}_{K[\mathfrak{m}\mathfrak{q}]\cap\mathcal{K}/K[\mathfrak{m}]\cap\mathcal{K}}(\tilde{\mathbf{c}}_{\mathfrak{m}\mathfrak{q}}) = \begin{cases} P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})\tilde{\mathbf{c}}_{\mathfrak{m}} & \text{if } \mathfrak{q}\nmid\mathfrak{m}\mathcal{N} \\ \tilde{\mathbf{c}}_{\mathfrak{m}} & \text{if } \mathfrak{q}\mid\mathfrak{m}\mathcal{N}. \end{cases}$$

For, given such a collection, if F is any subfield of $\mathcal{K}$, then we can define

$$\mathbf{c}_F = \mathrm{Cor}_{K[\mathfrak{m}]\cap\mathcal{K}/F}(\tilde{\mathbf{c}}_{\mathfrak{m}})$$

where $\mathfrak{m}$ is the conductor of F/K. One checks easily that the collection $\{\mathbf{c}_F\}$ is an Euler system. Conversely, given an Euler system $\{\mathbf{c}_F\}$ we can define

$$\tilde{\mathbf{c}}_{\mathfrak{m}} = \prod P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})\,\mathbf{c}_{K[\mathfrak{m}]\cap\mathcal{K}}$$

where the product is over primes dividing $\mathfrak{m}$, not dividing $\mathcal{N}$, which are unramified in $(K[\mathfrak{m}] \cap \mathcal{K})/K$.

Remark 1.4. Suppose now that we are given $\mathcal{N}$ and K_∞/K as in Definition 1.1. If $\mathfrak{r} = \mathfrak{q}_1 \cdots \mathfrak{q}_k$ is a product of distinct primes not dividing $\mathcal{N}$, then we define $K(\mathfrak{r})$ to be the compositum

$$K(\mathfrak{r}) = K(\mathfrak{q}_1) \cdots K(\mathfrak{q}_k).$$

and if $K \subset_{\mathrm{f}} F \subset K_\infty$ we let $F(\mathfrak{r}) = FK(\mathfrak{r})$. Let $\mathcal{K}_{\min}$ be the compositum of K_∞ and all $K(\mathfrak{q})$ for primes $\mathfrak{q}$ not dividing $\mathcal{N}$. Thus $\mathcal{K}_{\min}$ is the smallest extension of K satisfying the conditions of Definition 1.1 for $\mathcal{N}$ and K_∞/K. Every finite extension of K in $\mathcal{K}_{\min}$ is contained in $F(\mathfrak{r})$ for some squarefree ideal $\mathfrak{r}$ prime to $\mathcal{N}$ and some $K \subset_{\mathrm{f}} F \subset K_\infty$. It follows easily that an Euler system for $(T, \mathcal{K}_{\min}, \mathcal{N})$ is completely determined by the subcollection

$$\{\mathbf{c}_{F(\mathfrak{r})} : \mathfrak{r} \text{ is squarefree and prime to } \mathcal{N},\ K \subset_{\mathrm{f}} F \subset K_\infty\}.$$

Conversely, suppose we are given a collection $\{\mathbf{c}_{F(\mathfrak{r})}\}$ such that if $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset K_\infty$, $\mathfrak{r}$ is a squarefree ideal of K prime to $\mathcal{N}$, and $\mathfrak{q}$ is a prime of K not dividing $\mathfrak{r}\mathcal{N}$ such that $K(\mathfrak{q}) \neq K$, then

$$\begin{aligned}\mathrm{Cor}_{F(\mathfrak{r}\mathfrak{q})/F(\mathfrak{r})}(\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})}) &= P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; \mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{c}_{F(\mathfrak{r})},\\ \mathrm{Cor}_{F'(\mathfrak{r})/F(\mathfrak{r})}(\mathbf{c}_{F'(\mathfrak{r})}) &= \mathbf{c}_{F(\mathfrak{r})}.\end{aligned}$$

(Note that if $K(\mathfrak{q}) = K$ then $F(\mathfrak{r}\mathfrak{q}) = F(\mathfrak{r})$.) Then this collection determines an Euler system: if $K \subset_{\mathrm{f}} L \subset \mathcal{K}_{\min}$ then we can set

$$\mathbf{c}_L = \mathrm{Cor}_{F(\mathfrak{r})/L}(\mathbf{c}_{F(\mathfrak{r})})$$

where $\mathfrak{r}$ and F are minimal such that $L \subset F(\mathfrak{r})$. Thus we may view an Euler system for $(T, \mathcal{K}_{\min}, \mathcal{N})$ as such a collection $\{\mathbf{c}_{F(\mathfrak{r})}\}$.

Remark 1.5. Kolyvagin's original method (see [**Ko2**] or [**Ru3**]) required the Euler system to satisfy an additional "congruence" condition. By expanding on an idea from [**Ru6**], using our assumption that $\mathcal{K}$ contains K_∞ (i.e., that our Euler system extends "in the p-direction"), we will be able to bypass the need for the congruence condition. In fact, the congruence condition follows easily from the techniques we will use in Chapter IV, and although we do not need it, we will state and prove it in Chapter IV §8 (Corollary IV.8.1).

On the other hand, if we assume that our Euler system classes satisfy appropriate congruence conditions then we can remove from Definition 1.1(ii) the assumption that $\mathcal{K}$ contains K_∞, so we need not have classes that are "universal norms". See Chapter IX for a discussion of this and other possible variations in the definition of an Euler system.

2. Results over K

We now come to the fundamental application of Euler systems: using the "derivative" classes associated to an Euler system (see Chapter IV §4) and the duality theorems from Galois cohomology stated in Chapter I §7 to bound the order of a Selmer group (Theorems 2.2, 2.3, and 2.10).

Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$ and $\Bbbk = \mathcal{O}/\mathfrak{p}$ the residue field. Let $K(1)$ be the maximal p-extension of K inside the Hilbert class field of K. We will make use of two different sets of hypotheses on the Galois representation T. Hypotheses $\mathrm{Hyp}(K,T)$ are stronger than $\mathrm{Hyp}(K,V)$, and will allow us to prove a stronger conclusion.

HYPOTHESES $\mathrm{Hyp}(K,T)$.

(i) There is a $\tau \in G_K$ such that
- τ acts trivially on $\boldsymbol{\mu}_{p^\infty}$, on $(\mathcal{O}_K^\times)^{1/p^\infty}$, and on $K(1)$,
- $T/(\tau-1)T$ is free of rank one over $\mathcal{O}$.

(ii) $T \otimes \Bbbk$ is an irreducible $\Bbbk[G_K]$-module.

HYPOTHESES $\mathrm{Hyp}(K,V)$.

(i) There is a $\tau \in G_K$ such that
- τ acts trivially on $\boldsymbol{\mu}_{p^\infty}$, on $(\mathcal{O}_K^\times)^{1/p^\infty}$, and on $K(1)$,
- $\dim_\Phi(V/(\tau-1)V) = 1$.

(ii) V is an irreducible $\Phi[G_K]$-module.

DEFINITION 2.1. If $\mathbf{c}$ is an Euler system, we define the *index of divisibility* of $\mathbf{c}$ to be

$$\mathrm{ind}_\mathcal{O}(\mathbf{c}) = \sup\{n : \mathbf{c}_K \in \mathfrak{p}^n H^1(K,T) + H^1(K,T)_{\mathrm{tors}}\} \le \infty,$$

i.e., $\mathfrak{p}^{\mathrm{ind}_\mathcal{O}(\mathbf{c})}$ is the largest power of the maximal ideal by which $\mathbf{c}_K$ can be divided in $H^1(K,T)/H^1(K,T)_{\mathrm{tors}}$.

Write $\ell_\mathcal{O}(B)$ for the length of an $\mathcal{O}$-module B, so that $|B| = |\Bbbk|^{\ell_\mathcal{O}(B)}$. We allow $\ell_\mathcal{O}(B) = \infty$.

Define $\Omega = K(1)K(W)K(\boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})$ where $K(W)$ denotes the smallest extension of K such that $G_{K(W)}$ acts trivially on W.

Let Σ_p denote the set of primes of K above p.

THEOREM 2.2. *Suppose that $p > 2$ and that T satisfies* $\mathrm{Hyp}(K,T)$. *If* $\mathbf{c}$ *is an Euler system for T then*

$$\ell_\mathcal{O}(\mathcal{S}_{\Sigma_p}(K,W^*)) \le \mathrm{ind}_\mathcal{O}(\mathbf{c}) + \mathfrak{n}_W + \mathfrak{n}_W^*$$

where

$$\mathfrak{n}_W = \ell_\mathcal{O}(H^1(\Omega/K,W) \cap \mathcal{S}^{\Sigma_p}(K,W))$$
$$\mathfrak{n}_W^* = \ell_\mathcal{O}(H^1(\Omega/K,W^*) \cap \mathcal{S}_{\Sigma_p}(K,W^*))$$

THEOREM 2.3. *Suppose that V satisfies* $\mathrm{Hyp}(K,V)$ *and T is not the one-dimensional trivial representation. If* $\mathbf{c}$ *is an Euler system for T and* $\mathbf{c}_K \notin H^1(K,T)_{\mathrm{tors}}$, *then $\mathcal{S}_{\Sigma_p}(K,W^*)$ is finite.*

Note that Theorem 2.3 holds even if $p = 2$.

REMARK 2.4. Hypotheses $\mathrm{Hyp}(K,T)$ are satisfied if the image of the Galois representation on T is "sufficiently large". They often hold in practice; see the discussion of the examples in the next chapter. If $\mathrm{rank}_\mathcal{O}(T) = 1$, then (i) holds with $\tau = 1$, and (ii) holds as well.

REMARK 2.5. Corollary C.2.2 shows that if V is an irreducible $\Phi[G_K]$-module, then $H^1(\Omega/K, W)$ is finite (resp. $H^1(\Omega/K, W^*)$ is finite) unless $T = \mathcal{O}$ with trivial action (resp. $T = \mathcal{O}(1)$). Frequently the "error terms" $\mathfrak{n}_W$ and $\mathfrak{n}_W^*$ in Theorem 2.2 are zero; see the examples in Chapter III.

REMARK 2.6. Hypothesis $\mathrm{Hyp}(K, T)$(i) is used to guarantee the existence of a supply of primes $\mathfrak{q}$ of K such that $H^1_f(K(\mathfrak{q}), W_M)$ and $H^1_s(K(\mathfrak{q}), W^*_M)$ are free of rank one over $\mathcal{O}/M\mathcal{O}$. This in turn makes it possible to use Theorem I.7, along with the cohomology classes we will construct from the Euler system in Chapter IV, to bound the Selmer group as in Theorem 2.2.

REMARK 2.7. In the exceptional case $T = \mathcal{O}$ of Theorem 2.3, $\mathcal{S}_{\Sigma_p}(K, W^*)$ is finite if and only if Leopoldt's conjecture holds for K. See Corollary I.6.4.

REMARK 2.8. There is always a trivial Euler system defined by $\mathbf{c}_{F(\mathfrak{r})} = 0$ for all F and $\mathfrak{r}$. But in that case $\mathrm{ind}_{\mathcal{O}}(\mathbf{c}) = \infty$ so Theorems 2.2 and 2.3 say nothing.

REMARK 2.9. Theorem 2.2 gives a bound for the size of $\mathcal{S}_{\Sigma_p}(K, W^*)$, not the true Selmer group $\mathcal{S}(K, W^*)$. Since we have put no local conditions at p either on our representation T or our Euler system $\mathbf{c}$, that restricted Selmer group is all that the Euler system can "see". Combining the global duality results from Chapter I §7 with Theorems 2.2 and 2.3 gives Theorem 2.10 below concerning $\mathcal{S}(K, W^*)$.

Suppose that for every prime v dividing p we have subspaces $H^1_f(K_v, V) \subset H^1(K_v, V)$ and $H^1_f(K_v, V^*) \subset H^1(K_v, V^*)$ which are orthogonal complements under the pairing $\langle\ ,\ \rangle_{K_v}$, as in Chapter I §7. We write

$$H^1(K_p, \,\cdot\,) = \oplus_{v|p} H^1(K_v, \,\cdot\,)$$

and similarly for H^1_f and $H^1_s = H^1/H^1_f$, and let

$$\mathrm{loc}^s_{\Sigma_p} : \mathcal{S}^{\Sigma_p}(K, T) \to H^1_s(K_p, T)$$

be the localization map as in Corollary I.7.5.

By Corollary B.3.4 (see also Proposition IV.6.1) and Lemma I.3.5(ii), if $\mathbf{c}$ is an Euler system then $\mathbf{c}_K \in \mathcal{S}^{\Sigma_p}(K, T)$.

THEOREM 2.10. *Suppose* $\mathbf{c}$ *is an Euler system for* T *and* $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K) \neq 0$.

(i) *If* T *is not the one-dimensional trivial representation,* V *satisfies* $\mathrm{Hyp}(K, V)$, *and* $[H^1_s(K_p, T) : \mathcal{O}\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)]$ *is finite, then* $\mathcal{S}(K, W^*)$ *is finite.*
(ii) *Suppose that* $p > 2$ *and* T *satisfies* $\mathrm{Hyp}(K, T)$. *Let* $\mathfrak{n}_W$ *and* $\mathfrak{n}^*_W$ *be as in Theorem* 2.2. *Then*

$$\ell_{\mathcal{O}}(\mathcal{S}(K, W^*)) \le \ell_{\mathcal{O}}(H^1_s(K_p, T)/\mathcal{O}\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)) + \mathfrak{n}_W + \mathfrak{n}^*_W.$$

PROOF. We will use Theorems 2.2 and 2.3 to bound $\mathcal{S}_{\Sigma_p}(K, W^*)$, and Corollary I.7.5 to bound $[\mathcal{S}(K, W^*) : \mathcal{S}_{\Sigma_p}(K, W^*)]$.

For every v, $H^1_s(K_v, T)$ is torsion-free since by definition it injects into the vector space $H^1_s(K_v, V)$. Hence if $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)$ is not zero then $\mathbf{c}_K \notin H^1(K, T)_{\mathrm{tors}}$. Now Theorem 2.3 shows that $\mathcal{S}_{\Sigma_p}(K, W^*)$ is finite, and Corollary I.7.5 shows that

$$\begin{aligned} [\mathcal{S}(K, W^*) : \mathcal{S}_{\Sigma_p}(K, W^*)] &= [H^1_s(K_p, T) : \mathcal{O}\mathrm{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K, T))] \qquad (1)\\ &\le [H^1_s(K_p, T) : \mathcal{O}\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)]. \end{aligned}$$

This proves (i).

The definition of $\mathcal{S}^{\Sigma_p}(K,T)$ gives an injective map

$$H^1(K,T)/\mathcal{S}^{\Sigma_p}(K,T) \hookrightarrow \oplus_{v\nmid p} H^1_s(K_v,T),$$

so $H^1(K,T)/\mathcal{S}^{\Sigma_p}(K,T)$ is torsion-free. It follows that for every n,

$$\begin{aligned} \mathbf{c}_K \in \mathfrak{p}^n H^1(K,T) + H^1(K,T)_{\mathrm{tors}} \;&\Rightarrow\; \mathbf{c}_K \in \mathfrak{p}^n \mathcal{S}^{\Sigma_p}(K,T) + H^1(K,T)_{\mathrm{tors}} \\ &\Rightarrow\; \mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K) \in \mathfrak{p}^n \mathrm{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K,T)). \end{aligned}$$

Therefore if $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K) \neq 0$ then

$$\mathrm{ind}_{\mathcal{O}}(\mathbf{c}) \le \ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K,T))/\mathcal{O}\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)),$$

and so Theorem 2.2 shows that

$$\ell_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}(K,W^*)) \le \ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K,T))/\mathcal{O}\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)) + \mathfrak{n}_W + \mathfrak{n}^*_W.$$

Together with the equality (1) of Corollary I.7.5, this proves (ii). □

REMARK 2.11. Note that, although a full Euler system is required to prove Theorems 2.2, 2.3, and 2.10, only the class $\mathbf{c}_K$ appears in the statements of those theorems.

REMARK 2.12. The choice of subspace $H^1_f(K_p,V)$ intervenes on both sides of the inequality of Theorem 2.10.

REMARK 2.13. One would like a bound for the order of $\mathcal{S}(K,W^*)$ which involves a value of an appropriate L-function. However, Theorems 2.2 and 2.10 are purely algebraic and never "see" special values of L-functions. One hopes that (as in the examples of Chapter III) these L-values will arise as $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)$ for some Euler system $\mathbf{c}$, and thereby come into the bound for the order of $\mathcal{S}(K,W^*)$ via Theorem 2.10. See Chapter VIII for a discussion of a general framework in which one expects Euler systems which are related to L-values.

3. Results over K_∞

Fix for this section an abelian extension K_∞ of K such that $\mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^d$ for some d and such that no finite prime of K splits completely in K_∞.

Essentially by proving analogues of Theorem 2.2 for each field F, $K \subset_{\mathrm{f}} F \subset K_\infty$, we can pass to the limit and prove an Iwasawa-theoretic version of Theorem 2.2. See [**Lan**] Chapter 5 or [**Wa**] Chapter 13 for basic background on Iwasawa theory, or [**Se1**] for the more general situation of $\mathbf{Z}_p^d$-extensions with $d > 1$.

NOTATION. If $K \subset_{\mathrm{f}} F \subset K_\infty$, we will write $\Lambda_F = \mathcal{O}[\mathrm{Gal}(F/K)]$. Let $\Gamma = \mathrm{Gal}(K_\infty/K)$ and let Λ denote the Iwasawa algebra

$$\Lambda = \mathcal{O}[[\Gamma]] = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} \Lambda_F,$$

so Λ is (noncanonically) isomorphic to a power series ring over $\mathcal{O}$ in d variables, and let $\mathcal{M}$ denote the maximal ideal of Λ.

We say that a Λ-module B is pseudo-null if B is annihilated by an ideal of Λ of height at least two. A pseudo-isomorphism is a Λ-module homomorphism with pseudo-null kernel and cokernel, and two Λ-modules are pseudo-isomorphic if there is a pseudo-isomorphism between them. If B is a finitely generated torsion Λ-module then there is an injective pseudo-isomorphism

$$\bigoplus_i \Lambda/f_i\Lambda \hookrightarrow B$$

with $f_i \in \Lambda$, and we define the characteristic ideal of B

$$\mathrm{char}(B) = \prod_i f_i\Lambda.$$

The characteristic ideal is well-defined, although the individual f_i are not. The individual ideals (elementary divisors) $f_i\Lambda$ are uniquely determined if we add the extra requirement that $f_{i+1} \mid f_i$ for every i. If B is a finitely-generated Λ-module which is not torsion, we define $\mathrm{char}(B) = 0$. If

$$0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$$

is an exact sequence of finitely-generated Λ-modules, then

$$\mathrm{char}(B) = \mathrm{char}(B')\mathrm{char}(B'').$$

We will need the following weak assumption to rule out some very special bad cases. In particular it is satisfied if $K = \mathbf{Q}$.

HYPOTHESIS $\mathrm{Hyp}(K_\infty/K)$. If $\mathrm{rank}_{\mathbf{Z}_p}(\Gamma) = 1$ and G_{K_∞} acts either trivially or by the cyclotomic character on V, then either K is a totally real field and Leopoldt's conjecture holds for K (i.e., the p-adic completion of $\mathcal{O}_K^\times$ injects into $(\mathcal{O}_K \otimes \mathbf{Z}_p)^\times$), or K is an imaginary quadratic field.

We also write $\mathrm{Hyp}(K_\infty, T)$ (resp. $\mathrm{Hyp}(K_\infty, V)$) for hypotheses $\mathrm{Hyp}(K, T)$ (resp. $\mathrm{Hyp}(K, V)$) with G_K replaced by G_{K_∞}:

HYPOTHESES $\mathrm{Hyp}(K_\infty, T)$.

(i) There is a $\tau \in G_{K_\infty}$ such that
- τ acts trivially on $\boldsymbol{\mu}_{p^\infty}$, on $(\mathcal{O}_K^\times)^{1/p^\infty}$, and on $K(1)$,
- $T/(\tau-1)T$ is free of rank one over $\mathcal{O}$.

(ii) $T \otimes \Bbbk$ is an irreducible $\Bbbk[G_{K_\infty}]$-module.

HYPOTHESES $\mathrm{Hyp}(K_\infty, V)$.

(i) There is a $\tau \in G_{K_\infty}$ such that
- τ acts trivially on $\boldsymbol{\mu}_{p^\infty}$, on $(\mathcal{O}_K^\times)^{1/p^\infty}$, and on $K(1)$,
- $\dim_\Phi(V/(\tau-1)V) = 1$.

(ii) V is an irreducible $\Phi[G_{K_\infty}]$-module.

There are simple implications

$$\begin{array}{ccc} \mathrm{Hyp}(K_\infty, T) & \Rightarrow & \mathrm{Hyp}(K_\infty, V) \\ \Downarrow & & \Downarrow \\ \mathrm{Hyp}(K, T) & \Rightarrow & \mathrm{Hyp}(K, V). \end{array}$$

DEFINITION 3.1. Recall that $\mathbf{D} = \Phi/\mathcal{O}$. Define Λ-modules

$$\begin{aligned} \mathcal{S}_{\Sigma_p}(K_\infty, W^*) &= \varinjlim_{K \subset_{\mathrm{f}} F \subset K_\infty} \mathcal{S}_{\Sigma_p}(F, W^*) \\ X_\infty &= \mathrm{Hom}_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*), \mathbf{D}) \\ H^1_\infty(K,T) &= \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T), \end{aligned}$$

limits with respect to restriction and corestriction maps, respectively. If $\mathbf{c}$ is an Euler system let $\mathbf{c}_{K,\infty} = \{\mathbf{c}_F\}_{K \subset_{\mathrm{f}} F \subset K_\infty}$ denote the corresponding element of $H^1_\infty(K,T)$ and define an ideal

$$\mathrm{ind}_\Lambda(\mathbf{c}) = \{\phi(\mathbf{c}_{K,\infty}) : \phi \in \mathrm{Hom}_\Lambda(H^1_\infty(K,T), \Lambda)\} \subset \Lambda.$$

The ideal $\mathrm{ind}_\Lambda(\mathbf{c})$ is the analogue for Λ of the index of divisibility $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ of Definition 2.1.

Recall that $\mathbf{c}$ is an Euler system for (T, K_∞) if it is an Euler system for $(T, \mathcal{K}, \mathcal{N})$ with $K_\infty \subset \mathcal{K}$.

THEOREM 3.2. *Suppose* $\mathbf{c}$ *is an Euler system for* (T, K_∞)*, and* V *satisfies* $\mathrm{Hyp}(K_\infty, V)$*. If* $\mathbf{c}_{K,\infty}$ *does not belong to the* Λ*-torsion submodule of* $H^1_\infty(K,T)$ *then* X_∞ *is a torsion* Λ*-module.*

THEOREM 3.3. *Suppose* $\mathbf{c}$ *is an Euler system for* (T, K_∞)*, and* T *satisfies hypotheses* $\mathrm{Hyp}(K_\infty, T)$ *and* $\mathrm{Hyp}(K_\infty/K)$*. Then*

$$\mathrm{char}(X_\infty) \quad \textit{divides} \quad \mathrm{ind}_\Lambda(\mathbf{c}).$$

THEOREM 3.4. *Suppose* $\mathbf{c}$ *is an Euler system for* (T, K_∞)*, and* V *satisfies hypotheses* $\mathrm{Hyp}(K_\infty, V)$ *and* $\mathrm{Hyp}(K_\infty/K)$*. Then there is a nonnegative integer* t *such that*

$$\mathrm{char}(X_\infty) \quad \textit{divides} \quad p^t \mathrm{ind}_\Lambda(\mathbf{c}).$$

REMARK 3.5. The assertion that X_∞ is a torsion Λ-module is called the weak Leopoldt conjecture for T. See [**Gr2**] or [**PR4**] §1.3 and Appendice B.

REMARK 3.6. As with Theorem 2.2, these three theorems all give bounds for the size of $\mathcal{S}_{\Sigma_p}(K_\infty, W^*)$ rather than the true Selmer group $\varinjlim \mathcal{S}(F, W^*)$. Combining these results with the global duality results from Chapter I §7 gives Theorem 3.8 below concerning the true Selmer group.

Suppose that for every $K \subset_{\mathrm{f}} F \subset K_\infty$ and every prime w dividing p we have subspaces $H^1_f(F_w, V) \subset H^1(F_w, V)$ and $H^1_f(F_w, V^*) \subset H^1(F_w, V^*)$ which are orthogonal complements under the pairing $\langle\ ,\ \rangle_{F_w}$, as in Chapter I §7. We suppose further that if $F \subset F'$ and $w' \mid w$ then

$$\begin{aligned} &\mathrm{Cor}_{F'_{w'}/F_w} H^1_f(F'_{w'}, V) \subset H^1_f(F_w, V), \\ &\mathrm{Res}_{F'_{w'}/F_w} H^1_f(F_w, V^*) \subset H^1_f(F'_{w'}, V^*). \end{aligned}$$

(In fact, the local pairing and our assumptions about orthogonality show that these two inclusions are equivalent.) These conditions ensure that, if $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$, the natural restriction and corestriction maps induce maps

$$\mathcal{S}(F, W^*) \longrightarrow \mathcal{S}(F', W^*), \quad H^1_s(F'_p, T) \longrightarrow H^1_s(F_p, T)$$

where we write

$$H^1(F_p,\,\cdot\,) = \oplus_{w|p} H^1(F_w,\,\cdot\,)$$

and similarly for H^1_f and $H^1_s = H^1/H^1_f$. Define

$$\mathcal{S}(K_\infty, W^*) = \varinjlim_{K \subset_{\mathrm{f}} F \subset K_\infty} \mathcal{S}(F, W^*),$$
$$H^1_{\infty,s}(K_p, T) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1_s(F_p, T).$$

PROPOSITION 3.7. *There is an exact sequence*

$$0 \longrightarrow H^1_{\infty,s}(K_p,T)/\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(K,T)) \longrightarrow \mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(K_\infty,W^*),\mathbf{D}) \longrightarrow X_\infty \longrightarrow 0.$$

where $\mathrm{loc}^s_{\Sigma_p} : H^1_\infty(K,T) \to H^1_{\infty,s}(K_p,T)$ *is the localization map.*

PROOF. By Corollary B.3.4,

$$H^1_\infty(K,T) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} \mathcal{S}^{\Sigma_p}(F,T).$$

Thus the proposition follows from Corollary I.7.5 by passing to the (direct) limit and applying $\mathrm{Hom}_{\mathcal{O}}(\,\cdot\,,\mathbf{D})$. □

THEOREM 3.8. *Suppose* $\mathbf{c}$ *is an Euler system for* (T, K_∞), *and* V *satisfies hypotheses* $\mathrm{Hyp}(K_\infty, V)$ *and* $\mathrm{Hyp}(K_\infty/K)$. *If* $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty}) \notin H^1_{\infty,s}(K_p,T)_{\Lambda-\mathrm{tors}}$ *and* $H^1_{\infty,s}(K_p,T)/\Lambda\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty})$ *is a torsion* Λ*-module, then* $\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(K_\infty,W^*),\mathbf{D})$ *is a torsion* Λ*-module and*

(i) *there is a nonnegative integer* t *such that*

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(K_\infty,W^*),\mathbf{D})) \textit{ divides } p^t\mathrm{char}(H^1_{\infty,s}(K_p,T)/\Lambda\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty})),$$

(ii) *if* T *satisfies* $\mathrm{Hyp}(K_\infty,T)$ *then*

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(K_\infty,W^*),\mathbf{D})) \textit{ divides } \mathrm{char}(H^1_{\infty,s}(K_p,T)/\Lambda\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty})).$$

PROOF. Since $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty}) \notin H^1_{\infty,s}(K_p,T)_{\Lambda-\mathrm{tors}}$, $\mathbf{c}_{K,\infty} \notin H^1_\infty(K,T)_{\Lambda-\mathrm{tors}}$. Therefore Theorem 3.2 shows that X_∞ is a torsion Λ module, and then Proposition 3.7 shows that $\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(K_\infty,W^*),\mathbf{D})$ is a torsion Λ-module and that

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(K_\infty,W^*),\mathbf{D})) = \mathrm{char}(X_\infty)\mathrm{char}(H^1_{\infty,s}(K_p,T)/\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(K,T))).$$

Our assumptions ensure that $\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(K,T))$ is a rank-one Λ-module, so there is a map $\psi : \mathrm{loc}^s_{\Sigma_p}(H^1_\infty(K,T)) \to \Lambda$ with pseudo-null cokernel. Then

$$\begin{aligned}\psi(\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty}))\Lambda &= \mathrm{char}(\psi(\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(K,T)))/\psi(\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty}))\Lambda)\\ &\supset \mathrm{char}(\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(K,T))/\Lambda\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty})),\end{aligned}$$

and by definition $\mathrm{ind}_\Lambda(\mathbf{c})$ divides $\phi \circ \mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{K,\infty})$. The theorem follows easily from these divisibilities and the divisibilities of Theorems 3.4 and 3.3. □

4. Twisting by characters of finite order

Suppose $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$ as defined in Definition 1.1. The consequences of the existence of such an Euler system described in §2 and §3 do not depend on $\mathcal{K}$ (except that, in the case of §3, $\mathcal{K}$ must contain K_∞). We could always take $\mathcal{K}$ to be the "minimal" field $\mathcal{K}_{\min}$ described in Remark 1.4, and ignore the rest of our Euler system, and still obtain the results stated above.

However, there is a way to make use of the additional information contained in an Euler system for a non-minimal $\mathcal{K}$. Namely, in this section we show how to take an Euler system for $(T, \mathcal{K}, \mathcal{N})$ and obtain from it an Euler system for twists $T \otimes \chi$ of T by characters χ of finite order of $\mathrm{Gal}(\mathcal{K}/K)$ (see below). For example, if $\mathcal{K}$ is the maximal abelian extension of K, then we get Euler systems for *all* twists of T by characters of finite order, and the results of this chapter give (possibly trivial) bounds for *all* the corresponding Selmer groups.

Suppose $\chi : G_K \to \mathcal{O}^\times$ is a character of finite order. As in Example I.1.2 we will denote by $\mathcal{O}_\chi$ a free, rank-one $\mathcal{O}$-module on which G_K acts via χ, and we fix a generator ξ_χ of $\mathcal{O}_\chi$ We will write $T \otimes \chi$ for the representation $T \otimes_{\mathcal{O}} \mathcal{O}_\chi$.

Definition 4.1. Suppose $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$ and χ is a character of finite order of $\mathrm{Gal}(\mathcal{K}/K)$ into $\mathcal{O}^\times$. Let $L = \mathcal{K}^{\ker(\chi)}$ be the field cut out by χ. If $K \subset_{\mathrm{f}} F \subset \mathcal{K}$, define $\mathbf{c}_F^\chi \in H^1(F, T \otimes \chi)$ to be the image of $\mathbf{c}_{FL}$ under the composition

$$H^1(FL, T) \xrightarrow{\otimes \xi_\chi} H^1(FL, T) \otimes \mathcal{O}_\chi \cong H^1(FL, T \otimes \chi) \xrightarrow{\mathrm{Cor}} H^1(F, T \otimes \chi)$$

(we get the center isomorphism since G_{FL} is in the kernel of χ).

Proposition 4.2. *Suppose* $\mathbf{c}$ *is an Euler system for* $(T, \mathcal{K}, \mathcal{N})$ *and*

$$\chi : \mathrm{Gal}(\mathcal{K}/K) \to \mathcal{O}^\times$$

is a character of finite order. If $\mathfrak{f}$ *is the conductor of* χ *then the collection*

$$\{\mathbf{c}_F^\chi : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$$

defined above is an Euler system for $(T \otimes \chi, \mathcal{K}, \mathfrak{f}\mathcal{N})$.

Proof. If $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$ then using Definition 1.1

$$\begin{aligned}
\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}^\chi) &= \mathrm{Cor}_{F'L/F}(\mathbf{c}_{F'L} \otimes \xi_\chi) \\
&= \mathrm{Cor}_{FL/F}\left((\mathrm{Cor}_{F'L/FL}\mathbf{c}_{F'L}) \otimes \xi_\chi\right) \\
&= \mathrm{Cor}_{FL/F}\left(\Big(\prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; \mathrm{Fr}_\mathfrak{q}^{-1})\, \mathbf{c}_{FL}\Big) \otimes \xi_\chi\right) \\
&= \mathrm{Cor}_{FL/F}\left(\prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; \chi(\mathrm{Fr}_\mathfrak{q})\mathrm{Fr}_\mathfrak{q}^{-1})(\mathbf{c}_{FL} \otimes \xi_\chi)\right) \\
&= \prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; \chi(\mathrm{Fr}_\mathfrak{q})\mathrm{Fr}_\mathfrak{q}^{-1})\, \mathrm{Cor}_{FL/F}(\mathbf{c}_{FL} \otimes \xi_\chi) \\
&= \prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1}|(T \otimes \chi)^*; \mathrm{Fr}_\mathfrak{q}^{-1})\, \mathbf{c}_F^\chi
\end{aligned}$$

where as usual $P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|(T\otimes\chi)^*;x) = \det(1-\mathrm{Fr}_{\mathfrak{q}}^{-1}x|(T\otimes\chi)^*)$, and

$$\begin{aligned}\Sigma(F'L/FL) &= \{\text{primes } \mathfrak{q} \text{ not dividing } \mathcal{N} : \mathfrak{q} \text{ ramifies in } F'L \text{ but not in } FL\} \\ &= \{\text{primes } \mathfrak{q} \text{ not dividing } \mathfrak{f}\mathcal{N} : \mathfrak{q} \text{ ramifies in } F' \text{ but not in } F\}.\end{aligned}$$

This proves the proposition. □

LEMMA 4.3. *With notation as in Definition* 4.1, *if* $K \subset_{\mathrm{f}} F \subset K_\infty$, $L \subset L' \subset \mathcal{K}$, *and the conductor of* L'/K *is equal to the conductor of* L/K, *then the image of* $\mathbf{c}_F^\chi$ *under the map*

$$H^1(F, T\otimes\chi) \xrightarrow{\mathrm{Res}} H^1(FL', T\otimes\chi) \xrightarrow{\otimes\xi_\chi^{-1}} H^1(FL', T)$$

is

$$\sum_{\delta\in\mathrm{Gal}(FL'/F)} \chi(\delta)\delta\mathbf{c}_{FL'}.$$

PROOF. Since $\mathbf{c}$ is an Euler system, and every prime which ramifies in L'/K ramifies in L/K, we have $\mathrm{Cor}_{FL'/FL}\mathbf{c}_{FL'} = \mathbf{c}_{FL}$. Thus the image of $\mathbf{c}_F^\chi$ under the map above is

$$\begin{aligned}\big(\mathrm{Res}_{FL'/F}\mathrm{Cor}_{FL/F}(\mathbf{c}_{FL}\otimes\xi_\chi)\big)\otimes\xi_\chi^{-1} &= \big(\mathrm{Res}_{FL'/F}\mathrm{Cor}_{FL'/F}(\mathbf{c}_{FL'}\otimes\xi_\chi)\big)\otimes\xi_\chi^{-1} \\ &= \Big(\sum_{\delta\in\mathrm{Gal}(FL'/F)} \delta(\mathbf{c}_{FL'}\otimes\xi_\chi)\Big)\otimes\xi_\chi^{-1} \\ &= \sum_{\delta\in\mathrm{Gal}(FL'/F)} \chi(\delta)\delta\mathbf{c}_{FL'}.\end{aligned}$$

□

CHAPTER III

Examples and Applications

In this chapter we give the basic examples of Euler systems and their applications, using the results of Chapter II.

1. Preliminaries

Suppose χ is a character of G_K into $\mathcal{O}^\times$. As in Example I.1.2 we will denote by $\mathcal{O}_\chi$ a free, rank-one $\mathcal{O}$-module on which G_K acts via χ. Recall that $\mathbf{D} = \Phi/\mathcal{O} = \mathcal{O} \otimes (\mathbf{Q}_p/\mathbf{Z}_p)$, and we also write $\mathbf{D}_\chi = \mathbf{D} \otimes_{\mathcal{O}} \mathcal{O}_\chi = \mathcal{O}_\chi \otimes (\mathbf{Q}_p/\mathbf{Z}_p)$.

For the first three examples (§§2, 3, and 4) we fix a character $\chi : G_K \to \mathcal{O}^\times$ of finite, prime-to-p order into the ring of integers of a finite extension of $\mathbf{Q}_p$. As in Chapter I §6.2 we let $T = \mathcal{O}_\chi$, and then $W = \mathbf{D}_\chi$, $T^* = \mathcal{O}(1) \otimes \mathcal{O}_{\chi^{-1}} = \mathcal{O}_{\chi^{-1}\varepsilon_{\mathrm{cyc}}}$ where $\varepsilon_{\mathrm{cyc}}$ is the cyclotomic character.

Let $L = \bar{K}^{\ker\chi}$ be the abelian extension of K corresponding to χ, so $[L : K]$ is prime to p, and write $\Delta = \mathrm{Gal}(L/K)$. As in Definition I.6.2, if B is a $\mathbf{Z}[\Delta]$-module we write B^χ for the χ-component of $B\hat{\ } \otimes_{\mathbf{Z}_p} \mathcal{O}$ as in Definition I.6.2. We also fix a generator of $\mathcal{O}_{\chi^{-1}}$, and this choice determines an isomorphism $B^\chi \cong (B\hat{\ } \otimes \mathcal{O}_{\chi^{-1}})^\Delta$.

Lemma 1.1. (i) *If $\chi \neq 1$ then $H^1(L(\boldsymbol{\mu}_{p^\infty})/K, W) = 0$.*
(ii) *If χ is not congruent to the cyclotomic character modulo the maximal ideal of $\mathcal{O}$ then $H^1(L(\boldsymbol{\mu}_{p^\infty})/K, W^*) = 0$.*

Proof. Write $\Omega = L(\boldsymbol{\mu}_{p^\infty})$ as in §II.2. Suppose $\rho : G_K \to \mathcal{O}^\times$ is a character. Write $\Bbbk$ for the residue field $\mathcal{O}/\mathfrak{p}$ of $\mathcal{O}$ and $\Bbbk_\rho = \Bbbk \otimes \mathcal{O}_\rho$. Since $|\Delta|$ is prime to p, the inflation-restriction sequence shows that

$$H^1(\Omega/K, \Bbbk_\rho) = \mathrm{Hom}(\mathrm{Gal}(\Omega/L), \Bbbk_\rho)^\Delta = \mathrm{Hom}(\mathrm{Gal}(\Omega/L), \Bbbk_\rho^\Delta)$$

(note that Δ acts trivially on $\mathrm{Gal}(\Omega/L)$ because Ω/K is abelian). Further, if π is a generator of $\mathfrak{p}$, it follows from the exact sequence $0 \to \Bbbk_\rho \to \mathbf{D}_\rho \xrightarrow{\pi} \mathbf{D}_\rho \to 0$ that

$$H^1(\Omega/K, \Bbbk_\rho) = 0 \;\Rightarrow\; H^1(\Omega/K, \mathbf{D}_\rho)_\mathfrak{p} = 0 \;\Rightarrow\; H^1(\Omega/K, \mathbf{D}_\rho) = 0.$$

If ρ is not congruent to 1 modulo $\mathfrak{p}$, then $\Bbbk_\rho^\Delta = 0$ and so $H^1(\Omega/K, \mathbf{D}_\rho) = 0$. Applying this with $\rho = \chi$ proves (i), and with $\rho = \chi^{-1}\varepsilon_{\mathrm{cyc}}$ proves (ii). □

2. Cyclotomic units

The Euler system of cyclotomic units is studied in detail in [**Ko2**] and [**Ru3**].

2.1. An Euler system for $\mathbf{Z}_p(1)$. Take $K = \mathbf{Q}$. For every extension F of $\mathbf{Q}$, as in Example I.2.1 Kummer theory shows that

$$H^1(F, \mathbf{Z}_p(1)) = \varprojlim_n H^1(F, \boldsymbol{\mu}_{p^n}) = \varprojlim_n F^\times/(F^\times)^{p^n} = (F^\times)\hat{} \tag{1}$$

where $(F^\times)\hat{}$ is the p-adic completion of $F^\times$.

Fix a collection $\{\zeta_m : m \geq 1\}$ such that ζ_m is a primitive m-th root of unity and $\zeta_{mn}^n = \zeta_m$ for every m and n. (For example, we could fix an embedding of $\bar{\mathbf{Q}}$ into $\mathbf{C}$ and choose $\zeta_m = e^{2\pi i/m}$.) For every $m \geq 1$ and prime ℓ we have the relation

$$\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}(\boldsymbol{\mu}_m)}(\zeta_{m\ell} - 1) = \begin{cases} (\zeta_m - 1) & \text{if } \ell \mid m \\ (\zeta_m - 1)^{1-\mathrm{Fr}_\ell^{-1}} & \text{if } \ell \nmid m \text{ and } m > 1 \\ (-1)^{\ell-1}\ell & \text{if } m = 1 \end{cases} \tag{2}$$

where Fr_ℓ is the Frobenius of ℓ in $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})$ (see for example [**Lan**] Theorem 6.3.1). For every $m \geq 1$ we define

$$\tilde{\mathbf{c}}_{m\infty} = \mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{mp})/\mathbf{Q}(\boldsymbol{\mu}_m)}(\zeta_{mp} - 1) \in \mathbf{Q}(\boldsymbol{\mu}_m)^\times \subset H^1(\mathbf{Q}(\boldsymbol{\mu}_m), \mathbf{Z}_p(1))$$

and $\tilde{\mathbf{c}}_m = \mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q}(\boldsymbol{\mu}_m)^+}(\tilde{\mathbf{c}}_{m\infty})$. The distribution relation (2) shows that the collection $\{\tilde{\mathbf{c}}_{m\infty}, \tilde{\mathbf{c}}_m\}$ is an Euler system for $(\mathbf{Z}_p(1), \mathbf{Q}^{ab}, p)$ (see Definition II.1.1 and Remark II.1.3), since for every prime $\ell \neq p$,

$$\det(1 - \mathrm{Fr}_\ell^{-1}x | \mathbf{Z}_p(1)^*) = \det(1 - \mathrm{Fr}_\ell^{-1}x | \mathbf{Z}_p) = 1 - x.$$

Remark 2.1. If $p \mid m$ then (2) shows that $\tilde{\mathbf{c}}_{m\infty} = \zeta_m - 1$. But if $p \nmid m$, our definition takes into account that our Euler system must satisfy $\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{mp})/\mathbf{Q}(\boldsymbol{\mu}_m)}\tilde{\mathbf{c}}_{mp} = \tilde{\mathbf{c}}_m$. This causes us to lose some information, and leads to the unwanted hypothesis $\chi(p) \neq 1$ in Theorem 2.3 below. We can remove this hypothesis either by using Theorem 2.10 below (see Remark 2.5) or by modifying the definition of Euler system as in Example IX.1.1.

2.2. The setting. Let $K = \mathbf{Q}$ and $K_\infty = \mathbf{Q}_\infty$, the cyclotomic (and only) $\mathbf{Z}_p$-extension of $\mathbf{Q}$. As in §1 we fix a character $\chi : G_{\mathbf{Q}} \to \mathcal{O}^\times$ of finite, prime-to-p order, and we assume now that χ is even and nontrivial.

Let f denote the conductor of χ, and recall that L is the field cut out by χ. We will view χ as a Dirichlet character modulo f in the usual way, so that $\chi(q) = 0$ if the prime q divides f, and otherwise $\chi(q) = \chi(\mathrm{Fr}_q)$. For every $n \geq 0$ let $\mathbf{Q}_n \subset \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})$ be the extension of degree p^n in $\mathbf{Q}_\infty$, $L_n = L\mathbf{Q}_n$, and $L_\infty = L\mathbf{Q}_\infty$. Since $[L : \mathbf{Q}]$ is prime to p, $L \cap \mathbf{Q}_n = \mathbf{Q}$ for every n and we can identify $\Delta = \mathrm{Gal}(L/\mathbf{Q})$ with

$\mathrm{Gal}(L_n/\mathbf{Q}_n)$ for every n.

$$
\begin{tikzcd}
 & L_\infty \arrow[dl, dash, "\Delta"'] \arrow[ddrr, dash, "p^n\mathbf{Z}_p"] & & & \\
\mathbf{Q}_\infty \arrow[ddrr, dash, "p^n\mathbf{Z}_p"'] & & & & \\
 & & & L_n \arrow[dl, dash, "\Delta"'] \arrow[dr, dash, "\mathbf{Z}/p^n\mathbf{Z}"] & \\
 & & \mathbf{Q}_n \arrow[dr, dash, "\mathbf{Z}/p^n\mathbf{Z}"'] & & L \arrow[dl, dash, "\Delta"'] \\
 & & & \mathbf{Q} &
\end{tikzcd}
$$

Let $T = \mathcal{O}_\chi$ as in §1, so that $T^* = \mathbf{Z}_p(1) \otimes \chi^{-1}$. The restriction map gives an isomorphism (using (1))

$$H^1(\mathbf{Q}_n, T^*) \cong H^1(L_n, T^*)^\Delta \cong (L_n^\times \hat{\otimes} \mathcal{O}_{\chi^{-1}})^\Delta \cong (L_n^\times)^\chi \subset L_n^\times \hat{\otimes} \mathcal{O} \tag{3}$$

where the symbol $\hat{\otimes}$ stands for the (p-adically) completed tensor product.

The Euler system $\tilde{\mathbf{c}}$ for $\mathbf{Z}_p(1)$ constructed in §2.1 gives rise (by Proposition II.4.2) to an Euler system $\mathbf{c} = \tilde{\mathbf{c}}^{\chi^{-1}}$ for $(T^*, \mathbf{Q}^{\mathrm{ab}}, pf)$. By Lemma II.4.3, the image of $\mathbf{c}_\mathbf{Q}$ in $L^\times \hat{\otimes} \mathcal{O}$ under (3) is

$$\prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f)^+/\mathbf{Q})} (\delta \tilde{\mathbf{c}}_f)^{\chi^{-1}(\delta)} = \prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{fp})/\mathbf{Q})} (\zeta_{fp}^\delta - 1)^{\chi^{-1}(\delta)}. \tag{4}$$

2.3. The Selmer group. We have $W = \mathbf{D}_\chi$. Writing $\mathbf{Q}_{n,p}$ for the completion of $\mathbf{Q}_n$ at the unique prime above p, we take $H^1_f(\mathbf{Q}_{n,p}, V) = H^1_{\mathrm{ur}}(\mathbf{Q}_{n,p}, V)$ as in Chapter I §6.2.

For every n let A_n be the ideal class group of L_n. We also write $A_L = A_0$, the ideal class group of L. By Proposition I.6.1 we have isomorphisms

$$\mathcal{S}(\mathbf{Q}, W) \cong \mathrm{Hom}(A_L, \mathbf{D}_\chi)^\Delta, \quad \mathcal{S}(\mathbf{Q}_\infty, W) \cong \mathrm{Hom}(\varprojlim A_n, \mathbf{D}_\chi)^\Delta. \tag{5}$$

2.4. The ideal class group of L.

Definition 2.2. If $n \geq 0$ we let $\mathcal{E}_n$ denote the group of global units of L_n. We define the group of χ-cyclotomic units $\mathcal{C}_{n,\chi}$ to be the subgroup of $\mathcal{E}_n^\chi$ generated over $\mathcal{O}[\mathrm{Gal}(L_n/\mathbf{Q})]$ by

$$\xi_{n,\chi} = \begin{cases} \displaystyle\prod_{\delta \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f)/\mathbf{Q})} (\zeta_f^\delta - 1)^{\chi^{-1}(\delta)} & \text{if } n = 0 \\ \displaystyle\prod_{\delta \in \mathrm{Gal}(\mathbf{Q}_n(\boldsymbol{\mu}_{fp^{n+1}})/\mathbf{Q}_n)} (\zeta_{fp^{n+1}}^\delta - 1)^{\chi^{-1}(\delta)} & \text{if } n > 0. \end{cases}$$

We also will write $\mathcal{E}_L = \mathcal{E}_0$, $\mathcal{C}_{L,\chi} = \mathcal{C}_{0,\chi}$ and $\xi_{L,\chi} = \xi_{0,\chi}$.

The following theorem (actually, its Corollary 2.4) was first proved by Mazur and Wiles [**MW**]; the proof given here is due to Kolyvagin [**Ko2**]. See the additional remarks following the proof.

THEOREM 2.3. *Suppose that $p > 2$ and $\chi(p) \neq 1$. Then*

$$|A_L^\chi| \quad \textit{divides} \quad [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

PROOF. We will apply Theorem II.2.2 with the Euler system $\mathbf{c}$ constructed from cyclotomic units above. Since $\mathrm{rank}_{\mathcal{O}} T^* = 1$, $\mathrm{Hyp}(\mathbf{Q}, T^*)$ is satisfied with $\tau = 1$. Further, in this case $\Omega = L(\boldsymbol{\mu}_{p^\infty})$, and since χ is nontrivial and even, Lemma 1.1 shows that the error terms $\mathfrak{n}_{W^*}$ and $\mathfrak{n}_{W^*}^*$ in Theorem II.2.2 are both zero.

By (3) we have maps

$$\mathcal{E}_L^\chi \hookrightarrow (L^\times)^\chi \xrightarrow{\sim} H^1(\mathbf{Q}, T^*).$$

Identifying $\xi_{L,\chi}$ with its image in $H^1(\mathbf{Q}, T^*)$, it follows from (2) and (4) that

$$\mathbf{c}_{\mathbf{Q}} = \xi_{L,\chi}^{1-\chi^{-1}(p)} \tag{6}$$

where $\chi(p) = 0$ if $p \mid f$. Since $\chi(p) \neq 1$ and χ has order prime to p, $1 - \chi^{-1}(p) \in \mathcal{O}^\times$ so $\mathbf{c}_{\mathbf{Q}}$ generates $\mathcal{C}_{L,\chi}$.

Recall that $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is the index of divisibility defined in Definition II.2.1. Since $L^\times/\mathcal{E}_L$ is torsion-free, it follows that $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is the largest power of p by which a generator of $\mathcal{C}_{L,\chi}$ can be divided in $\mathcal{E}_L^\chi$. Since $p > 2$, χ is even, and $\chi \neq 1$, the Dirichlet unit theorem (see for example [**T5**] §I.4) shows that $\mathcal{E}_L^\chi$ is free of rank one over $\mathcal{O}$, and we conclude

$$\mathrm{ind}_{\mathcal{O}}(\mathbf{c}) = \ell_{\mathcal{O}}(\mathcal{E}_L^\chi / \mathcal{C}_{L,\chi}).$$

Putting all of this together, Theorem II.2.2 in this case gives

$$|\mathcal{S}_{\Sigma_p}(\mathbf{Q}, W)| \quad \text{divides} \quad [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

Let $\mathcal{I}$ denote an inertia group above p and $\mathrm{Fr}_p \in G_{\mathbf{Q}}$ a Frobenius element. By Lemma I.3.2(i),

$$H^1_{\mathrm{ur}}(\mathbf{Q}_p, V) = V^{\mathcal{I}}/(\mathrm{Fr}_p - 1)V^{\mathcal{I}} = V^{\mathcal{I}}/(\chi(p) - 1)V^{\mathcal{I}} = 0$$

since $\chi(p) \neq 1$. Therefore $H^1_f(\mathbf{Q}_p, W) = 0$ and

$$\mathcal{S}_{\Sigma_p}(\mathbf{Q}, W) = \mathcal{S}(\mathbf{Q}, W) = \mathrm{Hom}_{\mathcal{O}}(A_L^\chi, \mathbf{D}),$$

the second equality coming from (5). This completes the proof. □

A well-known argument using the analytic class number formula takes Theorem 2.3 for all such characters χ and gives the following strengthening.

COROLLARY 2.4 (Mazur & Wiles [**MW**] Theorem 1.10.1). *With hypotheses as in Theorem 2.3,*

$$|A_L^\chi| = [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

PROOF. See for example [**Ru3**] Theorem 4.2. □

REMARKS 2.5. When p divides the order of χ, Theorem II.2.2 still applies to give a bound for $\mathcal{S}(\mathbf{Q}, W)$, but (see Proposition I.6.1) this Selmer group is no longer exactly the ideal class group.

When $\chi(p) = 1$, (6) shows that $\mathbf{c}_{\mathbf{Q}} = 0$, so Theorem II.2.2 is of no use. However, in this case Greenberg ([**Gr1**] §5) has shown how to deduce the equality of Corollary

2.4 from Theorem 2.10 below (Iwasawa's "main conjecture") which we will prove below using Theorem II.3.3. See also Chapter IX §1.

Theorem II.3.3 also applies when $p = 2$.

2.5. Inverse limit of the ideal class groups. Recall that Λ is the Iwasawa algebra $\mathcal{O}[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$. For every n let $L_{n,p} = L_n \otimes \mathbf{Q}_p$ and denote by U_n the local units of $L_{n,p}$. Define

$$A_\infty = \varprojlim_n (A_n)\hat{}, \quad \mathcal{E}_\infty = \varprojlim_n (\mathcal{E}_n)\hat{}, \quad \mathcal{C}_{\infty,\chi} = \varprojlim_n (\mathcal{C}_{n,\chi})\hat{},$$
$$U_\infty = \varprojlim_n (U_n)\hat{}, \quad Y_\infty = \varprojlim_n (L_{n,p})\hat{},$$

all inverse limits with respect to norm maps, where $(\,\cdot\,)\hat{}$ denotes p-adic completion (Definition I.6.2). Also let $\mathcal{E}'_n$ denote the group of p-units of L_n (elements which are units at all primes not dividing p) and $\mathcal{E}'_\infty = \varprojlim (\mathcal{E}'_n)\hat{}$. Recall that $H^1_\infty(\mathbf{Q}, T^*) = \varprojlim H^1(\mathbf{Q}_n, T^*)$ and similarly for $H^1_\infty(\mathbf{Q}_p, T^*)$ and $H^1_{\infty,s}(\mathbf{Q}_p, T^*) = \varprojlim H^1(\mathbf{Q}_{n,p}, T^*)/H^1_f(\mathbf{Q}_{n,p}, T^*)$, where $H^1_f(\mathbf{Q}_{n,p}, V^*)$ is defined as in Chapter I §6.3.

PROPOSITION 2.6. (i) *With the natural horizontal inclusions and surjections, there are vertical isomorphisms making the following diagram commute.*

$$\begin{array}{ccccccc}
\Lambda\{\mathbf{c}_{\mathbf{Q}_n}\} & \hookrightarrow & H^1_\infty(\mathbf{Q}, T^*) & \hookrightarrow & H^1_\infty(\mathbf{Q}_p, T^*) & \twoheadrightarrow & H^1_{\infty,s}(\mathbf{Q}_p, T^*) \\
{\scriptstyle\cong}\downarrow & & {\scriptstyle\cong}\downarrow & & {\scriptstyle\cong}\downarrow & & {\scriptstyle\cong}\downarrow \\
\mathcal{C}_{\infty,\chi} & \hookrightarrow & (\mathcal{E}'_\infty)^\chi & \hookrightarrow & Y_\infty^\chi & \twoheadrightarrow & Y_\infty^\chi/U_\infty^\chi.
\end{array}$$

(ii) *There is a Λ-module isomorphism*

$$Y_\infty^\chi/U_\infty^\chi \cong \begin{cases} 0 & \text{if } \chi(p) \neq 1 \\ \mathcal{O} & \text{if } \chi(p) = 1. \end{cases}$$

(iii) *There is a Λ-module injection $(\mathcal{E}'_\infty)^\chi/\mathcal{E}_\infty^\chi \hookrightarrow \mathcal{O}$.*

PROOF. Just as for (4), Lemma II.4.3 shows that the image of $\mathbf{c}_{\mathbf{Q}_n}$ in $(L_n^\times)^\chi$ under (3) is $\xi_{n,\chi}$, so the left-hand vertical isomorphism is clear. As in Chapter I §6.3, the restriction isomorphism (3) identifies

$$\mathcal{S}^{\{p\}}(\mathbf{Q}_n, T^*) \cong (\mathcal{E}'_n)^\chi,$$

and by Corollary B.3.4

$$\varprojlim_n H^1(\mathbf{Q}_n, T^*) = \varprojlim_n \mathcal{S}^{\{p\}}(\mathbf{Q}_n, T^*),$$

so we get the second vertical isomorphism. With H^1_f as defined in Chapter I §6.3, we see as in (7) of §I.6.3 that there are restriction isomorphisms (the top row is the local analogue of (3))

$$\begin{array}{ccc}
H^1(\mathbf{Q}_{n,p}, T^*) & \xrightarrow{\sim} & (L_{n,p}^\times)^\chi \\
\cup & & \cup \\
H^1_f(\mathbf{Q}_{n,p}, T^*) & \xrightarrow{\sim} & U_n^\chi
\end{array}$$

and the rest of the diagram of (i) follows. (Note that once we have the vertical isomorphisms, the injectivity of the upper center horizontal map follows from that of the lower center horizontal map; the latter injectivity follows from Leopoldt's conjecture, which is known in this setting.)

Let Δ_p denote the decomposition group of p in Δ. For every $m > n$ there is a diagram with horizontal isomorphisms

$$\begin{array}{ccccc} L_{m,p}^{\times}/U_m & \xrightarrow[\sim]{\oplus_{w|p}\mathrm{ord}_w} & \bigoplus_{w|p}\mathbf{Z}w & \xrightarrow{\sim} & \mathbf{Z}[\Delta/\Delta_p] \\ {\scriptstyle \mathbf{N}_{L_m/L_n}}\downarrow & & {\scriptstyle w\mapsto w|_{L_n}}\downarrow & & \| \\ L_{n,p}^{\times}/U_n & \xrightarrow[\sim]{\oplus_{v|p}\mathrm{ord}_v} & \bigoplus_{v|p}\mathbf{Z}v & \xrightarrow{\sim} & \mathbf{Z}[\Delta/\Delta_p], \end{array}$$

and so $Y_\infty^\chi/U_\infty^\chi \cong \mathbf{Z}_p[\Delta/\Delta_p]^\chi$. Clearly $\mathbf{Z}_p[\Delta/\Delta_p]^\chi \neq 0$ if and only if χ is trivial on Δ_p, i.e. if and only if $\chi(p) = 1$. This proves (ii), and (iii) follows from (ii) since $\mathcal{E}_\infty^\chi$ is the kernel of the natural map $(\mathcal{E}'_\infty)^\chi \to Y_\infty^\chi/U_\infty^\chi$. □

THEOREM 2.7. $\mathrm{char}(A_\infty^\chi)$ *divides* $\mathrm{char}(\mathcal{E}_\infty^\chi/\mathcal{C}_{\infty,\chi})$.

PROOF. Hypotheses $\mathrm{Hyp}(\mathbf{Q}_\infty, T^*)$ are satisfied with $\tau = 1$, so we can apply Theorem II.3.3 and Proposition II.3.7 to conclude that

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(\mathbf{Q}_\infty, W), \mathbf{D})) \quad \text{divides} \quad \mathrm{ind}_\Lambda(\mathbf{c})\,\mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p, T^*))$$

with $\mathrm{ind}_\Lambda(\mathbf{c})$ as defined in Definition II.3.1. By [**Iw3**] Theorem 25, Y_∞^χ is a torsion-free, finitely-generated, rank-one Λ-module. Since $(\mathcal{E}'_\infty)^\chi$ is a nonzero Λ-submodule of Y_∞^χ, $(\mathcal{E}'_\infty)^\chi$ is also torsion-free, finitely-generated, and rank-one. Combined with the diagram of Proposition 2.6(i), it follows easily that $\mathrm{ind}_\Lambda(\mathbf{c}) = \mathrm{char}((\mathcal{E}'_\infty)^\chi/\mathcal{C}_{\infty,\chi})$, and so using Proposition 2.6(iii)

$$\mathrm{ind}_\Lambda(\mathbf{c}) \quad \text{divides} \quad \mathcal{J}\,\mathrm{char}(\mathcal{E}_\infty^\chi/\mathcal{C}_{\infty,\chi})$$

where $\mathcal{J} = \mathrm{char}(\mathcal{O})$, the augmentation ideal of Λ. By (5), $\mathrm{Hom}_{\mathcal{O}}(\mathcal{S}(\mathbf{Q}_\infty, W), \mathbf{D}) \cong A_\infty^\chi$, and by Proposition 2.6, $\mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p, T^*))$ divides $\mathcal{J}$. Thus we conclude that

$$\mathrm{char}(A_\infty^\chi) \quad \text{divides} \quad \mathcal{J}^2\mathrm{char}(\mathcal{E}_\infty^\chi/\mathcal{C}_{\infty,\chi})$$

so to prove the theorem we need only show that $\mathrm{char}(A_\infty^\chi)$ is not divisible by $\mathcal{J}$.

We only sketch the proof. A standard elementary Iwasawa theory argument (see for example [**Iw3**] §3.1) shows that $A_\infty^\chi/\mathcal{J}A_\infty^\chi$ is a finitely-generated $\mathbf{Z}_p$-module, that

$$\mathcal{J} \mid \mathrm{char}(A_\infty^\chi) \quad \Leftrightarrow \quad A_\infty^\chi/\mathcal{J}A_\infty^\chi \text{ is infinite,}$$

and that $A_\infty^\chi/\mathcal{J}A_\infty^\chi = \mathrm{Gal}(M_\infty/L_\infty)$ where M_∞ is an extension of L_∞ which is abelian over L. Since χ is even, L is a real abelian field, and Leopoldt's conjecture holds for L. Therefore class field theory shows that L has no $\mathbf{Z}_p^2$-extensions, so $\mathrm{Gal}(M_\infty/L)$ has $\mathbf{Z}_p$-rank one and $[M_\infty : L_\infty]$ must be finite. This completes the proof. □

COROLLARY 2.8. $\mathrm{char}(A_\infty^\chi) = \mathrm{char}(\mathcal{E}_\infty^\chi/\mathcal{C}_{\infty,\chi})$.

PROOF. As with Corollary 2.4, this follows from Theorem 2.7 and the analytic class number formula. See for example [**MW**] §1.6, or [**Ru3**] p. 414. □

2.6. The p-adic L-function. Let $\omega : G_{\mathbf{Q}} \to (\mathbf{Z}_p^\times)_{\mathrm{tors}}$ denote the Teichmüller character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$ (if p is odd) or $\boldsymbol{\mu}_4$ (if $p = 2$). Thus $\omega^{-1}\varepsilon_{\mathrm{cyc}}$ is a character of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Fix an embedding of $\mathcal{O} \hookrightarrow \overline{\mathbf{Q}_p} \hookrightarrow \mathbf{C}$ so that we can identify complex and p-adic characters of finite order of $G_{\mathbf{Q}}$. With this identification, a character ρ of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ of finite order extends naturally to an $\mathcal{O}$-algebra homomorphism $\rho : \Lambda \to \overline{\mathbf{Q}_p}$.

THEOREM 2.9. (i) *There is an element $\mathcal{L}_\chi \in \Lambda$ (the p-adic L-function attached to χ) such that for every $k \geq 1$ and every character ρ of finite order of* $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$*,*

$$(\omega^{-1}\varepsilon_{\mathrm{cyc}})^k\rho(\mathcal{L}_\chi) = (1 - \omega^{-k}\rho\chi(p)p^{k-1})L(1-k, \omega^{-k}\rho\chi).$$

(ii) $\mathrm{char}(U_\infty^\chi/\mathcal{C}_{\infty,\chi}) = \mathcal{L}_\chi\Lambda.$

PROOF. See for example [**Iw2**] §6 or [**Wa**] Theorem 7.10 for (i), and [**Iw1**], [**Wa**] Theorem 13.56, [**Lan**] Theorem 7.5.2, or (for the general case) [**Gi**] Théorème 1 for (ii). (See also Appendix D §2 where we carry out the main computation needed to prove (ii).) □

THEOREM 2.10. *Let M_∞ denote the maximal abelian p-extension of L_∞ which is unramified outside primes above p, and let $Z_\infty = \mathrm{Gal}(M_\infty/L_\infty)$. Then Z_∞ is a* $\mathrm{Gal}(L/\mathbf{Q})$*-module and a finitely-generated Λ-module, and*

$$\mathrm{char}(Z_\infty^\chi) = \mathcal{L}_\chi\Lambda$$

where $\mathcal{L}_\chi$ is the p-adic L-function defined in Theorem 2.9.

PROOF. Class field theory gives an exact sequence (see for example §III.1.7 of [**dS**])

$$0 \longrightarrow \mathcal{E}_\infty^\chi/\mathcal{C}_{\infty,\chi} \longrightarrow U_\infty^\chi/\mathcal{C}_{\infty,\chi} \longrightarrow Z_\infty^\chi \longrightarrow A_\infty^\chi \longrightarrow 0.$$

Applying Corollary 2.8 and Theorem 2.9(ii) proves the corollary. □

3. Elliptic units

Let K be an imaginary quadratic field, K_∞ a $\mathbf{Z}_p$- or $\mathbf{Z}_p^2$-extension of K in which no (finite) prime splits completely[1], $\chi : G_K \to \mathcal{O}^\times$ a character of finite order, and $T = \mathcal{O}_\chi$ as above. Using elliptic units in abelian extensions of K, exactly as with cyclotomic units in §2, we can define an Euler system $\mathbf{c}_{\mathrm{ell}}$ for $\mathbf{Z}_p(1)$ over K, from which we get an Euler system for T^*. See [**Ru5**] §1 and §2 for details.

Keep the notation of §2, except that we now for an abelian extension F of K we let $\mathcal{C}_{F,\chi}$ denote elliptic units in $(F^\times)^\chi$ instead of cyclotomic units. Then exactly as in §2, Theorems II.2.2 and II.3.3, respectively, prove the following two theorems (compare with [**Ru5**] Theorems 3.3 and 4.1).

THEOREM 3.1. *Suppose that $p > 2$ and $\chi(\mathfrak{P}) \neq 1$ for all primes $\mathfrak{P}$ of K above p. Then*

$$|A_L^\chi| \quad \textit{divides} \quad [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

[1]In fact, this splitting condition is unnecessary; see Chapter IX §2,

THEOREM 3.2. *If $\chi(\mathfrak{P}) \neq 1$ for all primes $\mathfrak{P}$ of K above p, then*

$$\operatorname{char}(\varprojlim A_F^\chi) \quad \textit{divides} \quad \operatorname{char}(\varprojlim \mathcal{E}_F^\chi/\mathcal{C}_{F,\chi}).$$

where the inverse limits are over finite extensions F of L in LK_∞.

REMARKS 3.3. As with cyclotomic units, one can use the analytic class number formula to turn the divisibility of Theorem 3.1 into an equality.

One can remove the hypothesis that $\chi(\mathfrak{P}) \neq 1$ from Theorem 3.2 by modifying the definition of an Euler system. See Chapter IX §1.

4. Stickelberger elements

The Euler system we present in this section is not the same as the Euler system of Gauss sums introduced by Kolyvagin in [**Ko2**] (see also [**Ru4**]), but it has the same applications to ideal class groups. We will use Stickelberger's theorem in the construction of our Euler system, so Gauss sums are implicitly being used.

DEFINITION 4.1. For every integer $m \geq 2$, define the Stickelberger element

$$\theta_m = \sum_{a \in (\mathbf{Z}/m\mathbf{Z})^\times} \left(\frac{\langle a \rangle}{m} - \frac{1}{2} \right) \gamma_a^{-1} \in \mathbf{Q}[\operatorname{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})]$$

where $0 \leq \langle a \rangle < m$, $\langle a \rangle \equiv a \pmod{m}$, and $\gamma_a \in \operatorname{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})$ is the automorphism which sends every m-th root of unity to its a-th power. Also define $\theta_1 = 0$. It is well-known (and easy to check; see for example [**Wa**] Lemma 6.9 or [**Lan**] §2.8) that

$$\text{if } b \in \mathbf{Z} \text{ is prime to } 2m, \text{ then } (b - \gamma_b)\theta_m \in \mathbf{Z}[\operatorname{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})] \tag{7}$$

and if ℓ is prime,

$$\theta_{m\ell} \mid_{\mathbf{Q}(\boldsymbol{\mu}_m)} = \begin{cases} (1 - \operatorname{Fr}_\ell^{-1})\theta_m & \text{if } \ell \nmid m \\ \theta_m & \text{if } \ell \mid m. \end{cases} \tag{8}$$

4.1. An Euler system for $\mathbf{Z}_p$. Again we take $K = \mathbf{Q}$. For every finite extension F of $\mathbf{Q}$, class field theory shows that

$$H^1(F, \mathbf{Z}_p) = \operatorname{Hom}(G_F, \mathbf{Z}_p) = \operatorname{Hom}(\mathbf{A}_F^\times/F^\times, \mathbf{Z}_p) = \operatorname{Hom}(\mathbf{A}_F^\times/(F^\times B_F), \mathbf{Z}_p) \tag{9}$$

where $\mathbf{A}_F^\times$ denotes the group of ideles of F and

$$B_F = \prod_{w \mid \infty} F_w^\times \times \prod_{w \mid p} \{1\} \times \prod_{w \nmid p\infty} \mathcal{O}_{F,w}^\times \subset \mathbf{A}_F^\times,$$

since any (continuous) homomorphism into $\mathbf{Z}_p$ must vanish on B_F. Further, the map which sends an idele to the corresponding ideal class induces an exact sequence

$$0 \longrightarrow U_F/\bar{\mathcal{E}}_F \longrightarrow \mathbf{A}_F^\times/(F^\times B_F) \longrightarrow A_F \longrightarrow 0 \tag{10}$$

where U_F denotes the local units of $F \otimes \mathbf{Q}_p$, $\bar{\mathcal{E}}_F$ is the closure of the global units of F in U_F, and A_F is the ideal class group of F. We will write $\mathbf{Z}_p[\boldsymbol{\mu}_m]^\times = U_{\mathbf{Q}(\boldsymbol{\mu}_m)}$.

DEFINITION 4.2. Fix an integer b prime to $2p$ (a precise choice will be made later), and for every $m \geq 1$ prime to b we use the Stickelberger elements above to define

$$\bar{\theta}_m^{(b)} = \begin{cases} (b-\gamma_b)\theta_m & \text{if } p \mid m \\ (b-\gamma_b)(1-\mathrm{Fr}_p^{-1})\theta_m & \text{if } p \nmid m \end{cases} \in \mathbf{Z}[\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})]$$

(the two separate cases are to ensure, using (8), that $\bar{\theta}_{mp}^{(b)} \mid_{\mathbf{Q}(\boldsymbol{\mu}_m)} = \bar{\theta}_m^{(b)}$ for every m). Stickelberger's Theorem (see for example [**Wa**] Theorem 6.10 or [**Lan**] Theorem 1.2.3) shows that $\bar{\theta}_m^{(b)} A_{\mathbf{Q}(\boldsymbol{\mu}_m)} = 0$. Thus, using (10) we can view (multiplication by) $\bar{\theta}_m^{(b)}$ as a map

$$\mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_m)}^{\times}/(\mathbf{Q}(\boldsymbol{\mu}_m)^{\times} B_{\mathbf{Q}(\boldsymbol{\mu}_m)}) \longrightarrow \mathbf{Z}_p[\boldsymbol{\mu}_m]^{\times}/\bar{\mathcal{E}}_{\mathbf{Q}(\boldsymbol{\mu}_m)},$$

and we define $\phi_m = \phi_m^{(b)} \in \mathrm{Hom}(\mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_m)}^{\times}/(\mathbf{Q}(\boldsymbol{\mu}_m)^{\times} B_{\mathbf{Q}(\boldsymbol{\mu}_m)}), \mathbf{Z}_p)$ to be the composition

$$\begin{aligned} \mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_m)}^{\times}/(\mathbf{Q}(\boldsymbol{\mu}_m)^{\times} B_{\mathbf{Q}(\boldsymbol{\mu}_m)}) &\xrightarrow{\bar{\theta}_m^{(b)}} \mathbf{Z}_p[\boldsymbol{\mu}_m]^{\times}/\bar{\mathcal{E}}_{\mathbf{Q}(\boldsymbol{\mu}_m)} \\ &\xrightarrow{1-c} \mathbf{Z}_p[\boldsymbol{\mu}_m]^{\times}/(\mathbf{Z}_p[\boldsymbol{\mu}_m]^{\times})_{\mathrm{tors}} \xrightarrow{\lambda_m} \mathbf{Z}_p \end{aligned}$$

where c denotes complex conjugation in $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})$, so $(1-c)\bar{\mathcal{E}}_{\mathbf{Q}(\boldsymbol{\mu}_m)}$ is finite, and λ_m is the map defined in Appendix D, Definition D.1.2. Finally, we define $\tilde{\mathbf{c}}'_m \in H^1(\mathbf{Q}(\boldsymbol{\mu}_m), \mathbf{Z}_p)$ to be the element corresponding to ϕ_m under (9).

PROPOSITION 4.3. *Suppose m is prime to b and ℓ is a prime not dividing b. Then*

$$\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}(\boldsymbol{\mu}_m)}(\tilde{\mathbf{c}}'_{m\ell}) = \begin{cases} (1-\mathrm{Fr}_\ell^{-1})\tilde{\mathbf{c}}'_m & \text{if } \ell \nmid mp \\ \tilde{\mathbf{c}}'_m & \text{if } \ell \mid mp. \end{cases}$$

PROOF. It follows from a standard result of class field theory (for example [**T2**] §11(13)) that, with the identification (9), the map $\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}(\boldsymbol{\mu}_m)}$ is induced by the inclusion $\mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_m)}^{\times} \hookrightarrow \mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})}^{\times}$.

Suppose first that $\ell \nmid mp$. By Lemma D.1.4, $\lambda_{m\ell}|_{\mathbf{Z}_p[\boldsymbol{\mu}_m]^{\times}} = \lambda_m \circ (-\mathrm{Fr}_\ell)$, and by (8), $\bar{\theta}_{m\ell}^{(b)} \mid_{\mathbf{Q}(\boldsymbol{\mu}_m)} = (1-\mathrm{Fr}_\ell^{-1})\bar{\theta}_m^{(b)}$. Therefore

$$\phi_{m\ell}|_{\mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_m)}^{\times}} = \phi_m \circ (-\mathrm{Fr}_\ell)(1-\mathrm{Fr}_\ell^{-1}) = \phi_m \circ (1-\mathrm{Fr}_\ell) = (1-\mathrm{Fr}_\ell^{-1})\phi_m$$

and hence $\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}(\boldsymbol{\mu}_m)}(\tilde{\mathbf{c}}'_{m\ell}) = (1-\mathrm{Fr}_\ell^{-1})\tilde{\mathbf{c}}'_m$. Similarly (but more simply), if ℓ divides mp then Lemma D.1.4 and (8) show that $\phi_{m\ell}|_{\mathbf{A}_{\mathbf{Q}(\boldsymbol{\mu}_m)}^{\times}} = \phi_m$ and then $\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}(\boldsymbol{\mu}_m)}(\tilde{\mathbf{c}}'_{m\ell}) = \tilde{\mathbf{c}}'_m$. □

REMARK 4.4. Technically we should write $\tilde{\mathbf{c}}'_{m\infty}$ instead of $\tilde{\mathbf{c}}'_m$, since the ray class field of $\mathbf{Q}$ modulo m is $\mathbf{Q}(\boldsymbol{\mu}_m)^+$. But

$$\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q}(\boldsymbol{\mu}_m)^+}(\tilde{\mathbf{c}}'_m) = 0 \in H^1(\mathbf{Q}(\boldsymbol{\mu}_m)^+, \mathbf{Z}_p)$$

(because we annihilated all even components in our definition), so we will never need to deal with those classes and there should be no confusion.

For every prime $\ell \neq p$,

$$\det(1 - \mathrm{Fr}_\ell^{-1} x | \mathbf{Z}_p^*) = \det(1 - \mathrm{Fr}_\ell^{-1} x | \mathbf{Z}_p(1)) = 1 - \ell^{-1} x.$$

But Proposition 4.3 shows that the collection $\{\tilde{\mathbf{c}}'_m \in H^1(\mathbf{Q}(\boldsymbol{\mu}_m), \mathbf{Z}_p)\}$ satisfies a distribution relation with polynomials $1 - \mathrm{Fr}_\ell^{-1}$, not $1 - \ell^{-1}\mathrm{Fr}_\ell^{-1}$, so this collection is *not* an Euler system for the trivial representation $\mathbf{Z}_p$. However, since

$$1 - \ell^{-1} x \equiv 1 - x \pmod{(\ell - 1)\mathbf{Z}_p[x]}$$

we can modify the classes $\tilde{\mathbf{c}}'_m$ (see Lemma IX.6.1 and Example IX.6.2) to produce a new collection

$$\{\tilde{\mathbf{c}}_m \in H^1(\mathbf{Q}(\boldsymbol{\mu}_m), \mathbf{Z}_p) : m > 1, (m, b) = 1\}$$

which *is* an Euler system for $(\mathbf{Z}_p, \mathbf{Q}^{\mathrm{ab},b}, bp)$, where $\mathbf{Q}^{\mathrm{ab},b}$ denotes the maximal abelian extension of $\mathbf{Q}$ unramified outside b. Further, we have $\tilde{\mathbf{c}}_{p^n} = \tilde{\mathbf{c}}'_{p^n}$ for every n. Note that this Euler system still depends on the choice of b.

4.2. The setting. As in §2 let $K = \mathbf{Q}$, $T = \mathcal{O}_\chi$ for a character χ of finite, prime-to-p order of G_K, and we keep the rest of the notation of the beginning of §2 as well. We now assume that χ is odd, and we let b be a nonzero integer prime to $2p$ and to the conductor f of χ. (A precise choice of b will be made later.)

Let $\Delta = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f)/\mathbf{Q})$. Since χ is nontrivial and of order prime to p, $H^i(\Delta, \mathcal{O}_\chi) = 0$ for every $i \geq 0$. Therefore the restriction map gives an isomorphism (compare with (9))

$$\begin{aligned} H^1(\mathbf{Q}_n, T) &= H^1(\mathbf{Q}_n(\boldsymbol{\mu}_f), \mathcal{O}_\chi)^\Delta \\ &\cong \mathrm{Hom}(\mathbf{A}^\times_{\mathbf{Q}_n(\boldsymbol{\mu}_f)}/\mathbf{Q}_n(\boldsymbol{\mu}_f)^\times, \mathcal{O}_\chi)^\Delta \subset \mathrm{Hom}(\mathbf{A}^\times_{\mathbf{Q}_n(\boldsymbol{\mu}_f)}, \mathcal{O}), \end{aligned} \tag{11}$$

the inclusion using our fixed generator of $\mathcal{O}_\chi$. The Euler system $\tilde{\mathbf{c}}$ for $\mathbf{Z}_p$ constructed in §4.1 gives rise (by Proposition II.4.2) to an Euler system $\mathbf{c} = \tilde{\mathbf{c}}^\chi$ for $(T, \mathbf{Q}^{\mathrm{ab},b}, bfp)$. By Lemmas II.4.3 and IX.6.1(iii), the image under (11) of $\mathbf{c}_\mathbf{Q}$ in $\mathrm{Hom}(\mathbf{A}^\times_{\mathbf{Q}(\boldsymbol{\mu}_f)}, \mathcal{O})$ is

$$\sum_{\delta \in \Delta} \chi(\delta)\delta\tilde{\mathbf{c}}_f = \sum_{\delta \in \Delta} \chi(\delta)\delta\tilde{\mathbf{c}}'_f = \sum_{\delta \in \Delta} \chi(\delta)\phi_f^\delta. \tag{12}$$

4.3. The Selmer group. We have $W^* = \mathbf{D}_{\chi^{-1}\varepsilon_{\mathrm{cyc}}}$. As in §2.2, let L be the fixed field of the kernel of χ, $L_n = L\mathbf{Q}_n$, $\mathbf{Q}_{n,p}$ the completion of $\mathbf{Q}_n$ above p, A_n the ideal class group of L_n, and $A_L = A_0$, the ideal class group of L.

We take $H^1_f(\mathbf{Q}_{n,p}, V)$ and $H^1_f(\mathbf{Q}_{n,p}, V^*)$ to be as defined in Chapter I §6.2 and §6.3, respectively.

Proposition 4.5. (i) $\mathcal{S}(\mathbf{Q}, W^*) \cong A_L^\chi$,
(ii) $\mathcal{S}(\mathbf{Q}_\infty, W^*) \cong \varinjlim_n A_n^\chi$.

Proof. Let $\mathcal{E}_n$ denote the group of global units of L_n. Since χ is odd, $\mathcal{E}_n^\chi$ is finite so $(\mathcal{E}_n \otimes \mathbf{Q}_p/\mathbf{Z}_p)^\chi = 0$. Now the proposition follows from Proposition I.6.3(ii). $\square$

4.4. The minus part of the ideal class group of L. The following theorem (or more precisely, its Corollary 4.7) was first proved by Mazur and Wiles in [**MW**]. A proof using Euler systems, but somewhat different from the one here, was given by Kolyvagin in [**Ko2**], see also [**Ru4**].

Define the generalized Bernouilli number

$$\mathbf{B}_{1,\chi^{-1}} = \frac{1}{f}\sum_{a=1}^{f}\chi^{-1}(a)a = \chi(\theta_f).$$

Recall $\omega : G_{\mathbf{Q}} \to (\mathbf{Z}_p^\times)_{\mathrm{tors}}$ is the Teichmüller character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$ (if p is odd) or $\boldsymbol{\mu}_4$ (if $p=2$).

THEOREM 4.6. *Suppose that $p>2$, $\chi(p)\neq 1$, and $\chi^{-1}\omega(p)\neq 1$. Then*

$$|A_L^\chi| \le |\mathcal{O}/\mathbf{B}_{1,\chi^{-1}}\mathcal{O}|.$$

PROOF. Since $\chi\neq\omega$, we can choose b prime to $2pf$ so that $b-\chi(b)\in\mathcal{O}^\times$. Let $\mathbf{c}$ be the Euler system for T constructed above from Stickelberger elements, with this choice of b.

Since T has rank one over $\mathcal{O}$, $\mathrm{Hyp}(\mathbf{Q},T)$(i) and (ii) are satisfied with $\tau=1$, so we can apply Theorem II.2.10 with this Euler system.

As in the proof of Theorem 2.3, since χ is odd and different from ω, Lemma 1.1 shows that $\mathfrak{n}_W=\mathfrak{n}_W^*=0$ in Theorem II.2.2.

Using the definition of H^1_f in Chapter I §6.2 and local class field theory, we have identifications (the top row is the local analogue of (11))

$$\begin{array}{ccccc}
H^1(\mathbf{Q}_p,T) & \xrightarrow{\sim} & \mathrm{Hom}(\oplus_{w\mid p}G_{\mathbf{Q}(\boldsymbol{\mu}_f)_w},\mathcal{O}_\chi)^\Delta & \xrightarrow{\sim} & \mathrm{Hom}(\mathbf{Q}_p(\boldsymbol{\mu}_f)^\times,\mathcal{O}_\chi)^\Delta \\
\downarrow & & \downarrow & & \downarrow \\
H^1_s(\mathbf{Q}_p,T) & \xrightarrow{\sim} & \mathrm{Hom}(\oplus_{w\mid p}\mathcal{I}_w,\mathcal{O}_\chi)^\Delta & \xrightarrow{\sim} & \mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times,\mathcal{O}_\chi)^\Delta
\end{array}$$

where $\mathbf{Q}_p(\boldsymbol{\mu}_f)=\mathbf{Q}(\boldsymbol{\mu}_f)\otimes\mathbf{Q}_p$ and $\mathcal{I}_w$ is the inertia group in G_{L_w}. Thus

$$H^1_s(\mathbf{Q}_p,T)\cong\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times,\mathcal{O}_\chi)^\Delta\cong\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times,\mathcal{O})^{\chi^{-1}}. \tag{13}$$

With this identification, using (12) and Definition 4.2 of $\bar\theta_f^{(b)}$,

$$\begin{aligned}
\mathrm{loc}^s_{\{p\},T}(\mathbf{c}_{\mathbf{Q}}) &= \sum_{\delta\in\Delta}\chi(\delta)(\lambda_f\circ\bar\theta_f^{(b)})^\delta \\
&= \sum_{\delta\in\Delta}\chi(\delta)(\lambda_f\circ\delta^{-1}\bar\theta_f^{(b)}) \\
&= \lambda_f\circ\sum_{\delta\in\Delta}(\chi(\delta)\delta^{-1})\bar\theta_f^{(b)} \\
&= (b-\chi(b))(1-\chi^{-1}(p))\mathbf{B}_{1,\chi^{-1}}\sum_{\delta\in\Delta}\chi(\delta)\lambda_f^\delta.
\end{aligned}$$

Since $\chi^{-1}\omega(p)\neq 1$, Lemma D.1.5 shows that $\sum_{\delta\in\Delta}\chi(\delta)\lambda_f^\delta$ generates the (free, rank-one) $\mathcal{O}$-module $\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times,\mathcal{O})^{\chi^{-1}}$. We chose b so that $b-\chi(b)\in\mathcal{O}^\times$, and we assumed that $\chi(p)\neq 1$ and χ has order prime to p, so $1-\chi(p)\in\mathcal{O}^\times$. Thus (13) shows that

$$\mathcal{O}\mathrm{loc}^s_{\{p\},T}(\mathbf{c}_{\mathbf{Q}})=\mathbf{B}_{1,\chi^{-1}}H^1_s(\mathbf{Q}_p,T).$$

Now Theorem II.2.10 yields

$$|\mathcal{S}(\mathbf{Q}, W^*)| \le [H^1_s(\mathbf{Q}_p, T) : \mathbf{B}_{1,\chi^{-1}} H^1_s(\mathbf{Q}_p, T)] = |\mathcal{O}/\mathbf{B}_{1,\chi^{-1}}\mathcal{O}|. \qquad \square$$

COROLLARY 4.7 (Mazur & Wiles [**MW**] Theorem 1.10.2). *With hypotheses as in Theorem* 4.6*,*

$$|A_L^\chi| = |\mathcal{O}/\mathbf{B}_{1,\chi^{-1}}\mathcal{O}|.$$

PROOF. As in Corollary 2.4, this follows from Theorem 4.6 by the usual analytic class number formula argument. See for example [**Ru4**] Theorem 4.3. $\square$

REMARKS 4.8. If $\chi = \omega$ then it is well-known that $A_L^\chi = 0$ (and $\mathbf{B}_{1,\chi^{-1}}\mathcal{O} = p^{-1}\mathcal{O}$).

If $\chi(p) = 1$, or $\chi^{-1}\omega(p) = 1$ but $\chi \ne \omega$, the equality of Corollary 4.7 can be deduced from Theorem 4.13 below (Iwasawa's "main conjecture"). See [**MW**], §1.10 Theorem 2. See also Chapter IX §1.

4.5. The p-adic L-function. There is a natural map

$$\chi_\Lambda : \mathcal{O}[[\mathrm{Gal}(\mathbf{Q}_\infty(\boldsymbol{\mu}_f)/\mathbf{Q})]] = \mathcal{O}[\Delta][[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]] \xrightarrow{\chi} \Lambda$$

given by χ on Δ and the identity on $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Let

$$\langle\varepsilon\rangle = \omega^{-1}\varepsilon_{\mathrm{cyc}} : \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \to 1 + p\mathbf{Z}_p,$$

let $\mathrm{Tw}_{\langle\varepsilon\rangle} : \Lambda \to \Lambda$ be the twisting map induced by

$$\gamma \mapsto \langle\varepsilon\rangle(\gamma)\gamma$$

for $\gamma \in \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$, and let $\eta \mapsto \eta^\bullet$ denote the involution of Λ induced by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$.

Write $\boldsymbol{\theta}_{fp^\infty} = \{\theta_{fp^{n+1}}\}_n$. If b is prime to $2fp$ then by (7) and (8),

$$(b - \gamma_b)\boldsymbol{\theta}_{fp^\infty} \in \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{fp^\infty})/\mathbf{Q})]],$$

and so by restriction we have $\chi_\Lambda((b-\gamma_b)\boldsymbol{\theta}_{fp^\infty}) \in \Lambda$. If $\chi \ne \omega$ then we can fix b so that $b - \chi(b) \in \mathcal{O}^\times$, and then $\chi_\Lambda(b - \gamma_b) \in \Lambda^\times$. We will write

$$\chi_\Lambda(\boldsymbol{\theta}_{fp^\infty}) = \chi_\Lambda(b-\gamma_b)^{-1}\chi_\Lambda((b-\gamma_b)\boldsymbol{\theta}_{fp^\infty}) \in \Lambda$$

which is independent of b.

THEOREM 4.9. *If* $\chi \ne \omega$ *then*

$$\chi_\Lambda(\boldsymbol{\theta}_{fp^\infty})^\bullet = \mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega})$$

where $\mathcal{L}_{\chi^{-1}\omega}$ *is the* p*-adic* L*-function defined in Theorem* 2.9 *for the even character* $\chi^{-1}\omega$*.*

PROOF. This was proved by Iwasawa; see [**Iw2**] §6 or [**Wa**] Theorem 7.10. If ρ is a character of finite order of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$, it follows from the definitions that

$$\begin{aligned}\rho(\chi_\Lambda(\boldsymbol{\theta}_{fp^\infty})^\bullet) &= \rho^{-1}(\chi_\Lambda(\boldsymbol{\theta}_{fp^\infty})) = (1-\chi^{-1}\rho(p))\mathbf{B}_{1,\chi^{-1}\rho} \\ &= (1-\chi^{-1}\rho(p))L(0,\chi^{-1}\rho) = \langle\varepsilon\rangle\rho(\mathcal{L}_{\chi^{-1}\omega}) = \rho(\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega})).\end{aligned}$$

Since this is true for every ρ, the equality of the theorem holds. $\square$

4.6. Direct limit of the ideal class groups. The main result of this section, Theorem 4.13 below, is equivalent to Theorem 2.10 by standard methods of Iwasawa theory (see for example [**Ru3**] §8), so we will only sketch the proof.

Let $\mathcal{U}$ denote the direct limit (not the inverse limit) of the local units of $\mathbf{Q}_n(\boldsymbol{\mu}_f) \otimes \mathbf{Q}_p$. Recall that $\Delta = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f)/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{Q}_n(\boldsymbol{\mu}_f)/\mathbf{Q}_n)$.

LEMMA 4.10. *There is an isomorphism of Λ-modules*

$$\mathrm{Hom}(\mathcal{U}, \mathcal{O}_\chi)^\Delta \cong \begin{cases} \Lambda & \text{if } \chi(p) \neq 1 \\ \Lambda \oplus \mathcal{O} & \text{if } \chi(p) = 1. \end{cases}$$

SKETCH OF PROOF. Let Y_∞ denote the inverse limit of the p-adic completions of the multiplicative groups $\mathbf{Q}_p(\boldsymbol{\mu}_{fp^n})^\times$. There is a natural Kummer pairing

$$\mathcal{U} \times Y_\infty \to \mathbf{Z}_p(1)$$

which leads to a Λ-module isomorphism

$$(Y_\infty \otimes \mathcal{O}_{\chi\omega^{-1}})^{\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f, \boldsymbol{\mu}_p)/\mathbf{Q})} \cong \mathrm{Hom}(\mathcal{U}, \mathcal{O}_\chi)^\Delta \otimes \mathcal{O}_{\langle\varepsilon\rangle}.$$

The lemma then follows from a result of Iwasawa ([**Iw3**] Theorem 25; see also [**Gi**] Proposition 1). □

COROLLARY 4.11. *Suppose $\chi \neq \omega$. Then we can choose b so that, if $\mathbf{c}$ is the Euler system of* §4.2, *then the characteristic ideal* $\mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p, T)/\Lambda \mathrm{loc}^s_{\{p\}}(\{\mathbf{c}_{\mathbf{Q}_n}\}_n))$ *is*

$$\begin{cases} \mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega}) & \text{if } \chi^{-1}\omega(p) \neq 1, \chi(p) \neq 1 \\ \mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{J}\mathcal{L}_{\chi^{-1}\omega}) & \text{if } \chi^{-1}\omega(p) = 1 \\ \mathcal{J}\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega}) & \text{if } \chi(p) = 1 \end{cases}$$

where $\mathcal{J}$ is the augmentation ideal of Λ.

SKETCH OF PROOF. For every n, exactly as in (13) we have

$$H^1_s(\mathbf{Q}_{n,p}, T) = \mathrm{Hom}(U_n, \mathcal{O}_\chi)^\Delta$$

and so $H^1_{\infty,s}(\mathbf{Q}_p, T) = \mathrm{Hom}(\mathcal{U}, \mathcal{O}_\chi)^\Delta$. Let

$$\lambda_{fp^\infty,\chi} = \lim_{n\to\infty} \sum_{\delta\in\Delta} \chi(\delta)\lambda^\delta_{fp^n} \in \mathrm{Hom}(\mathcal{U}, \mathcal{O}_\chi)^\Delta$$

One computes, using Lemma 4.10, that there are Λ-module isomorphisms

$$\mathrm{Hom}(\mathcal{U}, \mathcal{O}_\chi)^\Delta/\Lambda\lambda_{fp^\infty,\chi} \cong \begin{cases} 0 & \text{if } \chi^{-1}\omega(p) \neq 1, \chi(p) \neq 1 \\ \mathcal{O}_{\langle\varepsilon\rangle} & \text{if } \chi^{-1}\omega(p) = 1 \\ \mathcal{O} & \text{if } \chi(p) = 1. \end{cases}$$

(The first case follows from Lemma D.1.5; the others require more work.) Also, by definition of $\mathbf{c}_{\mathbf{Q}_n}$ and Lemma II.4.3

$$\mathrm{loc}^s_{\{p\}}(\mathbf{c}_{\mathbf{Q}_n}) = \sum_{\delta\in\Delta} \chi(\delta)\lambda_{fp^{n+1}} \circ (b - \gamma_b)\theta_{fp^{n+1}}.$$

Thus

$$\begin{aligned}\Lambda\mathrm{loc}^s_{\{p\}}(\{\mathbf{c}_{\mathbf{Q}_n}\}_n) &= \Lambda\lambda_{fp^\infty,\chi}\circ(\chi_\Lambda(b-\gamma_b)\chi_\Lambda(\boldsymbol{\theta}_{fp^\infty}))\\ &= \chi_\Lambda(b-\gamma_b)^\bullet\chi_\Lambda(\boldsymbol{\theta}_{fp^\infty})^\bullet\Lambda\lambda_{fp^\infty,\chi}\\ &= \chi_\Lambda(\boldsymbol{\theta}_{fp^\infty})^\bullet\Lambda\lambda_{fp^\infty,\chi}\end{aligned}$$

Since b was chosen so that $\chi_\Lambda(b-\gamma_b)\in\Lambda^\times$. Now the corollary follows from Theorem 4.9. □

THEOREM 4.12. *If χ is an odd character of order prime to p and $\chi\neq\omega$ then*

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))\quad \textit{divides}\quad \mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega}).$$

SKETCH OF PROOF. Since T has rank one over $\mathcal{O}$, $\mathrm{Hyp}(\mathbf{Q},T)$(i) and (ii) are satisfied with $\tau=1$. Thus we can apply Theorem II.3.8(ii), and we conclude (using Proposition 4.5(ii) to identify the Selmer group with the direct limit of the ideal class groups) that

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))\quad\text{divides}\quad \mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p,T)/\Lambda\mathrm{loc}^s_{\{p\}}(\{\mathbf{c}_{\mathbf{Q}_n}\}_n)).$$

If $\chi(p)\neq 1$ and $\chi^{-1}\omega(p)\neq 1$, the theorem now follows immediately from Corollary 4.11.

The two exceptional cases remain. First suppose that $\chi^{-1}\omega(p)=1$. In this case we conclude from Corollary 4.11 that $\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))$ divides $\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{J}\mathcal{L}_{\chi^{-1}\omega})$, so to complete the proof it will suffice to show that $\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{J})$ cannot divide $\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))$.

Briefly, if $\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{J})$ divides $\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))$ then class field theory and Kummer theory show (see for example [**Lan**] Chapter 6 or [**Wa**] §13.5) that there is a divisible subgroup of $\mathbf{Q}(\boldsymbol{\mu}_f,\boldsymbol{\mu}_p)^\times\otimes(\mathbf{Q}_p/\mathbf{Z}_p)$ which generates an unramified extension of $\mathbf{Q}(\boldsymbol{\mu}_{fp^\infty})$. But this would contradict Leopoldt's conjecture, which holds for $\mathbf{Q}(\boldsymbol{\mu}_f,\boldsymbol{\mu}_p)$.

Now suppose $\chi(p)=1$. In this case, if χ_0 denotes the trivial character then the definition (Theorem 2.9) of $\mathcal{L}_{\chi^{-1}\omega}$ shows that

$$\chi_0(\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega}))=\langle\varepsilon\rangle(\mathcal{L}_{\chi^{-1}\omega})=\omega^{-1}\varepsilon_{\mathrm{cyc}}(\mathcal{L}_{\chi^{-1}\omega})=(1-\chi(p))L(0,\chi)=0.$$

In other words, $\mathcal{J}$ divides $\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega})$ so we cannot hope to show in this case that $\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))$ is not divisible by $\mathcal{J}$. Instead, one must "improve" the Euler system $\mathbf{c}$ of §4.2, to remove this extra zero. We omit the details. □

THEOREM 4.13 (Mazur & Wiles [**MW**]). *If χ is an odd character of order prime to p and $\chi\neq\omega$ then*

$$\mathrm{char}(\mathrm{Hom}_{\mathcal{O}}(\varinjlim A_n^\chi,\mathbf{D}))=\mathrm{Tw}_{\langle\varepsilon\rangle}(\mathcal{L}_{\chi^{-1}\omega}).$$

PROOF. This follows from Theorem 4.12 by the usual analytic class number argument. See [**MW**] §1.6, where this equality is deduced from divisibilities opposite to those of Theorem 4.12. □

5. Elliptic curves

The "Heegner point Euler system" for modular elliptic curves used by Kolyvagin in [**Ko2**] does not fit precisely into the framework we have established. We will discuss later in Chapter IX §4 how to adapt Definition II.1.1 to include the system of Heegner points. However, Kato [**Ka3**], [**Scho**] has constructed an Euler system for the Tate module of a modular elliptic curve, using Beilinson elements in the K-theory of modular curves.

5.1. The setting. Suppose E is an elliptic curve defined over $\mathbf{Q}$, and take $K = \mathbf{Q}$, $K_\infty = \mathbf{Q}_\infty$, $\mathcal{O} = \mathbf{Z}_p$, and $T = T_p(E)$, the p-adic Tate module of E as in Example I.1.5. Then $V = V_p(E) = T_p(E) \otimes \mathbf{Q}_p$ and $W = E_{p^\infty}$. The Weil pairing gives isomorphisms $V \cong V^*$, $T \cong T^*$, and $W \cong W^*$. As in the previous sections, $\mathbf{Q}_n$ will denote the extension of degree p^n in $\mathbf{Q}_\infty$ and $\mathbf{Q}_{n,p}$ is the completion of $\mathbf{Q}_n$ at the unique prime above p.

5.2. The p-adic cohomology groups. As in Example I.6.4, for every n we let

$$H^1_f(\mathbf{Q}_{n,p}, V) = \mathrm{image}(E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p \hookrightarrow H^1(\mathbf{Q}_{n,p}, V)).$$

Since $V = V^*$, this also fixes a choice of $H^1_f(\mathbf{Q}_{n,p}, V^*)$, and these subgroups are orthogonal complements as required.

For every n let $\tan(E_{/\mathbf{Q}_{n,p}})$ denote the tangent space of $E_{/\mathbf{Q}_{n,p}}$ at the origin and consider the Lie group exponential map

$$\exp_E : \tan(E_{/\mathbf{Q}_{n,p}}) \xrightarrow{\sim} E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p.$$

Fix a minimal Weierstrass model of E and let ω_E denote the corresponding holomorphic differential. Then the cotangent space $\mathrm{cotan}(E_{/\mathbf{Q}_{n,p}})$ is $\mathbf{Q}_{n,p}\omega_E$, and we let ω_E^* be the corresponding dual basis of $\tan(E)$. We have a commutative diagram in which all maps are isomorphisms

$$\begin{tikzcd}
\tan(E_{/\mathbf{Q}_{n,p}}) \arrow[rr, "\exp_E"] & & E(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p \\
\mathbf{Q}_{n,p} \arrow[u, "\cdot\omega_E^*"'] & \hat{E}(\mathfrak{p}_n) \otimes \mathbf{Q}_p \arrow[l, "\lambda_E"'] \arrow[r, "\sim"] & E_1(\mathbf{Q}_{n,p}) \otimes \mathbf{Q}_p \arrow[u]
\end{tikzcd}$$

where $\hat{E}$ is the formal group of E, $\mathfrak{p}_n$ is the maximal ideal of $\mathbf{Q}_{n,p}$, $E_1(\mathbf{Q}_{n,p})$ is the kernel of reduction in $E(\mathbf{Q}_p)$, and the bottom isomorphisms are induced by the formal group logarithm λ_E and the isomorphism $\hat{E}(\mathfrak{p}_n) \xrightarrow{\sim} E_1(\mathbf{Q}_{n,p})$ of [**T3**] Theorem 4.2. Using the latter isomorphism we will also view λ_E as a homomorphism from $E(\mathbf{Q}_{n,p})$ to $\mathbf{Q}_{n,p}$.

Since $V \cong V^*$, the local Tate pairing gives the second isomorphism in

$$\mathrm{Hom}(E(\mathbf{Q}_{n,p}), \mathbf{Q}_p) \cong \mathrm{Hom}(H^1_f(\mathbf{Q}_{n,p}, V), \mathbf{Q}_p) \cong H^1_s(\mathbf{Q}_{n,p}, V).$$

Thus there is a dual exponential map (see [**Ka1**] §II.1.2)

$$\exp_E^* : H^1_s(\mathbf{Q}_{n,p}, V) \xrightarrow{\sim} \mathrm{cotan}(E_{/\mathbf{Q}_{n,p}}) = \mathbf{Q}_{n,p}\omega_E.$$

We write $\exp^*_{\omega_E} : H^1_s(\mathbf{Q}_{n,p}, V) \xrightarrow{\sim} \mathbf{Q}_{n,p}$ for the composition $\omega_E^* \circ \exp_E^*$. Since $H^1_s(\mathbf{Q}_{n,p}, T)$ injects into $H^1_s(\mathbf{Q}_{n,p}, V)$, $\exp^*_{\omega_E}$ is injective on $H^1_s(\mathbf{Q}_{n,p}, T)$. The local pairing allows us to identify

$$\begin{array}{ccc} H^1_s(\mathbf{Q}_{n,p}, V) & \xrightarrow{\sim} & \mathrm{Hom}(E(\mathbf{Q}_{n,p}), \mathbf{Q}_p) \\ \uparrow & & \uparrow \\ H^1_s(\mathbf{Q}_{n,p}, T) & \xrightarrow{\sim} & \mathrm{Hom}(E(\mathbf{Q}_{n,p}), \mathbf{Z}_p). \end{array} \tag{14}$$

Explicitly (see [**Ka1**] Theorem II.1.4.1(iv)), $z \in H^1_s(\mathbf{Q}_{n,p}, V)$ is identified with the map

$$x \mapsto \mathrm{Tr}_{\mathbf{Q}_{n,p}/\mathbf{Q}_p} \lambda_E(x) \exp^*_{\omega_E}(z). \tag{15}$$

PROPOSITION 5.1. $\exp^*_{\omega_E}(H^1_s(\mathbf{Q}_p, T)) = [E(\mathbf{Q}_p) : E_1(\mathbf{Q}_p) + E(\mathbf{Q}_p)_{\mathrm{tors}}] p^{-1}\mathbf{Z}_p$.

PROOF. The diagram (14) shows that an element of $H^1_s(\mathbf{Q}_p, V)$ belongs to $H^1_s(\mathbf{Q}_p, T)$ if and only if the corresponding homomorphism takes $E(\mathbf{Q}_p)$ into $\mathbf{Z}_p$. Thus by (15),

$$\exp^*_{\omega_E}(H^1_s(\mathbf{Q}_p, T)) = p^a \mathbf{Z}_p$$

where

$$\lambda_E(E(\mathbf{Q}_p)) = p^{-a}\mathbf{Z}_p.$$

We have $\lambda_E(E_1(\mathbf{Q}_p)) = p\mathbf{Z}_p$ and, since $\mathrm{rank}_{\mathbf{Z}_p} E(\mathbf{Q}_p) = 1$,

$$[\lambda_E(E(\mathbf{Q}_p)) : \lambda_E(E_1(\mathbf{Q}_p)] = [E(\mathbf{Q}_p) : E_1(\mathbf{Q}_p) + E(\mathbf{Q}_p)_{\mathrm{tors}}].$$

This proves the proposition. □

5.3. The L-functions.

DEFINITION 5.2. Let

$$L(E, s) = \sum_{n \geq 1} a_n n^{-s} = \prod_q \ell_q(q^{-s})^{-1}$$

denote the Hasse-Weil L-function of E, where $\ell_q(q^{-s})$ is the usual Euler factor at q. If $m \in \mathbf{Z}^+$ we will also write

$$L_m(E, s) = \sum_{(n,m)=1} a_n n^{-s} = \prod_{q \nmid m} \ell_q(q^{-s})^{-1} = \Big(\prod_{q \mid m} \ell_q(q^{-s})\Big) L(E, s)$$

for the L-function with the Euler factors dividing m removed. If χ is a character of $G_{\mathbf{Q}}$ of conductor f_χ, let

$$L_m(E, \chi, s) = \sum_{(n, f_\chi m)=1} \chi(n) a_n n^{-s} = \prod_{q \nmid f_\chi m} \ell_q(q^{-s}\chi(q))^{-1}.$$

When $m = 1$ we write simply $L(E, \chi, s)$, and then we have

$$L_m(E, \chi, s) = \Big(\prod_{q \mid m} \ell_q(q^{-s}\chi(q))\Big) L(E, \chi, s). \tag{16}$$

If E is modular then these functions all have analytic continuations to $\mathbf{C}$.

5.4. The Euler system. Kato has constructed an Euler system in this setting. Let N denote the conductor of E, and let Ω_E be the fundamental real period of E (which corresponds to our choice of differential ω_E).

THEOREM 5.3 (Kato [**Ka3**]; see also [**Scho**]). *Suppose E is modular. There is a positive integer r_E, independent of p, and an Euler system* $\mathbf{c}$ *for $T_p(E)$ such that*

$$\exp^*_{\omega_E}(\mathrm{loc}^s_{\{p\}}(\mathbf{c}_{\mathbf{Q}})) = r_E L_{Np}(E,1)/\Omega_E$$

and more generally for every $n \geq 0$ and every character χ of $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})$*,*

$$\sum_{\gamma \in \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})} \chi(\gamma) \exp^*_{\omega_E}(\mathrm{loc}^s_{\{p\}}(\mathbf{c}^{\gamma}_{\mathbf{Q}_n})) = r_E L_{Np}(E,\chi,1)/\Omega_E.$$

See [**Scho**], especially §5, for the construction of the Euler system and the proof of the identities in the case where E has good reduction at p. (See also [**Ru9**] Corollary 7.2 to get from [**Scho**] Theorem 5.2.6 to the statement above.)

5.5. Consequences of Kato's Euler system. Following Kato, we will apply the results of Chapter II to bound the Selmer group of E. Let $Ш(E)$ be the Tate-Shafarevich group of E.

THEOREM 5.4 (Kato [**Ka3**]). *Suppose E is modular and E does not have complex multiplication.*

(i) *If $L(E,1) \neq 0$ then $E(\mathbf{Q})$ and $Ш(E)$ are finite.*
(ii) *If L is a finite abelian extension of $\mathbf{Q}$, χ is a character of* $\mathrm{Gal}(L/\mathbf{Q})$*, and $L(E,\chi,1) \neq 0$, then $E(L)^{\chi}$ and $Ш(E_{/L})^{\chi}$ are finite.*

REMARKS 5.5. We will prove a more precise version of Theorem 5.4(i) in Theorem 5.11 below. Kato's is an Euler system for $(T_p(E), \mathbf{Q}^{\mathrm{ab},DD'}, NpDD')$ for appropriate auxiliary integers D, D', where $\mathbf{Q}^{\mathrm{ab},DD'}$ is the maximal abelian extension of $\mathbf{Q}$ unramified outside DD'. Thus (for some choice of D and D', depending on χ) Proposition II.4.2 gives an Euler system for $T_p(E) \otimes \chi$ for every character χ of $G_{\mathbf{Q}}$ of finite order, with properties analogous to those of Theorem 5.3. These twisted Euler systems are needed to prove Theorem 5.4(ii). For simplicity we will not treat this more general setting here, so we will only prove Theorem 5.4(i) below. But the method for (ii) is the same.

Theorem 5.4(i) was first proved by Kolyvagin in [**Ko2**], using a system of Heegner points, along with work of Gross and Zagier [**GZ**], Bump, Friedberg, and Hoffstein [**BFH**], and Murty and Murty [**MM**]. The Euler system proof given here, due to Kato, is self-contained in the sense that it replaces all of those other analytic results with the calculation of Theorem 5.3.

COROLLARY 5.6. *Suppose E is modular and E does not have complex multiplication. Then $E(\mathbf{Q}_\infty)$ is finitely generated.*

PROOF. A theorem of Rohrlich [**Ro**] shows that $L(E,\chi,1) \neq 0$ for almost all characters χ of finite order of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Serre's [**Se4**] Théorème 3 shows that $E(\mathbf{Q}_\infty)_{\mathrm{tors}}$ is finite, and the corollary follows without difficulty from Theorem 5.4(ii). (See for example [**RW**], pp. 242–243.) □

REMARK 5.7. When E has complex multiplication, the representation $T_p(E)$ does not satisfy hypothesis $\mathrm{Hyp}(\mathbf{Q}, V)$(i) (see Remark 5.10 below), so we cannot apply the results of §2 and §3 with Kato's Euler system. However, Theorem 5.4 and Corollary 5.6 are known in that case, as Theorem 5.4 for CM curves can be proved using the Euler system of elliptic units. See [**CW**], [**Ru5**] §11, and [**RW**]. See also Chapter VI §5.3.

5.6. Verification of the hypotheses. Fix a $\mathbf{Z}_p$-basis of T and let

$$\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}(T) \xrightarrow{\sim} \mathrm{GL}_2(\mathbf{Z}_p)$$

be the p-adic representation of $G_{\mathbf{Q}}$ attached to E with this basis.

PROPOSITION 5.8. (i) *If E has no complex multiplication, then $T_p(E)$ satisfies hypotheses* $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$ *and* $H^1(\mathbf{Q}(E_{p^\infty})/\mathbf{Q}, E_{p^\infty})$ *is finite.*

(ii) *If the p-adic representation $\rho_{E,p}$ is surjective, then $T_p(E)$ satisfies hypotheses* $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$ *and* $H^1(\mathbf{Q}(E_{p^\infty})/\mathbf{Q}, E_{p^\infty}) = 0$.

PROOF. The Weil pairing shows that

$$G_{\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})} = \rho_{E,p}^{-1}(\mathrm{SL}_2(\mathbf{Z}_p)).$$

If E has no complex multiplication then a theorem of Serre ([**Se4**] Théorème 3) says that the image of $\rho_{E,p}$ is open in $\mathrm{GL}_2(\mathbf{Z}_p)$. It follows that $V_p(E)$ is an irreducible $G_{\mathbf{Q}_\infty}$-representation, and if $\rho_{E,p}$ is surjective then E_p is an irreducible $\mathbf{F}_p[G_{\mathbf{Q}_\infty}]$-representation.

It also follows that we can find $\tau \in G_{\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})}$ such that

$$\rho_{E,p}(\tau) = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$$

with $x \neq 0$, and such a τ satisfies hypothesis $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$(i). If $\rho_{E,p}$ is surjective we can take $x = 1$, and then τ satisfies hypothesis $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$(i).

We have

$$H^1(\mathbf{Q}(E_{p^\infty})/\mathbf{Q}, E_{p^\infty}) = H^1(\rho_{E,p}(G_{\mathbf{Q}}), (\mathbf{Q}_p/\mathbf{Z}_p)^2)$$

which is zero if $\rho_{E,p}(G_{\mathbf{Q}}) = \mathrm{GL}_2(\mathbf{Z}_p)$, and finite if $\rho_{E,p}(G_{\mathbf{Q}})$ is open in $\mathrm{GL}_2(\mathbf{Z}_p)$. This completes the proof of the proposition. □

REMARK 5.9. Serre's theorem (see [**Se4**] Corollaire 1 of Théorème 3) also shows that if E has no complex multiplication then $\rho_{E,p}$ is surjective for all but finitely many p.

REMARK 5.10. The conditions on τ in hypotheses $\mathrm{Hyp}(\mathbf{Q}, V)$(i) force $\rho_{E,p}(\tau)$ to be nontrivial and unipotent. Thus if E has complex multiplication then there is no τ satisfying $\mathrm{Hyp}(\mathbf{Q}, V)$(i).

5.7. Bounding $\mathcal{S}(\mathbf{Q}, E_{p^\infty})$. Recall that N is the conductor of E.

THEOREM 5.11. *Suppose E is modular, E does not have complex multiplication, and $L(E, 1) \neq 0$.*

(i) *$E(\mathbf{Q})$ and $Ш(E)_{p^\infty}$ are finite.*

(ii) *Suppose in addition that E has good reduction at p, $p \nmid 2r_E|\tilde{E}(\mathbf{F}_p)|$ (where $\tilde{E}$ is the reduction of E modulo p and r_E is as in Theorem 5.3), and $\rho_{E,p}$ is surjective. Then*

$$|\text{Ш}(E)_{p^\infty}| \quad \textit{divides} \quad \frac{L_N(E,1)}{\Omega_E}.$$

PROOF. Recall that $\ell_q(q^{-s})$ is the Euler factor of $L(E,s)$ at q, and that by Proposition I.6.7, $\mathcal{S}(\mathbf{Q}, E_{p^\infty})$ is the usual p-power Selmer group of E.

Since $L(E,1) \neq 0$, and $\ell_q(q^{-1})$ is easily seen to be nonzero for every q, Theorem 5.3 shows that $\mathrm{loc}^s_{\{p\}}(\mathbf{c}_\mathbf{Q}) \neq 0$. By Propositions 5.8(i) and 5.1 we can apply Theorem II.2.10(i) to conclude that $\mathcal{S}(\mathbf{Q}, E_{p^\infty})$ is finite. This proves (i), and it follows (see for example Proposition I.6.7) that $\mathcal{S}(\mathbf{Q}, E_{p^\infty}) = \text{Ш}(E)_{p^\infty}$.

If E has good reduction at p then $p\ell_p(p^{-1}) = |\tilde{E}(\mathbf{F}_p)|$ and

$$[E(\mathbf{Q}_p) : E_1(\mathbf{Q}_p) + E(\mathbf{Q}_p)_{\mathrm{tors}}] \quad \text{divides} \quad |\tilde{E}(\mathbf{F}_p)|.$$

Therefore if $p \nmid r_E|\tilde{E}(\mathbf{F}_p)|$ then

$$\begin{array}{ccc}
\exp^*_{\omega_E}(H^1_s(\mathbf{Q}_p, T_p(E))) & = & p^{-1}\mathbf{Z}_p \\
\cup & & \cup \\
\exp^*_{\omega_E}(\mathbf{Z}_p \mathrm{loc}^s_{\{p\}}(\mathbf{c}_\mathbf{Q})) & = & p^{-1}(L_N(E,1)/\Omega_E)\mathbf{Z}_p
\end{array}$$

by Proposition 5.1 and Theorem 5.3. By Proposition 5.8(ii), if further $p \neq 2$ and $\rho_{E,p}$ is surjective then we can apply Theorem II.2.10(ii) (with $\mathfrak{n}_W = \mathfrak{n}^*_W = 0$) and (ii) follows. $\square$

REMARKS 5.12. In Corollary 5.18 below, using Iwasawa theory, we will prove that Theorem 5.11(ii) holds for almost all p, even when p divides $|\tilde{E}(\mathbf{F}_p)|$. This is needed to prove Theorem 5.4(i), since $|\tilde{E}(\mathbf{F}_p)|$ could be divisible by p for infinitely many p. However, since $|\tilde{E}(\mathbf{F}_p)| < 2p$ for all primes $p > 5$, we see that if $E(\mathbf{Q})_{\mathrm{tors}} \neq 0$ then $|\tilde{E}(\mathbf{F}_p)|$ is prime to p for almost all p. Thus Theorem 5.4(i) for such a curve follows directly from Theorem 5.11.

The Euler system techniques we are using give an upper bound for the order of the Selmer group, but no lower bound. In this case there is no analogue of the analytic class number formula that enabled us to go from the Euler system divisibility to equality in Corollaries 2.4 and 4.7.

5.8. The p-adic L-function and the Coleman map. Suppose for this section that E has good ordinary reduction or multiplicative reduction at p. Let $\alpha \in \mathbf{Z}_p^\times$ and $\beta = p/\alpha \in p\mathbf{Z}_p$ be the eigenvalues of Frobenius over $\mathbf{F}_p$ if E has good ordinary reduction at p, and let $(\alpha, \beta) = (1, p)$ (resp. $(-1, -p)$) if E has split (resp. nonsplit) multiplicative reduction.

Fix a generator $\{\zeta_{p^n}\}_n$ of $\varprojlim \boldsymbol{\mu}_{p^n}$. Write $G_n = \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}_{n,p}/\mathbf{Q}_p)$. If χ is a character of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ of conductor p^n define the Gauss sum

$$\tau(\chi) = \sum_{\gamma \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^n})/\mathbf{Q})} \chi(\gamma)\zeta_{p^n}^\gamma.$$

Fix also an embedding of $\overline{\mathbf{Q}_p}$ into $\mathbf{C}$ so that we can identify complex and p-adic characters of $G_\mathbf{Q}$.

The following theorem is proved in [**MSD**] in the case of good ordinary reduction. See [**MTT**] for the (even more) general statement.

THEOREM 5.13. *Suppose E is modular and E has good ordinary reduction or multiplicative reduction at p, and let α be as above. Then there is a nonzero integer c_E independent of p, and a p-adic L-function $\mathcal{L}_E \in c_E^{-1}\Lambda$ such that for every character χ of* $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ *of finite order,*

$$\chi(\mathcal{L}_E) = \begin{cases} (1-\alpha^{-1})^2 L(E,1)/\Omega_E & \text{if } \chi = 1 \text{ and } E \text{ has good reduction at } p \\ (1-\alpha^{-1}) L(E,1)/\Omega_E & \text{if } \chi = 1 \text{ and } E \text{ is multiplicative at } p \\ \alpha^{-n}\tau(\chi) L(E,\chi^{-1},1)/\Omega_E & \text{if } \chi \text{ has conductor } p^n > 1. \end{cases}$$

If $m \in \mathbf{Z}^+$, define

$$\mathcal{L}_{E,m} = \Big(\prod_{q \mid m, q \neq p} \ell_q(q^{-1}\mathrm{Fr}_q^{-1})\Big)\mathcal{L}_E \in c_E^{-1}\Lambda.$$

Using (16) and Theorem 5.13 one obtains analogous expressions for $\chi(\mathcal{L}_{E,m})$ in terms of $L_m(E,\chi^{-1},1)$.

PROPOSITION 5.14. *Suppose that E has good ordinary reduction or multiplicative reduction at p. Then there is a Λ-module map*

$$\mathrm{Col}_\infty : H^1_{\infty,s}(\mathbf{Q}_p, T) \hookrightarrow \Lambda$$

such that for every $z = \{z_n\} \in H^1_{\infty,s}(\mathbf{Q}_p,T)$ and every nontrivial character χ of G_n,

$$\chi(\mathrm{Col}_\infty(z)) = \alpha^{-k}\tau(\chi)\sum_{\gamma \in G_n} \chi^{-1}(\gamma)\exp^*_{\omega_E}(z_n^\gamma)$$

where p^k is the conductor of χ. If χ_0 is the trivial character then

$$\chi_0(\mathrm{Col}_\infty(z)) = (1-\alpha^{-1})(1-\beta^{-1})^{-1}\exp^*_{\omega_E}(z_0).$$

Further, if E has split multiplicative reduction at p then the image of Col_∞ *is contained in the augmentation ideal of Λ.*

PROOF. The proof is based on work of Coleman [**Co**]. See the appendix of [**Ru9**] for an explicit construction of Col_∞ in this case, and see Chapter VIII §1 for a discussion of a generalization due to Perrin-Riou [**PR2**]. □

Using the Coleman map Col_∞ described above, we can relate Kato's Euler system to the p-adic L-function.

COROLLARY 5.15. *With hypotheses and notation as in Theorems* 5.3 *and* 5.13*,*

$$\mathrm{Col}_\infty(\mathrm{loc}^s_{\{p\}}(\{\mathbf{c}_{\mathbf{Q}_n}\})) = r_E\mathcal{L}_{E,N}.$$

PROOF. If χ is a character of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ of finite order, then the definition (Theorem 5.13) of $\mathcal{L}_E$ and (16) allow us to compute $\chi(r_E\mathcal{L}_{E,N})$, Theorem 5.3 and Proposition 5.14 allow us to compute $\chi(\mathrm{Col}_\infty(\mathrm{loc}^s_{\{p\}}(\{\mathbf{c}_{\mathbf{Q}_n}\})))$, and these values are equal (note that $\ell_p(p^{-1})$ is $(1-\alpha^{-1})(1-\beta^{-1})$ (resp. $(1-\beta^{-1})$) if E has good (resp. multiplicative) reduction at p). Since this holds for all such χ, the corollary follows. □

5.9. Bounding $\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})$. Let $Z_\infty = \mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p)$. Recall that N is the conductor of E.

THEOREM 5.16. *Suppose E is modular, E does not have complex multiplication, and E has good ordinary reduction or nonsplit multiplicative reduction at p. Then Z_∞ is a finitely-generated torsion Λ-module and there is an integer t such that*

$$\mathrm{char}(Z_\infty) \quad \textit{divides} \quad p^t \mathcal{L}_{E,N}\Lambda.$$

If $\rho_{E,p}$ is surjective and $p \nmid r_E \prod_{q|N, q\neq p} \ell_q(q^{-1})$ then $\mathrm{char}(Z_\infty)$ *divides* $\mathcal{L}_E\Lambda$.

If E has split multiplicative reduction at p, the same results hold with $\mathrm{char}(Z_\infty)$ *replaced by* $\mathcal{J}\mathrm{char}(Z_\infty)$ *where $\mathcal{J}$ is the augmentation ideal of* Λ.

PROOF. Rohrlich [**Ro**] proved that $\mathcal{L}_E \neq 0$. Thus the theorem is immediate from Propositions 5.8 and 5.14, Corollary 5.15, and Theorem II.3.8. □

COROLLARY 5.17. *Let E be as in Theorem* 5.16. *If p is a prime where E has good ordinary reduction and*

$$p \nmid \prod_{q|N} |E(\mathbf{Q}_q)_{\mathrm{tors}}|,$$

then Z_∞ has no nonzero finite submodules.

PROOF. This corollary is due to Greenberg [**Gr2**], [**Gr3**]; we sketch a proof here. Let Σ be the set of places of $\mathbf{Q}$ dividing $Np\infty$, and let $\mathbf{Q}_\Sigma$ be the maximal extension of $\mathbf{Q}$ unramified outside Σ. By Lemma I.5.3 there is an exact sequence

$$0 \longrightarrow \mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}) \longrightarrow H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E_{p^\infty}) \longrightarrow \oplus_{q\in\Sigma} \oplus_{v|q} H^1_s(\mathbf{Q}_{\infty,v}, E_{p^\infty}). \quad (17)$$

Suppose $q \in \Sigma$, $q \neq p$, and $v \mid q$. If $p \nmid |E(\mathbf{Q}_q)_{\mathrm{tors}}|$ then it is not hard to show that $E(\mathbf{Q}_{\infty,v})$ has no p-torsion, and so by [**Gr2**] Proposition 2, $H^1(\mathbf{Q}_{\infty,v}, E_{p^\infty}) = 0$. Thus for p as in the statement of the corollary, the Pontryagin dual of (17) is

$$\varprojlim_n E(\mathbf{Q}_{n,p}) \otimes \mathbf{Z}_p \longrightarrow \mathrm{Hom}(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow Z_\infty \longrightarrow 0.$$

Since $\mathbf{Q}_\infty/\mathbf{Q}$ is totally ramified at p,

$$\varprojlim_n E(\mathbf{Q}_{n,p}) \otimes \mathbf{Z}_p = \varprojlim_n E_1(\mathbf{Q}_{n,p}) = \varprojlim_n \hat{E}(\mathfrak{p}_n)$$

and this is free of rank one over Λ (see for example [**PR1**] Théorème 3.1 or [**Schn**] Lemma 6, §A.1). It now follows, using the fact that Z_∞ is a torsion Λ-module (Theorem 5.16) and [**Gr2**] Propositions 3, 4, and 5 that $\mathrm{Hom}(H^1(\mathbf{Q}_\Sigma/\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p)$ has no nonzero finite submodules, and by the Lemma on p. 123 of [**Gr2**] the same is true of Z_∞. □

COROLLARY 5.18. *Suppose E is modular, E does not have complex multiplication, E has good reduction at p, $p \nmid 2r_E \prod_{q|N} \ell_q(q^{-1})|E(\mathbf{Q}_q)_{\mathrm{tors}}|$ (where r_E is as in Theorem* 5.3*), and $\rho_{E,p}$ is surjective. Then*

$$|\text{Ш}(E)_{p^\infty}| \quad \textit{divides} \quad \frac{L(E,1)}{\Omega_E}.$$

PROOF. First, if E has supersingular reduction at p then $|\tilde{E}(\mathbf{F}_p)|$ is prime to p, so the corollary follows from Theorem 5.11(ii).

Thus we may assume that E has good ordinary reduction at p. In this case the corollary is a well-known consequence of Theorem 5.16 and Corollary 5.17; see for example [**PR1**] §6 or [**Schn**] §2 for details. The idea is that if Z_∞ has no nonzero finite submodules and $\mathrm{char}(Z_\infty)$ divides $\mathcal{L}_E\Lambda$, then

$$|\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})^{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}| \quad \text{divides} \quad \chi_0(\mathcal{L}_{E,N}),$$

where χ_0 denotes the trivial character, and

$$\chi_0(\mathcal{L}_{E,N}) = (1-\alpha^{-1})^2 \prod_{q|N} \ell_q(q^{-1})(L(E,1)/\Omega_E).$$

On the other hand, one can show that the restriction map

$$\mathcal{S}(\mathbf{Q}, E_{p^\infty}) \longrightarrow \mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})^{\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})}$$

is injective with cokernel of order divisible by $(1-\alpha^{-1})^2$, and the corollary follows. □

REMARK 5.19. The Birch and Swinnerton-Dyer conjecture predicts that the conclusion of Corollary 5.18 holds for almost all, but not all, primes p.

PROOF OF THEOREM 5.4(i). Suppose E is modular, E does not have complex multiplication, and $L(E,1) \neq 0$. By Theorem 5.11, $E(\mathbf{Q})$ is finite and $\text{Ш}(E)_{p^\infty}$ is finite for every p. By Corollary 5.18 (and using Serre's theorem, see Remark 5.9) $\text{Ш}(E)_{p^\infty} = 0$ for almost all p. This proves Theorem 5.4(i). □

We can also now prove part of Theorem 5.4(ii) in the case where E has good ordinary or multiplicative reduction at p and $L \subset \mathbf{Q}_\infty$. For in that case, by Theorem 5.16, $\chi(\mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty}), \mathbf{Q}_p/\mathbf{Z}_p)))$ is a nonzero multiple of $L(E,\chi,1)/\Omega_E$. If $L(E,\chi,1) \neq 0$ it follows that $\mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})^\chi$ is finite. The kernel of the restriction map $\mathcal{S}(L, E_{p^\infty}) \to \mathcal{S}(\mathbf{Q}_\infty, E_{p^\infty})$ is contained in the finite group $H^1(\mathbf{Q}_\infty/L, E_{p^\infty}^{G_{\mathbf{Q}_\infty}})$, and so we conclude that both $E(L)^\chi$ and $\text{Ш}(E_{/L})^\chi_{p^\infty}$ are finite.

6. Symmetric square of an elliptic curve

Let E be an elliptic curve over $\mathbf{Q}$ and $T_p(E)$ the p-adic Tate module of E. Let T be the symmetric square of $T_p(E)$, the three-dimensional $\mathbf{Z}_p$-representation of $G_\mathbf{Q}$ defined by

$$T = T_p(E) \otimes T_p(E)/\{t \otimes t' - t' \otimes t : t, t' \in T_p(E)\}.$$

Suppose τ has eigenvalues α, α^{-1} on $T_p(E)$ with $\alpha^2 \not\equiv 1 \pmod{p}$. Then $\tau \in G_{\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})}$ (as in Proposition 5.8), and τ has eigenvalues $\alpha^2, 1, \alpha^{-2}$ on T, so τ satisfies hypothesis $\mathrm{Hyp}(\mathbf{Q}, T)$(i). If the p-adic representation attached to E is surjective and $p > 3$, then we can always find such a τ, and further T/pT is an irreducible $G_\mathbf{Q}$-module and $H^1(\Omega/\mathbf{Q}, W) = H^1(\Omega/\mathbf{Q}, W^*) = 0$. Thus in this case *if* we had an Euler system for T we could apply Theorem II.2.10 to study the Selmer group $\mathcal{S}(\mathbf{Q}, W^*)$. See [**Fl**] for important progress in this direction.

CHAPTER IV

Derived cohomology classes

The proofs of the main theorems stated in Chapter II consist of two steps. First we use an Euler system to construct auxiliary cohomology classes which Kolyvagin calls "derivative" classes, and second we use these derived classes along with the duality theorems of Chapter I §7 to bound Selmer groups.

In this chapter we carry out the first of these steps. In §2 and §3 we define and study the "universal Euler system" associated to T and K_∞/K. In §4 we construct the Kolyvagin derivative classes, and in §5 we state the local properties of these derivative classes, which will be crucial in all the applications. The remainder of this chapter is devoted to the proofs of these properties.

1. Setup

Keep the notation of Chapter II §1: we have a fixed number field K, a p-adic representation T of G_K with coefficients in the ring of integers $\mathcal{O}$ of some finite extension Φ of $\mathbf{Q}_p$, and we assume that T is unramified outside a finite set of primes of K.

The letter $\mathfrak{q}$ will always denote a prime of K. For every prime $\mathfrak{q}$ of K not dividing p, $K(\mathfrak{q})$ will denote the maximal p-extension of K inside the ray class field of K modulo $\mathfrak{q}$. Similarly, let $K(1)$ denote the maximal p-extension of K inside the Hilbert class field of K. Class field theory shows that $K(\mathfrak{q})/K(1)$ is unramified outside $\mathfrak{q}$, totally ramified above $\mathfrak{q}$, and cyclic with Galois group equal to the maximal p-quotient of $(\mathcal{O}_K/\mathfrak{q})^\times/(\mathcal{O}_K^\times \pmod{\mathfrak{q}})$. Let $\Gamma_\mathfrak{q} = \mathrm{Gal}(K(\mathfrak{q})/K(1))$.

Fix an ideal $\mathcal{N}$ of K divisible by p and by all primes where T is ramified, as in Definition II.1.1. Define

$$\mathcal{R} = \mathcal{R}(\mathcal{N}) = \{\text{squarefree products of primes } \mathfrak{q} \text{ of } K,\ \mathfrak{q} \nmid \mathcal{N}\}.$$

If $\mathfrak{r} \in \mathcal{R}$, say $\mathfrak{r} = \mathfrak{q}_1 \cdots \mathfrak{q}_k$, then we define $K(\mathfrak{r})$ to be the compositum

$$K(\mathfrak{r}) = K(\mathfrak{q}_1) \cdots K(\mathfrak{q}_k).$$

Note that $K(\mathfrak{r})$ is contained in, but not in general equal to, the maximal p-extension of K inside the ray class field of K modulo $\mathfrak{r}$. We define

$$\Gamma_\mathfrak{r} = \mathrm{Gal}(K(\mathfrak{r})/K(1)).$$

Ramification considerations show that the fields $K(\mathfrak{q})$ are linearly disjoint over $K(1)$, so there is a natural isomorphism

$$\Gamma_\mathfrak{r} \cong \prod_{\text{primes } \mathfrak{q} \mid \mathfrak{r}} \Gamma_\mathfrak{q}$$

where $\Gamma_{\mathfrak{q}}$ is identified with the inertia group of $\mathfrak{q}$ in $\Gamma_{\mathfrak{r}}$. If $\mathfrak{s} \mid \mathfrak{r}$ this allows us to view $\Gamma_{\mathfrak{s}}$ as a subgroup of $\Gamma_{\mathfrak{r}}$, as well as a quotient.

Fix a $\mathbf{Z}_p^d$-extension K_∞/K in which no finite prime splits completely, as in Definition II.1.1. If $K \subset F \subset K_\infty$, let $F(\mathfrak{r}) = FK(\mathfrak{r})$. As in Chapter II, we will write $K \subset_{\mathrm{f}} F$ to indicate that F is a finite extension of K, and if $K \subset_{\mathrm{f}} F \subset K_\infty$ we let

$$\Gamma_{F(\mathfrak{r})} = \mathrm{Gal}(F(\mathfrak{r})/K(1)).$$

Again, we will often identify $\Gamma_{\mathfrak{r}}$ with the subgroup of $\Gamma_{F(\mathfrak{r})}$ generated by the inertia groups of primes dividing $\mathfrak{r}$, and $\Gamma_{F(1)}$ with the the subgroup generated by the inertia groups of primes dividing p, and then (since K_∞/K is unramified outside p)

$$\Gamma_{F(\mathfrak{r})} \cong \Gamma_{F(1)} \times \Gamma_{\mathfrak{r}}.$$

As above, if $\mathfrak{s} \mid \mathfrak{r}$ we can also identify $\Gamma_{F(\mathfrak{s})}$ with a subgroup of $\Gamma_{F(\mathfrak{r})}$.

Figure 1 illustrates these fields and Galois groups.

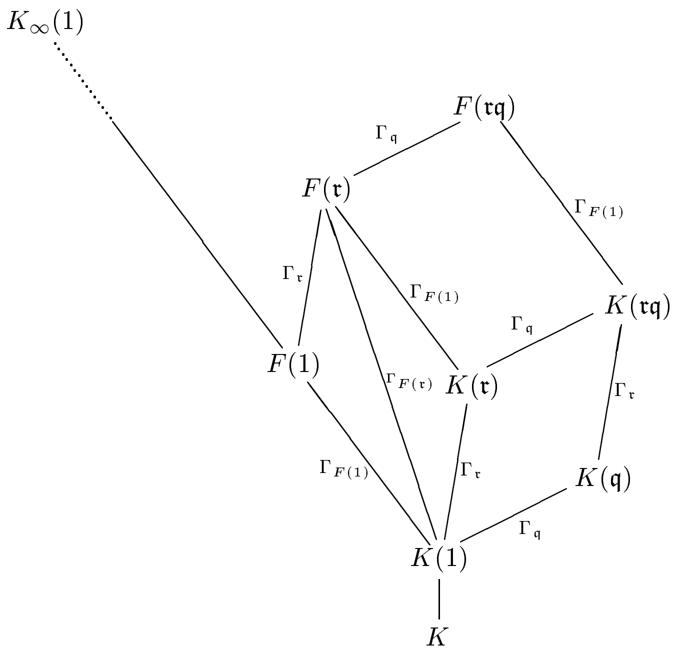

FIGURE 1

For $\mathfrak{r} \in \mathcal{R}$ define

$$N_{\mathfrak{r}} = \sum_{\sigma \in \Gamma_{\mathfrak{r}}} \sigma \in \mathbf{Z}[\Gamma_{\mathfrak{r}}] \subset \mathbf{Z}[\mathrm{Gal}(K(\mathfrak{r})/K)].$$

If $\mathfrak{s} \mid \mathfrak{r}$ and $K \subset_{\mathrm{f}} F \subset K_\infty$ we can view $N_{\mathfrak{s}} \in \mathbf{Z}[\Gamma_{\mathfrak{r}}] \subset \mathbf{Z}[\mathrm{Gal}(F(\mathfrak{r})/K)]$ as above, and then $N_{\mathfrak{r}} = N_{\mathfrak{s}} N_{\mathfrak{r}/\mathfrak{s}}$.

As in Chapter II, let $\mathrm{Fr}_{\mathfrak{q}}$ denote a Frobenius of $\mathfrak{q}$ in G_K, and

$$P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;x) = \det(1 - \mathrm{Fr}_{\mathfrak{q}}^{-1}x|T^*) \in \mathcal{O}[x].$$

DEFINITION 1.1. If $K \subset_{\mathrm{f}} F \subset K_\infty$ and $M \in \mathcal{O}$ is nonzero, define $\mathcal{R}_{F,M} \subset \mathcal{R}$ by

$$\mathcal{R}_{F,M} = \{\mathfrak{r} \in \mathcal{R} : \text{for every prime } \mathfrak{q} \text{ dividing } \mathfrak{r},\ M \mid [K(\mathfrak{q}) : K(1)],\\ M \mid P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;1), \text{ and } \mathfrak{q} \text{ splits completely in } F(1)/K\}.$$

As in Definition I.4.6, if $M \in \mathcal{O}$ is nonzero we let $\bar{M} \in \mathbf{Z}^+$ denote the smallest power of p which is divisible by M.

LEMMA 1.2. *Suppose $\mathfrak{q} \in \mathcal{R}$ is a prime of K.*

(i) $M \mid [K(\mathfrak{q}) : K(1)]$ *if and only if $\mathfrak{q}$ splits completely in $K(\boldsymbol{\mu}_{\bar{M}}, (\mathcal{O}_K^\times)^{1/\bar{M}})$.*
(ii) $P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathbf{N}(\mathfrak{q})\mathrm{Fr}_\mathfrak{q}^{-1})$ *annihilates T.*
(iii) *If $M \mid [K(\mathfrak{q}) : K(1)]$ then $P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;x) \equiv \det(1 - \mathrm{Fr}_\mathfrak{q} x|W_M) \pmod{M}$*
(iv) *If $M \mid [K(\mathfrak{q}) : K(1)]$ then $P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})$ annihilates W_M.*

PROOF. Class field theory identifies $\mathrm{Gal}(K(\mathfrak{q})/K)$ with the maximal p-quotient of $(\mathcal{O}_K/\mathfrak{q})^\times/(\mathcal{O}_K^\times \pmod{\mathfrak{q}})$. Thus if $\mathfrak{q} \nmid p$, then $[K(\mathfrak{q}) : K(1)]$ divides $(\mathbf{N}(\mathfrak{q}) - 1)$ and

$$\mathrm{Fr}_\mathfrak{q} \text{ fixes } \boldsymbol{\mu}_{\bar{M}} \;\Leftrightarrow\; \bar{M} \text{ divides } |(\mathcal{O}_K/\mathfrak{q})^\times| \;\Leftrightarrow\; M \text{ divides } |(\mathcal{O}_K/\mathfrak{q})^\times|.$$

If $\mathrm{Fr}_\mathfrak{q}$ fixes $\boldsymbol{\mu}_{\bar{M}}$ we have further

$$\mathrm{Fr}_\mathfrak{q} \text{ fixes } (\mathcal{O}_K^\times)^{1/\bar{M}} \;\Leftrightarrow\; (\mathcal{O}_K^\times \pmod{\mathfrak{q}}) \subset ((\mathcal{O}_K/\mathfrak{q})^\times)^{\bar{M}}.$$

This proves (i).

One checks easily that

$$P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;x) = \det(1 - \mathrm{Fr}_\mathfrak{q}^{-1}x|T^*) = \det(1 - \mathbf{N}(\mathfrak{q})^{-1}\mathrm{Fr}_\mathfrak{q} x|T).$$

This and the Cayley-Hamilton Theorem prove (ii), (iii), and (iv). $\square$

The following lemma, together with the Tchebotarev theorem, will give a large supply of primes in $\mathcal{R}_{F,M}$. By $F(W_M)$ we mean the smallest extension of F whose absolute Galois group acts trivially on W_M (or equivalently, the fixed field of the kernel of the action of G_F on W_M).

LEMMA 1.3. *Suppose $\tau \in G_{K_\infty(1)}$ acts trivially on $\boldsymbol{\mu}_{p^\infty}$ and on $(\mathcal{O}_K^\times)^{1/p^\infty}$, and $T^{\tau=1} \neq 0$. Suppose further that $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \in \mathcal{O}$ is nonzero, and $\mathfrak{q}$ is a prime of K not dividing $\mathcal{N}$ such that the Frobenius $\mathrm{Fr}_\mathfrak{q}$ of $\mathfrak{q}$ is equal to (a conjugate of) τ on $F(1)(\boldsymbol{\mu}_{\bar{M}}, (\mathcal{O}_K^\times)^{1/\bar{M}}, W_M)$. Then $\mathfrak{q} \in \mathcal{R}_{F,M}$.*

PROOF. First, such a $\mathfrak{q}$ is unramified in $F(1)(\boldsymbol{\mu}_{\bar{M}}, (\mathcal{O}_K^\times)^{1/\bar{M}}, W_M)/K$. Since $\mathrm{Fr}_\mathfrak{q}$ fixes $K(\boldsymbol{\mu}_{\bar{M}}, (\mathcal{O}_K^\times)^{1/\bar{M}})$, Lemma 1.2(i) shows that $M \mid [K(\mathfrak{q}) : K(1)]$, and since $\mathrm{Fr}_\mathfrak{q}$ fixes $F(1)$, $\mathfrak{q}$ splits completely in $F(1)/K$. Also by Lemma 1.2(iii)

$$P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;1) \equiv \det(1 - \mathrm{Fr}_\mathfrak{q}|W_M) = \det(1 - \tau|W_M) \equiv \det(1 - \tau|T) = 0 \pmod{M},$$

the first equality since $\mathrm{Fr}_\mathfrak{q}$ is (a conjugate of) τ on W_M, the second since $T^{\tau=1} \neq 0$. Thus $\mathfrak{q} \in \mathcal{R}_{F,M}$. $\square$

2. The universal Euler system

DEFINITION 2.1. For every $\mathfrak{r} \in \mathcal{R}$ and $K \subset_{\mathrm{f}} F \subset K_\infty$, let $x_{F(\mathfrak{r})}$ be an indeterminate. Define an $\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)]$-module $\mathbf{X}_{F(\mathfrak{r})} = Y_{F(\mathfrak{r})}/Z_{F(\mathfrak{r})}$ where

$Y_{F(\mathfrak{r})}$ is the free $\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)]$-module on the generators $\{x_{F(\mathfrak{s})} : \mathfrak{s} \mid \mathfrak{r}\}$,

$Z_{F(\mathfrak{r})}$ is the submodule of $Y_{F(\mathfrak{r})}$ generated by the relations

$$\begin{array}{rl} \sigma x_{F(\mathfrak{s})} - x_{F(\mathfrak{s})} & \sigma \in \mathrm{Gal}(F(\mathfrak{r})/F(\mathfrak{s})) = \Gamma_{\mathfrak{r}/\mathfrak{s}} \\ N_{\mathfrak{q}} x_{F(\mathfrak{q}\mathfrak{s})} - P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*; \mathrm{Fr}_{\mathfrak{q}}^{-1}) x_{F(\mathfrak{s})} & \mathfrak{q} \text{ prime}, \mathfrak{q}\mathfrak{s} \mid \mathfrak{r}, K(\mathfrak{q}) \neq K(1) \\ x_{F(\mathfrak{q}\mathfrak{s})} - x_{F(\mathfrak{s})} & \mathfrak{q} \text{ prime}, \mathfrak{q}\mathfrak{s} \mid \mathfrak{r}, K(\mathfrak{q}) = K(1). \end{array}$$

In other words, $\mathbf{X}_{F(\mathfrak{r})}$ is the quotient of the free $\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)]$-module on the generators $\{x_{F(\mathfrak{s})} : \mathfrak{s} \mid \mathfrak{r}\}$ by the relations

- $\Gamma_{\mathfrak{r}/\mathfrak{s}}$ acts trivially on $x_{F(\mathfrak{s})}$,
- $N_{\mathfrak{q}} x_{F(\mathfrak{q}\mathfrak{s})} = P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*; \mathrm{Fr}_{\mathfrak{q}}^{-1}) x_{F(\mathfrak{s})}$ if $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$ and $\mathfrak{q}$ ramifies in $F(\mathfrak{r})/K$,
- $x_{F(\mathfrak{q}\mathfrak{s})} = x_{F(\mathfrak{s})}$ if $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$ and $\mathfrak{q}$ does not ramify in $F(\mathfrak{r})/K$.

(Note that if $\mathfrak{q} \mid \mathfrak{r}$, then $\mathfrak{q}$ ramifies in $F(\mathfrak{r})/K$ if and only if the ramification degree of $\mathfrak{q}$ in the ray class field of K modulo $\mathfrak{q}$ is divisible by p. This is independent of $\mathfrak{r}$ and F.)

If $\mathfrak{s} \mid \mathfrak{r}$ and $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset K_\infty$ there are natural $\mathcal{O}[\mathrm{Gal}(F'(\mathfrak{r})/K)]$-module maps

$$\mathbf{X}_{F'(\mathfrak{r})} \longrightarrow \mathbf{X}_{F(\mathfrak{r})} \text{ induced by } x_{F'(\mathfrak{t})} \mapsto x_{F(\mathfrak{t})} \text{ for } \mathfrak{t} \mid \mathfrak{r}, \tag{1}$$

$$\mathbf{X}_{F(\mathfrak{s})} \longrightarrow \mathbf{X}_{F'(\mathfrak{r})} \text{ induced by } x_{F(\mathfrak{t})} \mapsto \mathbf{N}_{F'(\mathfrak{r})/F(\mathfrak{r})} x_{F'(\mathfrak{t})} \text{ for } \mathfrak{t} \mid \mathfrak{s}. \tag{2}$$

The map (1) is clearly surjective, and Lemma 3.1(v) below will show that the map (2) is injective.

DEFINITION 2.2. The *universal Euler system* (for $(T, \mathcal{N}, K_\infty/K)$) is

$$\mathcal{X} = \mathcal{X}(T, \mathcal{N}, K_\infty/K) = \varinjlim_{F,\mathfrak{r}} \mathbf{X}_{F(\mathfrak{r})}.$$

Using the maps (2), (1) we also define

$$\mathbf{X}_{\infty,\mathfrak{r}} = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} \mathbf{X}_{F(\mathfrak{r})} \quad \text{and} \quad \mathbf{X}_{\infty,\mathcal{R}} = \varinjlim_{\mathfrak{r} \in \mathcal{R}} \mathbf{X}_{\infty,\mathfrak{r}}.$$

For every $\mathfrak{r} \in \mathcal{R}$ define

$$H^1_\infty(K(\mathfrak{r}), T) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F(\mathfrak{r}), T).$$

LEMMA 2.3. *If $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$ with $K_\infty \subset \mathcal{K}$, then sending $x_{F(\mathfrak{r})}$ to $\mathbf{c}_{F(\mathfrak{r})}$ induces G_K-equivariant maps*

$$\mathbf{X}_{F(\mathfrak{r})} \longrightarrow H^1(F(\mathfrak{r}), T) \qquad \mathbf{X}_{\infty,\mathfrak{r}} \longrightarrow H^1_\infty(K(\mathfrak{r}), T)$$

$$\mathcal{X} \longrightarrow \varinjlim_{F,\mathfrak{r}} H^1(F(\mathfrak{r}), T) \qquad \mathbf{X}_{\infty,\mathcal{R}} \longrightarrow \varinjlim_{\mathfrak{r} \in \mathcal{R}} H^1_\infty(K(\mathfrak{r}), T)$$

direct limits with respect to restriction maps.

PROOF. This is immediate, since (by Definition II.1.1) the Euler system classes $\{\mathbf{c}_{F(\mathfrak{r})}\}$ satisfy all the relations that the $\{x_{F(\mathfrak{r})}\}$ do. $\square$

REMARK 2.4. Conversely, although we will not make use of it, it follows from the following lemma that a map

$$\mathbf{X}_{\infty,\mathcal{R}} \longrightarrow \varinjlim_{\mathfrak{r}\in\mathcal{R}} H^1_\infty(K(\mathfrak{r}),T)$$

induces an Euler system for $(T,\mathcal{K}_{\min},\mathcal{N})$, where $\mathcal{K}_{\min}$ is as in Remark II.1.4.

LEMMA 2.5. (i) *If $K \subset_{\mathrm{f}} F \subset K_\infty$ and $\mathfrak{r}\in\mathcal{R}$, then*

$$T^{G_{F(\mathfrak{r})}} = T^{G_{F(1)}} \quad \textit{and} \quad W^{G_{F(\mathfrak{r})}} = W^{G_{F(1)}}.$$

(ii) *If $\mathfrak{rs}\in\mathcal{R}$ then the restriction map induces an isomorphism*

$$H^1_\infty(K(\mathfrak{r}),T) \cong H^1_\infty(K(\mathfrak{rs}),T)^{\Gamma_\mathfrak{s}}.$$

PROOF. Since $\mathrm{Gal}(F(\mathfrak{r})/F(1)) = \Gamma_\mathfrak{r}$ is generated by inertia groups of primes dividing $\mathfrak{r}$, and T is unramified at those primes, $\mathrm{Gal}(F(\mathfrak{r})/F(1))$ acts trivially on $T^{G_{F(\mathfrak{r})}}$ and $W^{G_{F(\mathfrak{r})}}$. This proves (i).

Let S be a finite set of places of K containing all places dividing $\mathcal{N}\mathfrak{rs}\infty$, and let K_S be the maximal extension of K unramified outside S. (Recall that $\mathcal{N}$ is divisible by p and all primes where T is ramified, so in particular $K_\infty(\mathfrak{rs}) \subset K_S$ and T is a $\mathrm{Gal}(K_S/K)$-module). By Propositions B.2.5(ii) and B.2.7(i), and using our identification $\mathrm{Gal}(F(\mathfrak{rs})/F(\mathfrak{r})) \cong \Gamma_\mathfrak{s}$, we have an inflation-restriction exact sequence

$$\begin{aligned} H^1(F(\mathfrak{rs})/F(\mathfrak{r}),&T^{G_{F(\mathfrak{rs})}}) \longrightarrow H^1(K_S/F(\mathfrak{r}),T) \\ &\longrightarrow H^1(K_S/F(\mathfrak{rs}),T)^{\Gamma_\mathfrak{s}} \longrightarrow H^2(F(\mathfrak{rs})/F(\mathfrak{r}),T^{G_{F(\mathfrak{rs})}}). \end{aligned} \tag{3}$$

By (i),

$$H^1(F(\mathfrak{rs})/F(\mathfrak{r}),T^{G_{F(\mathfrak{rs})}}) = H^1(F(\mathfrak{rs})/F(\mathfrak{r}),T^{G_{F(1)}}) = \mathrm{Hom}(\Gamma_\mathfrak{s},T^{G_{F(1)}}) = 0$$

and similarly

$$H^2(F(\mathfrak{rs})/F(\mathfrak{r}),T^{G_{F(\mathfrak{rs})}}) = T^{G_{F(1)}}/|\Gamma_\mathfrak{s}|T^{G_{F(1)}}.$$

Now passing to the inverse limit over F in (3), and using Corollary B.3.5 and our assumption that the decomposition group of every finite prime is infinite in $\mathrm{Gal}(K_\infty/K)$, gives an exact sequence

$$0 \longrightarrow H^1_\infty(K(\mathfrak{r}),T) \longrightarrow H^1_\infty(K(\mathfrak{rs}),T)^{\Gamma_\mathfrak{s}} \longrightarrow \varprojlim_{K\subset_{\mathrm{f}} F\subset K_\infty} T^{G_{F(1)}}/|\Gamma_\mathfrak{s}|T^{G_{F(1)}}$$

where the inverse limit on the right is with respect to norm maps. By Lemma B.3.2, this inverse limit is zero, so this proves (ii). □

3. Properties of the universal Euler system

Recall that Φ is the field of fractions of $\mathcal{O}$.

PROPOSITION 3.1. *Suppose $\mathfrak{r}\in\mathcal{R}$, $\mathfrak{s}\mid\mathfrak{r}$, and $K\subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset K_\infty$.*

(i) *$\mathbf{X}_{F(\mathfrak{r})}$ is a finitely generated, free $\mathcal{O}$-module.*
(ii) *$\mathbf{X}_{F(\mathfrak{r})}\otimes\Phi$ is a free, rank-one module over $\Phi[\mathrm{Gal}(F(\mathfrak{r})/K)]$.*
(iii) *$\mathbf{X}_{F(\mathfrak{r})}$ is a free $\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K(\mathfrak{r}))]$-module of rank $[K(\mathfrak{r}):K]$.*
(iv) *The map (1) induces an isomorphism*

$$\mathbf{X}_{F'(\mathfrak{r})}\otimes_{\mathcal{O}[\mathrm{Gal}(F'(\mathfrak{r})/K)]}\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)] \xrightarrow{\sim} \mathbf{X}_{F(\mathfrak{r})}.$$

(v) *The map* (2) *induces an isomorphism* $\mathbf{X}_{F(\mathfrak{s})} \xrightarrow{\sim} \mathbf{X}_{F'(\mathfrak{r})}^{\mathrm{Gal}(F'(\mathfrak{r})/F(\mathfrak{s}))}$.

Proof. Let $\mathfrak{r}'$ be the product of all primes $\mathfrak{q}$ dividing $\mathfrak{r}$ such that $\Gamma_\mathfrak{q} \neq \{1\}$. Then $\mathbf{X}_{F(\mathfrak{r}')} = \mathbf{X}_{F(\mathfrak{r})}$, $F(\mathfrak{r}') = F(\mathfrak{r})$, and $K(\mathfrak{r}') = K(\mathfrak{r})$, so the proposition for $\mathfrak{r}$ is equivalent to the proposition for $\mathfrak{r}'$. Thus we may replace $\mathfrak{r}$ by $\mathfrak{r}'$, i.e., we may simplify the proof by assuming that $\Gamma_\mathfrak{q} \neq \{1\}$ for every $\mathfrak{q}$ dividing $\mathfrak{r}$.

We will prove the proposition by constructing a specific $\mathcal{O}$-basis of $\mathbf{X}_{F(\mathfrak{r})}$. Fix a set of representatives $A_1 \subset G_K$ of $\mathrm{Gal}(K(1)/K)$, and for every prime $\mathfrak{q}$ dividing $\mathfrak{r}$ let $A_\mathfrak{q} = \Gamma_\mathfrak{q} - \{1\} \subset \mathrm{Gal}(F(\mathfrak{r})/K)$. For every ideal $\mathfrak{s}$ dividing $\mathfrak{r}$, define a subset $A_{F,\mathfrak{s}} \subset \mathrm{Gal}(F(\mathfrak{r})/K)$ by

$$\begin{aligned} A_{F,\mathfrak{s}} &= \mathrm{Gal}(F(\mathfrak{r})/K(\mathfrak{r}))A_1 \prod_{\text{primes } \mathfrak{q}|\mathfrak{s}} A_\mathfrak{q} \\ &= \Big\{ g_F g_1 \prod_{\mathfrak{q}|\mathfrak{s}} g_\mathfrak{q} : g_F \in \mathrm{Gal}(F(\mathfrak{r})/K(\mathfrak{r})), g_1 \in A_1, 1 \neq g_\mathfrak{q} \in \Gamma_\mathfrak{q} \Big\} \end{aligned}$$

and then define a finite subset $B_{F(\mathfrak{r})}$ of $\mathbf{X}_{F(\mathfrak{r})}$

$$B_{F(\mathfrak{r})} = \bigcup_{\mathfrak{s}|\mathfrak{r}} A_{F,\mathfrak{s}} x_{F(\mathfrak{s})} \subset \mathbf{X}_{F(\mathfrak{r})}.$$

We will show that $B_{F(\mathfrak{r})}$ is an $\mathcal{O}$-basis of $\mathbf{X}_{F(\mathfrak{r})}$.

Clearly $A_\mathfrak{q} \cup \{N_\mathfrak{q}\}$ is an $\mathcal{O}$-basis of $\mathcal{O}[\Gamma_\mathfrak{q}]$, so $\mathrm{Gal}(F(\mathfrak{r})/K(\mathfrak{r}))A_1 \prod_{\mathfrak{q}|\mathfrak{s}}(A_\mathfrak{q} \cup \{N_\mathfrak{q}\})$ is an $\mathcal{O}$-basis of $\mathcal{O}[\Gamma_{F(\mathfrak{s})}]$. It follows easily by induction on the number of primes dividing $\mathfrak{r}$ that $B_{F(\mathfrak{r})}$ generates $\mathbf{X}_{F(\mathfrak{r})}$ over $\mathcal{O}$, since for every $\mathfrak{q}$ dividing $\mathfrak{s}$,

$$N_\mathfrak{q} x_{F(\mathfrak{s})} = P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; \mathrm{Fr}_\mathfrak{q}^{-1}) x_{F(\mathfrak{s}/\mathfrak{q})}$$

can be expressed in terms of $x_{F(\mathfrak{s}/\mathfrak{q})}$ in $\mathbf{X}_{F(\mathfrak{r})}$. Further,

$$|B_{F(\mathfrak{r})}| \leq \sum_{\mathfrak{s}|\mathfrak{r}} |A_{F,\mathfrak{s}}| = [F(1):K] \prod_{\mathfrak{q}|\mathfrak{r}} (|A_\mathfrak{q}| + 1) = [F(1):K] \prod_{\mathfrak{q}|\mathfrak{r}} |\Gamma_\mathfrak{q}| = [F(\mathfrak{r}):K].$$

On the other hand, we claim that $\mathrm{rank}_\mathcal{O}(\mathbf{X}_{F(\mathfrak{r})}) \geq [F(\mathfrak{r}):K]$. To see this, let $Y_{F(\mathfrak{r})}$ and $Z_{F(\mathfrak{r})}$ be as in Definition 2.1 of $\mathbf{X}_{F(\mathfrak{r})}$. One can check directly that the assignment

$$x_{F(\mathfrak{s})} \mapsto \prod_{\mathfrak{q}|(\mathfrak{r}/\mathfrak{s})} N_\mathfrak{q} \prod_{\mathfrak{q}|\mathfrak{s}} \Big(|\Gamma_\mathfrak{q}| + (P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; \mathrm{Fr}_\mathfrak{q}^{-1}) - |\Gamma_\mathfrak{q}|) \frac{N_\mathfrak{q}}{|\Gamma_\mathfrak{q}|} \Big)$$

induces a well-defined homomorphism from $Y_{F(\mathfrak{r})}$ to $\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)]$ which is zero on $Z_{F(\mathfrak{r})}$. Thus we obtain a map

$$\varphi : \mathbf{X}_{F(\mathfrak{r})} \otimes \Phi \to \Phi[\mathrm{Gal}(F(\mathfrak{r})/K)].$$

If χ is a character of $\mathrm{Gal}(F(\mathfrak{r})/K)$ into an algebraic closure of Φ, say χ has conductor exactly $\mathfrak{s}$, then

$$\chi(\varphi(x_{F(\mathfrak{s})})) = \prod_{\mathfrak{q}|\mathfrak{r}} |\Gamma_\mathfrak{q}| \neq 0.$$

It follows that φ is surjective, and in particular

$$\mathrm{rank}_\mathcal{O}(\mathbf{X}_{F(\mathfrak{r})}) = \dim_\Phi(\mathbf{X}_{F(\mathfrak{r})} \otimes \Phi) \geq [F(\mathfrak{r}):K] \geq |B_{F(\mathfrak{r})}|.$$

Since $B_{F(\mathfrak{r})}$ generates $\mathbf{X}_{F(\mathfrak{r})}$ over $\mathcal{O}$, we conclude that equality holds, $B_{F(\mathfrak{r})}$ is an $\mathcal{O}$-basis of $\mathbf{X}_{F(\mathfrak{r})}$, $\mathbf{X}_{F(\mathfrak{r})}$ is torsion-free, and φ is an isomorphism. This proves (i) and (ii). Further, since $\mathrm{Gal}(F(\mathfrak{r})/K(\mathfrak{r}))$ permutes the elements of the basis $B_{F(\mathfrak{r})}$, (iii) follows as well.

The map (1), defined by $x_{F'(\mathfrak{s})} \mapsto x_{F(\mathfrak{s})}$, induces a surjective map

$$\mathbf{X}_{F'(\mathfrak{r})} \otimes_{\mathcal{O}[\mathrm{Gal}(F'(\mathfrak{r})/K)]} \mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)] \twoheadrightarrow \mathbf{X}_{F(\mathfrak{r})}.$$

By (iii) applied to F and F', this map must be injective as well, which proves (iv).

By (iii), the map (2) induces an isomorphism $\mathbf{X}_{F(\mathfrak{r})} \xrightarrow{\sim} \mathbf{X}_{F'(\mathfrak{r})}^{\mathrm{Gal}(F'(\mathfrak{r})/F(\mathfrak{r}))}$. Also we see that $B_{F(\mathfrak{s})} \subset B_{F(\mathfrak{r})}$, so the map $\mathbf{X}_{F(\mathfrak{s})} \to \mathbf{X}_{F(\mathfrak{r})}$ is injective and its cokernel is torsion free. By (ii), $\mathbf{X}_{F(\mathfrak{r})}^{\mathrm{Gal}(F(\mathfrak{r})/F(\mathfrak{s}))}/\mathbf{X}_{F(\mathfrak{s})}$ is finite, so it must be zero. Now (v) follows. $\square$

If G is a profinite abelian group, we write $\mathcal{O}[[G]] = \varprojlim_{U \subset G} \mathcal{O}[G/U]$.

COROLLARY 3.2. *If $\Gamma = \mathrm{Gal}(K_\infty(\mathfrak{r})/K(\mathfrak{r}))$ then $\mathbf{X}_{\infty,\mathfrak{r}}$ is a free $\mathcal{O}[[\Gamma]]$-module of rank $[K(\mathfrak{r}) : K]$ and for every $K \subset_{\mathrm{f}} F \subset K_\infty$,*

$$\mathbf{X}_{\infty,\mathfrak{r}} \otimes_{\mathcal{O}[[\mathrm{Gal}(K_\infty(\mathfrak{r})/K)]]} \mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)] \cong \mathbf{X}_{F(\mathfrak{r})}.$$

PROOF. This is immediate from Proposition 3.1(iii) and (iv). $\square$

LEMMA 3.3. *Suppose R is a ring, G is a profinite abelian group, and H is subgroup of finite index in G. Suppose B is an $R[[G]]$-module.*

(i) $\mathrm{Hom}_{R[[G]]}(B, R[[G]]) \cong \mathrm{Hom}_{R[[H]]}(B, R[[H]])$ *as $R[[H]]$-modules.*

(ii) *If B is free as an $R[[H]]$-module then* $\mathrm{Ext}^1_{R[[G]]}(B, R[[G]]) = 0$.

PROOF. Write $S = R[[H]]$ and $S' = R[[G]]$. Fix a set $C \subset G$ containing 1 of coset representatives of G/H. Then C is an S-basis of S', and we let $\pi : S' \to S$ be the S-module map

$$\sum_{\eta \in C} a_\eta \eta \mapsto a_1.$$

Define a homomorphism $\mathrm{Hom}_{S'}(B, S') \to \mathrm{Hom}_S(B, S)$ by composition with π. One can check directly that this map is both injective and surjective, which proves (i).

It follows from (i) that $\mathrm{Ext}^1_{S'}(B, S') = \mathrm{Ext}^1_S(B, S)$, and if B is free over S this is zero. $\square$

PROPOSITION 3.4. *Suppose $\mathfrak{r} \in \mathcal{R}$, $k \geq 0$, and $M \in \mathcal{O}$ is nonzero.*

(i) *If $K \subset_{\mathrm{f}} F \subset K_\infty$ and $G = \mathrm{Gal}(F(\mathfrak{r})/K)$, then*

$$\mathrm{Ext}^1_{(\mathcal{O}/M\mathcal{O})[G]}(\mathbf{X}_{F(\mathfrak{r})}/M\mathbf{X}_{F(\mathfrak{r})}, (\mathcal{O}/M\mathcal{O})[G]^k) = 0.$$

(ii) *If $G = \mathrm{Gal}(K_\infty(\mathfrak{r})/K)$, then*

$$\mathrm{Ext}^1_{(\mathcal{O}/M\mathcal{O})[[G]]}(\mathbf{X}_{\infty,\mathfrak{r}}/M\mathbf{X}_{\infty,\mathfrak{r}}, (\mathcal{O}/M\mathcal{O})[[G]]^k) = 0.$$

PROOF. Apply Lemma 3.3(ii) with $R = \mathcal{O}/M\mathcal{O}$ and

$$G = \mathrm{Gal}(F(\mathfrak{r})/K), \quad H = \{1\}, \quad B = \mathbf{X}_{F(\mathfrak{r})}/M\mathbf{X}_{F(\mathfrak{r})}$$

for (i), and

$$G = \mathrm{Gal}(K_\infty(\mathfrak{r})/K), \quad H = \mathrm{Gal}(K_\infty(\mathfrak{r})/K(\mathfrak{r})), \quad B = \mathbf{X}_{\infty,\mathfrak{r}}/M\mathbf{X}_{\infty,\mathfrak{r}}$$

for (ii). That B is free over $R[[H]]$ is Proposition 3.1(i) and Corollary 3.2, respectively. $\square$

REMARK 3.5. Alternatively, Proposition 3.4(i) follows immediately from the fact that $(\mathcal{O}/M\mathcal{O})[G]$ is injective (as a module over itself) when G is finite. However, this is not true for $(\mathcal{O}/M\mathcal{O})[[\mathrm{Gal}(K_\infty(\mathfrak{r})/K)]]$.

4. Kolyvagin's derivative construction

Following Kolyvagin [**Ko2**], we will associate to an Euler system a collection of "derivative" classes

$$\kappa_{F,\mathfrak{r},M} \in H^1(F, W_M)$$

for every nonzero $M \in \mathcal{O}$, $K \subset_{\mathrm{f}} F \subset K_\infty$, and $\mathfrak{r} \in \mathcal{R}_{F,M}$ (where $\mathcal{R}_{F,M}$ is the subset of $\mathcal{R}$ given by Definition 1.1.

DEFINITION 4.1. Fix a generator ξ of $\varprojlim \boldsymbol{\mu}_{p^n}$, and for every prime $\mathfrak{q}$ of K not dividing p fix a prime $\mathfrak{Q}$ of $\bar{K}$ above $\mathfrak{q}$. We will fix a generator $\sigma_\mathfrak{q}$ of $\Gamma_\mathfrak{q}$ as follows.

Let $\mathcal{I}_\mathfrak{Q}$ denote the inertia group of $\mathfrak{Q}$ in G_K and let $M = |\Gamma_\mathfrak{q}| = [K(\mathfrak{q}) : K(1)]$. Since M is a power of p and $\mathfrak{q}$ is prime to p, Lemma I.4.5 shows that $\mathcal{I}_\mathfrak{Q}$ has a unique cyclic quotient of order M, and this quotient is canonically isomorphic to $\boldsymbol{\mu}_M$. Since $\Gamma_\mathfrak{q}$ itself is a cyclic quotient of $\mathcal{I}_\mathfrak{Q}$, this allows us to identify $\Gamma_\mathfrak{q}$ with $\boldsymbol{\mu}_M$. The chosen generator ξ gives us a generator ζ of $\boldsymbol{\mu}_M$; we define $\sigma_\mathfrak{q} \in \Gamma_\mathfrak{q}$ to be the corresponding generator of $\Gamma_\mathfrak{q}$. (This definition depends on the choices of $\mathfrak{Q}$ and ξ, but we will suppress this dependence from the notation.)

Now define, for every prime $\mathfrak{q}$ not dividing p,

$$D_\mathfrak{q} = \sum_{i=0}^{|\Gamma_\mathfrak{q}|-1} i\sigma_\mathfrak{q}^i \quad \in \mathbf{Z}[\Gamma_\mathfrak{q}].$$

If $\mathfrak{r} \in \mathcal{R}$ and $\mathfrak{q} \mid \mathfrak{r}$ we view $D_\mathfrak{q} \in \mathbf{Z}[\Gamma_\mathfrak{r}]$ and define

$$D_\mathfrak{r} = \prod_{\text{primes } \mathfrak{q} \mid \mathfrak{r}} D_\mathfrak{q} \in \mathbf{Z}[\Gamma_\mathfrak{r}].$$

We have the easy "telescoping" identity

$$(\sigma_\mathfrak{q} - 1)D_\mathfrak{q} = |\Gamma_\mathfrak{q}| - N_\mathfrak{q}. \tag{4}$$

This is the key step in the following lemma, which in turn is crucial for the construction of the derivative classes.

LEMMA 4.2. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \in \mathcal{O}$ is nonzero, and $\mathfrak{r} \in \mathcal{R}_{F,M}$. If $N_{F(1)/F} \in \mathbf{Z}[\mathrm{Gal}(F(\mathfrak{r})/F)]$ is an element whose restriction to $\mathbf{Z}[\mathrm{Gal}(F(1)/F)]$ is $\sum_{\gamma \in \mathrm{Gal}(F(1)/F))} \gamma$, then*

$$N_{F(1)/F} D_\mathfrak{r} x_{F(\mathfrak{r})} \in (\mathbf{X}_{F(\mathfrak{r})}/M\mathbf{X}_{F(\mathfrak{r})})^{\mathrm{Gal}(F(\mathfrak{r})/F)}.$$

Further, $N_{F(1)/F} D_\mathfrak{r} x_{F(\mathfrak{r})}$ is independent of the choice of $N_{F(1)/F}$.

PROOF. We will show that

$$(\sigma - 1)D_\mathfrak{r} x_{F(\mathfrak{r})} \in M\mathbf{X}_{F(\mathfrak{r})} \quad \text{for every } \sigma \in \mathrm{Gal}(F(\mathfrak{r})/F(1)),$$

and then both assertions of the lemma follow.

The proof is by induction on the number of primes dividing $\mathfrak{r}$. If $\mathfrak{r}=1$, there is nothing to prove. In general, if $\mathfrak{q}$ is a prime dividing $\mathfrak{r}$, say $\mathfrak{r}=\mathfrak{q}\mathfrak{s}$, then

$$(\sigma_{\mathfrak{q}}-1)D_{\mathfrak{r}}=(\sigma_{\mathfrak{q}}-1)D_{\mathfrak{q}}D_{\mathfrak{s}}=(|\Gamma_{\mathfrak{q}}|-N_{\mathfrak{q}})D_{\mathfrak{s}}$$

so, since $N_{\mathfrak{q}}x_{F(\mathfrak{r})}=P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})x_{F(\mathfrak{s})}$,

$$\begin{aligned}(\sigma_{\mathfrak{q}}-1)D_{\mathfrak{r}}x_{F(\mathfrak{r})}&=|\Gamma_{\mathfrak{q}}|D_{\mathfrak{s}}x_{F(\mathfrak{r})}-P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})D_{\mathfrak{s}}x_{F(\mathfrak{s})}\\&\equiv|\Gamma_{\mathfrak{q}}|D_{\mathfrak{s}}x_{F(\mathfrak{r})}-P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;1)D_{\mathfrak{s}}x_{F(\mathfrak{s})}\pmod{(\mathrm{Fr}_{\mathfrak{q}}-1)D_{\mathfrak{s}}x_{F(\mathfrak{s})}}\\&\equiv 0\pmod{M\mathbf{X}_{F(\mathfrak{r})}}\end{aligned}$$

by definition of $\mathcal{R}_{F,M}$ and the induction hypothesis. Since $\mathrm{Gal}(F(\mathfrak{r})/F(1))$ is generated by the $\sigma_{\mathfrak{q}}$, this proves the lemma. □

REMARK 4.3. The idea of the construction of the derivative class $\kappa_{F,\mathfrak{r},M}$ is as follows. By Lemma 4.2 (and Lemma 2.3) the image of $N_{F(1)/F}D_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$ in $H^1(F(\mathfrak{r}),W_M)$ is fixed by $\mathrm{Gal}(F(\mathfrak{r})/F)$. If $W^{G_{F(\mathfrak{r})}}=0$ then the restriction map

$$H^1(F,W_M)\longrightarrow H^1(F(\mathfrak{r}),W_M)^{\mathrm{Gal}(F(\mathfrak{r})/F)} \tag{5}$$

is an isomorphism, and we define $\kappa_{F,\mathfrak{r},M}\in H^1(F,W_M)$ to be the inverse image of $N_{F(1)/F}D_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$.

When $W^{G_{F(\mathfrak{r})}}\neq 0$, the map (5) need not be an isomorphism. The rest of this section will be devoted to showing, using Proposition 3.4 and the universal Euler system, that the image of $N_{F(1)/F}D_{\mathfrak{r}}\mathbf{c}_{F(\mathfrak{r})}$ always has a canonical inverse image under (5). That inverse image will be our class $\kappa_{F,\mathfrak{r},M}$ (see Definition 4.10). Our construction will also be quite explicit, so that we can use it to prove the local properties of the derivative classes which we state in §5 below.

Fix, for the rest of this section, a nonzero $M\in\mathcal{O}$.

DEFINITION 4.4. Let $\mathbb{W}_M=\mathrm{Ind}(W_M)$ denote the induced module defined (and called $\mathrm{Ind}_{\{1\}}^{G_K}(W_M)$) in Appendix B §4:

$$\mathbb{W}_M=\mathrm{Maps}(G_K,W_M),$$

i.e., continuous maps (not necessarily homomorphisms) from G_K to W_M, with G_K acting via

$$(\gamma f)(g)=f(g\gamma)\qquad\text{for all }\gamma,g\in G_K.$$

There is a natural G_K-module inclusion $W_M\hookrightarrow\mathbb{W}_M$ given by $t\mapsto(g\mapsto gt)$, and we will identify W_M with a submodule of $\mathbb{W}_M$ using this inclusion.

PROPOSITION 4.5. *For every $\mathfrak{r}\in\mathcal{R}$ and every L, $K\subset_{\mathrm{f}}L\subset K_\infty(\mathfrak{r})$ there is a canonical map*

$$\delta_L:(\mathbb{W}_M/W_M)^{G_L}\longrightarrow H^1(L,W_M)$$

such that

(i) *there is an exact sequence*

$$0\longrightarrow W_M^{G_L}\longrightarrow\mathbb{W}_M^{G_L}\longrightarrow(\mathbb{W}_M/W_M)^{G_L}\xrightarrow{\delta_L}H^1(L,W_M)\longrightarrow 0,$$

(ii) *if $f\in(\mathbb{W}_M/W_M)^{G_L}$ and $\hat{f}\in\mathbb{W}_M$ lifts f, then $\delta_L(f)$ is represented by the cocycle*

$$\gamma\mapsto(\gamma-1)\hat{f}\in W_M\quad\textit{for }\gamma\in G_L,$$

(iii) *if $K \subset_{\mathrm{f}} L \subset_{\mathrm{f}} L' \subset K_\infty(\mathfrak{r})$ then the following diagram commutes:*

$$\begin{tikzcd}
(\mathbb{W}_M/W_M)^{G_L} \arrow[r, hook] \arrow[d, "\delta_L"] & (\mathbb{W}_M/W_M)^{G_{L'}} \arrow[r, "\mathbf{N}_{L'/L}"] \arrow[d, "\delta_{L'}"] & (\mathbb{W}_M/W_M)^{G_L} \arrow[d, "\delta_L"] \\
H^1(L, W_M) \arrow[r, "\mathrm{Res}_{L'}"] & H^1(L', W_M) \arrow[r, "\mathrm{Cor}_{L'/L}"] & H^1(L, W_M)
\end{tikzcd}$$

PROOF. By Proposition B.4.5, G_L-cohomology of the exact sequence

$$0 \longrightarrow W_M \longrightarrow \mathbb{W}_M \longrightarrow \mathbb{W}_M/W_M \longrightarrow 0$$

gives the exact sequence of (i) and the commutativity of (iii). Assertion (ii) is just the standard calculation of the connecting map in Galois cohomology, together with our identification of W_M inside $\mathbb{W}_M$. □

LEMMA 4.6. *Let $d = \mathrm{rank}_{\mathcal{O}}(T)$, and suppose $\mathfrak{r} \in \mathcal{R}$.*

(i) *For every $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathbb{W}_M^{G_{F(\mathfrak{r})}}$ is a free $(\mathcal{O}/M\mathcal{O})[\mathrm{Gal}(F(\mathfrak{r})/K)]$-module of rank d.*

(ii) *Let $\Lambda_{\mathfrak{r}} = \mathcal{O}[[\mathrm{Gal}(K_\infty(\mathfrak{r})/K)]]$. Then $\varprojlim_F \mathbb{W}_M^{G_{F(\mathfrak{r})}}$ (inverse limit with respect to the norm maps) is a free $\Lambda_{\mathfrak{r}}/M\Lambda_{\mathfrak{r}}$-module of rank d, and if $K \subset_{\mathrm{f}} F' \subset K_\infty$*

$$\varprojlim_F \mathbb{W}_M^{G_{F(\mathfrak{r})}} \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{O}[\mathrm{Gal}(F'(\mathfrak{r})/K)] \cong \mathbb{W}_M^{G_{F'(\mathfrak{r})}}.$$

PROOF. Let W_M^0 denote the $\mathbf{Z}_p$-module W_M with trivial action of G_K. Then there are Galois-equivariant homomorphisms

$$\begin{aligned}
\mathbb{W}_M^{G_{F(\mathfrak{r})}} = \mathrm{Maps}(\mathrm{Gal}(F(\mathfrak{r})/K), W_M) &= \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)], W_M^0) \\
&= \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)], \mathcal{O}/M\mathcal{O}) \otimes_{\mathcal{O}} W_M^0.
\end{aligned}$$

Since W_M is free of rank d over $\mathcal{O}/M\mathcal{O}$, and $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)], \mathcal{O}/M\mathcal{O})$ is free of rank one over $(\mathcal{O}/M\mathcal{O})[\mathrm{Gal}(F(\mathfrak{r})/K)]$, the lemma follows. □

If $\mathfrak{r} \in \mathcal{R}$ we write $H^1_\infty(K(\mathfrak{r}), W_M) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F(\mathfrak{r}), W_M)$.

PROPOSITION 4.7. *Suppose $\mathfrak{r} \in \mathcal{R}$. Then the maps $\delta_{F(\mathfrak{r})}$ of Proposition 4.5 induce an exact sequence*

$$0 \longrightarrow \varprojlim_F \mathbb{W}_M^{G_{F(\mathfrak{r})}} \longrightarrow \varprojlim_F (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \xrightarrow{\delta_{\mathfrak{r}}} H^1_\infty(K(\mathfrak{r}), W_M) \longrightarrow 0.$$

PROOF. By Lemma 4.6(i), $\mathbb{W}_M^{G_{F(\mathfrak{r})}}$ is finite for every F, $K \subset_{\mathrm{f}} F \subset K_\infty$. Therefore taking inverse limits over F of the exact sequence of Proposition 4.5(i) (with respect to norm maps for the first three terms and corestriction for the fourth; see Proposition 4.5(iii)) yields a new exact sequence (see Proposition B.1.1(i))

$$\begin{aligned}
0 \longrightarrow \varprojlim_F W_M^{G_{F(\mathfrak{r})}} \longrightarrow \varprojlim_F \mathbb{W}_M^{G_{F(\mathfrak{r})}} \\
\longrightarrow \varprojlim_F (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \xrightarrow{\delta_{\mathfrak{r}}} H^1_\infty(K(\mathfrak{r}), W_M) \longrightarrow 0.
\end{aligned}$$

By Lemma B.3.2, $\varprojlim W_M^{G_{F(\mathfrak{r})}} = 0$, and the proposition follows. □

PROPOSITION 4.8. *Suppose* $\mathbf{c}$ *is an Euler system and* $\mathfrak{r} \in \mathcal{R}$. *There is a family of* $\mathcal{O}[G_K]$*-module maps*

$$\{\mathbf{d}_F : \mathbf{X}_{F(\mathfrak{r})} \to (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} : K \subset_{\mathrm{f}} F \subset K_\infty\}$$

lifting $\mathbf{c}$*, i.e., such that the following diagrams commute*

$$\begin{tikzcd} & (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \arrow[d, "\delta_{F(\mathfrak{r})}"] \\ \mathbf{X}_{F(\mathfrak{r})} \arrow[ur, "\mathbf{d}_F"] \arrow[r, "\mathbf{c}"'] & H^1(F(\mathfrak{r}), W_M) \end{tikzcd} \qquad \begin{tikzcd} \mathbf{X}_{F'(\mathfrak{r})} \arrow[r, "\mathbf{d}_{F'}"] \arrow[d, "\mathbf{N}_{F'(\mathfrak{r})/F(\mathfrak{r})}"'] & (\mathbb{W}_M/W_M)^{G_{F'(\mathfrak{r})}} \arrow[d, "\mathbf{N}_{F'(\mathfrak{r})/F(\mathfrak{r})}"] \\ \mathbf{X}_{F(\mathfrak{r})} \arrow[r, "\mathbf{d}_F"] & (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \end{tikzcd}$$

where the bottom map on the left sends $x_{F(\mathfrak{s})} \mapsto \mathbf{c}_{F(\mathfrak{s})}$ *for all* $\mathfrak{s}$ *dividing* $\mathfrak{r}$ *as in Lemma 2.3, and on the right* $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset K_\infty$. *These conditions determine each* $\mathbf{d}_F$ *uniquely up to an element of* $\mathrm{Hom}_{\mathcal{O}[G_K]}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M)$.

PROOF. We first illustrate the proof in a simplified setting. If $W_M^{G_{F(\mathfrak{r})}} = 0$, then Proposition 4.5(i) becomes a short exact sequence which (abbreviating $R = (\mathcal{O}/M\mathcal{O})[\mathrm{Gal}(F(\mathfrak{r})/K)]$ and $\mathbf{X}_{F(\mathfrak{r})}/M = \mathbf{X}_{F(\mathfrak{r})}/M\mathbf{X}_{F(\mathfrak{r})}$) induces an exact sequence

$$\begin{aligned} 0 \to \mathrm{Hom}_R(\mathbf{X}_{F(\mathfrak{r})}/M, \mathbb{W}_M^{G_{F(\mathfrak{r})}}) &\to \mathrm{Hom}_R(\mathbf{X}_{F(\mathfrak{r})}/M, (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}}) \\ &\xrightarrow{\delta_{F(\mathfrak{r})}} \mathrm{Hom}_R(\mathbf{X}_{F(\mathfrak{r})}/M, H^1(F(\mathfrak{r}), W_M)) \to \mathrm{Ext}^1_R(\mathbf{X}_{F(\mathfrak{r})}/M, \mathbb{W}_M^{G_{F(\mathfrak{r})}}). \end{aligned}$$

Lemma 4.6(i) and Proposition 3.4(i) show that $\mathrm{Ext}^1_R(\mathbf{X}_{F(\mathfrak{r})}/M, \mathbb{W}_M^{G_{F(\mathfrak{r})}}) = 0$, so we can choose a map $\mathbf{d}_F$ lifting $\mathbf{c}$ in this case.

In general, since $W_M^{G_{F(1)}}$ may be nonzero, we pass to the limit and use the short exact sequence of Proposition 4.7 instead of Proposition 4.5(i). Arguing as above, using Lemma 4.6(ii) and Propositions 4.7 and 3.4(ii), and writing $\Lambda_{\mathfrak{r}} = \mathcal{O}[[\mathrm{Gal}(K_\infty(\mathfrak{r})/K)]]$, we get an exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{\Lambda_{\mathfrak{r}}/M\Lambda_{\mathfrak{r}}}&(\mathbf{X}_{\infty,\mathfrak{r}}/M\mathbf{X}_{\infty,\mathfrak{r}}, \varprojlim_F \mathbb{W}_M^{G_{F(\mathfrak{r})}}) \\ &\longrightarrow \mathrm{Hom}_{\Lambda_{\mathfrak{r}}/M\Lambda_{\mathfrak{r}}}(\mathbf{X}_{\infty,\mathfrak{r}}/M\mathbf{X}_{\infty,\mathfrak{r}}, \varprojlim_F (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}}) \qquad (6) \\ &\qquad \xrightarrow{\boldsymbol{\delta}_{\mathfrak{r}}} \mathrm{Hom}_{\Lambda_{\mathfrak{r}}/M\Lambda_{\mathfrak{r}}}(\mathbf{X}_{\infty,\mathfrak{r}}/M\mathbf{X}_{\infty,\mathfrak{r}}, H^1_\infty(K(\mathfrak{r}), W_M)) \longrightarrow 0. \end{aligned}$$

Therefore there is a map $\mathbf{d}_\infty : \mathbf{X}_{\infty,\mathfrak{r}} \to \varprojlim_F (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}}$ such that

$$\boldsymbol{\delta}_{\mathfrak{r}} \circ \mathbf{d}_\infty(\{x_{F(\mathfrak{s})}\}_F) = \{\mathbf{c}_{F(\mathfrak{s})}\}_F$$

for every $\mathfrak{s}$ dividing $\mathfrak{r}$. We define $\mathbf{d}_F$ to be the composition

$$\begin{aligned} \mathbf{X}_{F(\mathfrak{r})} &\xrightarrow{\sim} \mathbf{X}_{\infty,\mathfrak{r}} \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)] \\ &\xrightarrow{\mathbf{d}_\infty \otimes 1} \varprojlim_{F'} (\mathbb{W}_M/W_M)^{G_{F'(\mathfrak{r})}} \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{O}[\mathrm{Gal}(F(\mathfrak{r})/K)] \longrightarrow (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \end{aligned}$$

where the left-hand isomorphism comes from Corollary 3.2 and the right-hand map is the natural projection. (Explicitly, $\mathbf{d}_F(x_{F(\mathfrak{s})})$ is the projection of $\mathbf{d}_\infty(\{x_{F'(\mathfrak{s})}\})$ to $(\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}}$.) It is straightforward to check that these maps have the desired properties. By (6), $\mathbf{d}_\infty$ is unique up to an element of $\mathrm{Hom}_{G_K}(\mathbf{X}_{\infty,\mathfrak{r}}, \varprojlim \mathbb{W}_M^{G_{F(\mathfrak{r})}})$, and it follows that $\mathbf{d}_F$ is well-defined up to an element of $\mathrm{Hom}_{\mathcal{O}[G_K]}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M)$. ☐

REMARK 4.9. We will only need to use the existence of the maps $\mathbf{d}_F$ of Proposition 4.8 for individual F. The compatibility as F varies (the right-hand diagram of the proposition) is needed in order to get the uniqueness portion of the proposition, i.e., to make the map $\mathbf{d}_F$ well-defined up to an element of $\mathrm{Hom}_{\mathcal{O}[G_K]}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M)$.

DEFINITION 4.10. Suppose $\mathbf{c}$ is an Euler system, $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \in \mathcal{O}$ is nonzero, and $\mathfrak{r} \in \mathcal{R}_{F,M}$. Fix a map

$$\mathbf{d} = \mathbf{d}_F : \mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M / W_M$$

lifting $\mathbf{c}$ as in Proposition 4.8.

Fix an element $N_{F(1)/F} \in \mathbf{Z}[\mathrm{Gal}(F(\mathfrak{r})/F)]$ whose restriction to $\mathrm{Gal}(F(1)/F)$ is $\sum_{\gamma \in \mathrm{Gal}(F(1)/F))} \gamma$ and write

$$D_{\mathfrak{r},F} = N_{F(1)/F} D_{\mathfrak{r}}.$$

Lemma 4.2 shows that $\mathbf{d}(D_{\mathfrak{r},F} x_{F(\mathfrak{r})}) \in (\mathbb{W}_M/W_M)^{G_F}$ and we define

$$\kappa_{F,\mathfrak{r},M} = \delta_F(\mathbf{d}(D_{\mathfrak{r},F} x_{F(\mathfrak{r})})) \in H^1(F, W_M).$$

We can describe this definition with the following diagram

$$\begin{tikzcd}
\mathbf{d}(D_{\mathfrak{r},F} x_{F(\mathfrak{r})}) \arrow[rrrrr, mapsto, bend left] & \in & (\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \arrow[r, "\delta_{F(\mathfrak{r})}"] & H^1(F(\mathfrak{r}), W_M) & \ni & D_{\mathfrak{r},F}\mathbf{c}_{F(\mathfrak{r})} \\
\mathbf{d}(D_{\mathfrak{r},F} x_{F(\mathfrak{r})}) \arrow[u, mapsto] \arrow[rrrrr, mapsto, bend right] & \in & (\mathbb{W}_M/W_M)^{G_F} \arrow[u, hook] \arrow[r, "\delta_F"] & H^1(F, W_M) \arrow[u, "\mathrm{res}"'] & \ni & \kappa_{F,\mathfrak{r},M}
\end{tikzcd}$$

where the commutativity of the inner square is part of Proposition 4.5(iii).

REMARK 4.11. The definition of $\kappa_{F,\mathfrak{r},M}$ is independent of the choice of $N_{F(1)/F}$, since by Lemma 4.2, $D_{\mathfrak{r},F} x_{F(\mathfrak{r})} \in \mathbf{X}_{F(\mathfrak{r})}/M\mathbf{X}_{F(\mathfrak{r})}$ is independent of this choice. The definition is also independent the choice of $\mathbf{d}$ in Proposition 4.8. For if $\mathbf{d}'$ is any other choice, then $\mathbf{d} - \mathbf{d}' \in \mathrm{Hom}_{G_K}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M)$, so by Lemma 4.2 and Proposition 4.5(i),

$$\mathbf{d}(D_{\mathfrak{r},F} x_{F(\mathfrak{r})}) - \mathbf{d}'(D_{\mathfrak{r},F} x_{F(\mathfrak{r})}) \in \mathrm{image}((\mathbb{W}_M)^{G_F}) = \ker(\delta_F).$$

Also, note that the definition of $\kappa_{F,\mathfrak{r},M}$ depends only on the images of the classes $\{\mathbf{c}_{F(\mathfrak{s})} : \mathfrak{s} \mid \mathfrak{r}\}$ in $H^1(F(\mathfrak{r}), W_M)$. See Chapter IX §3 for a further discussion in this direction.

For the next two lemmas, suppose $\mathbf{c}$ is an Euler system, $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \in \mathcal{O}$ is nonzero, and $\mathfrak{r} \in \mathcal{R}_{F,M}$ as in Definition 4.10.

LEMMA 4.12. *Suppose $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M/W_M$ is a lifting of the Euler system $\mathbf{c}$ as in Proposition 4.8. Let $f \in \mathbb{W}_M$ be any lifting of $\mathbf{d}(D_{\mathfrak{r},F} x_{F(\mathfrak{r})})$. Then $\kappa_{F,\mathfrak{r},M}$ is represented by the cocycle*

$$\gamma \mapsto (\gamma - 1)f \in W_M.$$

PROOF. This is a combination of the definition of $\kappa_{F,\mathfrak{r},M}$ above with the explicit description of the connecting map δ_F (Proposition 4.5(ii)). $\square$

LEMMA 4.13. (i) *The class $\kappa_{F,1,M}$ is the image of $\mathbf{c}_F$ in $H^1(F, W_M)$.*
(ii) *The restriction of $\kappa_{F,\mathfrak{r},M}$ to $F(\mathfrak{r})$ is the image of $D_{\mathfrak{r},F}\mathbf{c}_{F(\mathfrak{r})}$ in $H^1(F(\mathfrak{r}), W_M)$.*
(iii) *If $M \mid M'$ and $\mathfrak{r} \in \mathcal{R}_{F,M'}$ then under the natural maps we have*

$$\begin{array}{ccc} H^1(F, W_{M'}) \longrightarrow H^1(F, W_M) & \qquad & H^1(F, W_M) \longrightarrow H^1(F, W_{M'}) \\ \kappa_{F,\mathfrak{r},M'} \longmapsto \kappa_{F,\mathfrak{r},M} & \qquad & \kappa_{F,\mathfrak{r},M} \longmapsto (M'/M)\kappa_{F,\mathfrak{r},M'} \end{array}$$

PROOF. All three assertions follow from Definition 4.10. For the first we take $\mathfrak{r} = 1$, $D_{\mathfrak{r},F} = N_{F(1)/F}$, and use Proposition 4.5(iii) and the Euler system relation $\mathrm{Cor}_{F(1)/F}\mathbf{c}_{F(1)} = \mathbf{c}_F$. $\square$

5. Local properties of the derivative classes

Fix an Euler system $\mathbf{c}$ for T. In this section we will state the main results describing the local behavior of the derivative classes $\kappa_{F,\mathfrak{r},M}$ of §4. We will see (Theorem 5.1) that $\kappa_{F,\mathfrak{r},M}$ belongs to the Selmer group $\mathcal{S}^{\Sigma}(F, W_M)$ where Σ is the set of primes dividing $p\mathfrak{r}$. At primes dividing $\mathfrak{r}$, $\kappa_{F,\mathfrak{r},M}$ will in general be ramified, and understanding this ramification (Theorem 5.4) is crucial for the applications.

The proofs will be given in the remaining sections of this chapter.

THEOREM 5.1. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \in \mathcal{O}$ is nonzero, and $\mathfrak{r} \in \mathcal{R}_{F,M}$. If w is a place of F not dividing $p\mathfrak{r}$ then*

$$(\kappa_{F,\mathfrak{r},M})_w \in H^1_f(F_w, W_M).$$

Equivalently,

$$\kappa_{F,\mathfrak{r},M} \in \mathcal{S}^{\Sigma_{p\mathfrak{r}}}(F, W_M)$$

where $\Sigma_{p\mathfrak{r}}$ is the set of primes of K dividing $p\mathfrak{r}$.

Theorem 5.1 will be proved in §6.

LEMMA 5.2. *Suppose $M \in \mathcal{O}$ is nonzero and $\mathfrak{q} \in \mathcal{R}_{K,M}$. Then there is a unique $Q_\mathfrak{q}(x) \in (\mathcal{O}/M\mathcal{O})[x]$ such that $P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; x) \equiv (x-1)Q_\mathfrak{q}(x) \pmod{M}$.*

PROOF. Take

$$Q_\mathfrak{q}(x) = \frac{P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; x) - P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; 1)}{x-1}.$$

Since M divides $P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*; 1)$ this polynomial has the desired property, and the uniqueness comes from the fact that $x-1$ is not a zero divisor in $(\mathcal{O}/M\mathcal{O})[x]$. $\square$

DEFINITION 5.3. Suppose $M \in \mathcal{O}$ is nonzero and $\mathfrak{q} \in \mathcal{R}_{K,M}$. The choices of $\sigma_\mathfrak{q} \in \Gamma_\mathfrak{q}$ (Definition 4.1) and $\mathrm{Fr}_\mathfrak{q}$ depend on the choice of a prime $\mathfrak{Q}$ of $\bar{K}$ above $\mathfrak{q}$. We use the same choice for both, and we further fix $\bar{\sigma}_\mathfrak{q}$ in the inertia group of $\mathfrak{Q}$ extending $\sigma_\mathfrak{q}$.

By Lemma I.4.7(i) (which applies thanks to Lemma 1.2(i)) there are well-defined isomorphisms

$$\alpha_{\mathfrak{q}} : H^1_s(K_{\mathfrak{q}}, W_M) \xrightarrow{\sim} W_M^{\mathrm{Fr}_{\mathfrak{q}}=1}$$
$$\beta_{\mathfrak{q}} : H^1_f(K_{\mathfrak{q}}, W_M) \xrightarrow{\sim} W_M/(\mathrm{Fr}_{\mathfrak{q}}-1)W_M$$

given on cocycles by

$$\alpha_{\mathfrak{q}}(c) = c(\bar{\sigma}_{\mathfrak{q}}), \qquad \beta_{\mathfrak{q}}(c) = c(\mathrm{Fr}_{\mathfrak{q}})$$

If $\mathfrak{q} \in \mathcal{R}_{K,M}$, then $P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*; \mathrm{Fr}_{\mathfrak{q}}^{-1})$ annihilates W_M by Lemma 1.2(iv). Thus the polynomial $Q_{\mathfrak{q}}$ of Lemma 5.2 induces a map

$$Q_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) : W_M/(\mathrm{Fr}_{\mathfrak{q}}-1)W_M \to W_M^{\mathrm{Fr}_{\mathfrak{q}}=1}.$$

We define the "finite-singular comparison" map

$$\phi^{fs}_{\mathfrak{q}} : H^1_f(K_{\mathfrak{q}}, W_M) \to H^1_s(K_{\mathfrak{q}}, W_M)$$

to be the composition

$$H^1_f(K_{\mathfrak{q}}, W_M) \xrightarrow{\beta_{\mathfrak{q}}} W_M/(\mathrm{Fr}_{\mathfrak{q}}-1)W_M \xrightarrow{Q_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})} W_M^{\mathrm{Fr}_{\mathfrak{q}}=1} \xrightarrow{\alpha_{\mathfrak{q}}^{-1}} H^1_s(K_{\mathfrak{q}}, W_M).$$

If $K \subset_{\mathrm{f}} F \subset K_\infty$ and $\mathfrak{q} \in \mathcal{R}_{F,M}$, then $F_{\mathfrak{Q}} = K_{\mathfrak{q}}$, and we can view $\phi^{fs}_{\mathfrak{q}}$ as a map from $H^1_f(F_{\mathfrak{Q}}, W_M)$ to $H^1_s(F_{\mathfrak{Q}}, W_M)$. We will still write $\phi^{fs}_{\mathfrak{q}}$ in this case, and suppress the dependence on $\mathfrak{Q}$.

THEOREM 5.4. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \in \mathcal{O}$ is nonzero, and $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,M}$. If $\phi^{fs}_{\mathfrak{q}}$ is the map defined above, and $(\kappa_{F,\mathfrak{r}\mathfrak{q},M})^s_{\mathfrak{q}}$ denotes the image of $\kappa_{F,\mathfrak{r}\mathfrak{q},M}$ in $H^1_s(F_{\mathfrak{Q}}, W_M)$, then*

$$(\kappa_{F,\mathfrak{r}\mathfrak{q},M})^s_{\mathfrak{q}} = \phi^{fs}_{\mathfrak{q}}(\kappa_{F,\mathfrak{r},M}).$$

In other words, the singular part of $\kappa_{F,\mathfrak{r}\mathfrak{q},M}$ at $\mathfrak{q}$ is controlled by the (finite) localization of $\kappa_{F,\mathfrak{r},M}$ at $\mathfrak{q}$. Theorem 5.4 will be proved in §7.

COROLLARY 5.5. *Suppose $0 \neq M \in \mathcal{O}$, $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{K,M}$, and $W_M/(\mathrm{Fr}_{\mathfrak{q}}-1)W_M$ is free of rank one over $\mathcal{O}/M\mathcal{O}$. Then the order of $(\kappa_{K,\mathfrak{r}\mathfrak{q},M})^s_{\mathfrak{q}}$ in $H^1_s(K_{\mathfrak{q}}, W_M)$ is equal to the order of $(\kappa_{K,\mathfrak{r},M})_{\mathfrak{q}}$ in $H^1_f(K_{\mathfrak{q}}, W_M)$.*

PROOF. The maps $\alpha_{\mathfrak{q}}$ and $\beta_{\mathfrak{q}}$ in Definition 5.3 are isomorphisms, and by Lemma 1.2(iii) and Corollary A.2.7 (applied with $\tau = \mathrm{Fr}_{\mathfrak{q}}^{-1}$ and $Q(x) = Q_{\mathfrak{q}}(x)$), so is the map $Q_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})$. Thus $\phi^{fs}_{\mathfrak{q}}$ is an isomorphism and the corollary follows from Theorem 5.4. □

6. Local behavior at primes not dividing $p\mathfrak{r}$

Fix for this section an Euler system $\mathbf{c}$ for T and a nonzero $M \in \mathcal{O}$. If $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathfrak{r} \in \mathcal{R}_{F,M}$, and w is a place of F not dividing $p\mathfrak{r}$, we need to show that $(\kappa_{F,\mathfrak{r},M})_w \in H^1_f(F_w, W_M)$. When w is archimedean (Lemma 6.3), or when w is nonarchimedean and T is unramified at w (Corollary 6.2(ii)), this is not difficult. We treat those cases first, and then go on to the general case.

PROPOSITION 6.1. *If $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathfrak{r} \in \mathcal{R}$, and $\mathcal{Q}$ is a prime of $F(\mathfrak{r})$ not dividing p, then for every $\gamma \in G_K$,*

$$(\gamma \mathbf{c}_{F(\mathfrak{r})})_{\mathcal{Q}} \in H^1_{\mathrm{ur}}(F(\mathfrak{r})_{\mathcal{Q}}, T), \quad (\gamma \bar{\mathbf{c}}_{F(\mathfrak{r})})_{\mathcal{Q}} \in H^1_{\mathrm{ur}}(F(\mathfrak{r})_{\mathcal{Q}}, W_M)$$

where $\bar{\mathbf{c}}_{F(\mathfrak{r})}$ is the image of $\mathbf{c}_{F(\mathfrak{r})}$ under the map $H^1(F(\mathfrak{r}), T) \to H^1(F(\mathfrak{r}), W_M)$.

PROOF. Since $\{\gamma \mathbf{c}_{F(\mathfrak{r})}\}_F \in H^1_\infty(K(\mathfrak{r}), T)$, this is immediate from Corollary B.3.4. $\square$

COROLLARY 6.2. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathfrak{r} \in \mathcal{R}_{F,M}$, and $\mathcal{Q}$ is a prime of F not dividing $p\mathfrak{r}$.*

(i) $(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in H^1_{\mathrm{ur}}(F_{\mathcal{Q}}, W_M)$.

(ii) *If T is unramified at $\mathcal{Q}$ then $(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in H^1_f(F_{\mathcal{Q}}, W_M)$.*

PROOF. Let $D_{\mathfrak{r},F}$ be as in Definition 4.10 and write $\mathcal{I}$ for an inertia group of $\mathcal{Q}$ in G_F. Since $F(\mathfrak{r})/F$ is unramified at $\mathcal{Q}$, $\mathcal{I} \subset G_{F(\mathfrak{r})}$, so by Lemma 4.13(ii) the restriction of $\kappa_{F,\mathfrak{r},M}$ to $\mathcal{I}$ is equal to the image of $D_{\mathfrak{r},F}\mathbf{c}_{F(\mathfrak{r})}$ in $H^1(\mathcal{I}, W_M)$. By Proposition 6.1, the latter is zero. This shows that $(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in H^1_{\mathrm{ur}}(F_{\mathcal{Q}}, W_M)$, and if T is unramified at $\mathcal{Q}$ then Lemma I.3.8(ii) shows that $H^1_f(F_{\mathcal{Q}}, W_M) = H^1_{\mathrm{ur}}(F_{\mathcal{Q}}, W_M)$. $\square$

LEMMA 6.3. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathfrak{r} \in \mathcal{R}_{F,M}$, and w is an infinite place of F. Then $(\kappa_{F,\mathfrak{r},M})_w \in H^1_f(F_w, W_M)$.*

PROOF. Let $\tilde{w}$ be a place of $F(\mathfrak{r})$ above w. Since $F(\mathfrak{r})/F$ ramifies only at primes dividing $\mathfrak{r}$, w splits completely in $F(\mathfrak{r})/F$. Thus Lemma 4.13(ii) shows that $(\kappa_{F,\mathfrak{r},M})_w$ is the image of $(D_{\mathfrak{r},F}\mathbf{c}_{F(\mathfrak{r})})_{\tilde{w}}$ under the map

$$H^1(F(\mathfrak{r})_{\tilde{w}}, T) = H^1(F_w, T) \to H^1(F_w, W_M).$$

By Remark I.3.7, $H^1_f(F_w, T) = H^1(F_w, T)$ so the lemma follows from Lemma I.3.8(i). $\square$

REMARK 6.4. In the nonarchimedean case, if w is a prime of K not dividing $p\mathfrak{r}$, then Corollary 6.2(i) shows that $(\kappa_{F,\mathfrak{r},M})_w \in H^1_{\mathrm{ur}}(F_w, W_M)$. Unfortunately, for primes where T is ramified it may not be true that $H^1_f(F_w, W_M) = H^1_{\mathrm{ur}}(F_w, W_M)$. However, we do get immediately the following corollary, with only a slightly stronger assumption on $\mathfrak{r}$.

COROLLARY 6.5. *There is a positive integer m, independent of M, such that for every $K \subset_{\mathrm{f}} F \subset K_\infty$, every $\mathfrak{r} \in \mathcal{R}_{F,Mm}$, and every prime $\mathcal{Q}$ of F not dividing $p\mathfrak{r}$, $(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in H^1_f(F_{\mathcal{Q}}, W_M)$.*

PROOF. Let

$$m = \sup_{\substack{\text{primes } \mathfrak{q} \text{ of } K \\ \mathfrak{q} \nmid p}} [W^{\mathcal{I}_\mathfrak{q}} : (W^{\mathcal{I}_\mathfrak{q}})_{\mathrm{div}}]$$

where $\mathcal{I}_\mathfrak{q}$ is an inertia group for $\mathfrak{q}$ in G_K. Clearly m is finite, since these indices are all finite and almost all equal to 1. If $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathcal{Q}$ is a prime of F not dividing p, and $\mathfrak{q}$ is the prime of K below $\mathcal{Q}$, then $\mathcal{I}_\mathfrak{q}$ is also an inertia group of $\mathcal{Q}$ in G_F. Therefore by Lemma I.3.5(iii), m annihilates $H^1_{\mathrm{ur}}(F_{\mathcal{Q}}, W_{Mm})/H^1_f(F_{\mathcal{Q}}, W_{Mm})$, so by Corollary 6.2, $(m\kappa_{F,\mathfrak{r},Mm})_{\mathcal{Q}} \in H^1_f(F_{\mathcal{Q}}, W_{Mm})$. Lemma 4.13(iii) shows that $m\kappa_{F,\mathfrak{r},Mm}$ is the image of $\kappa_{F,\mathfrak{r},M}$, and the corollary follows. □

Corollary 6.5 is already strong enough to use in place of Theorem 5.1 in proving the Theorems of Chapter II. So one could skip the rest of this section if one is so inclined.

To prove Theorem 5.1 for primes $\mathcal{Q}$ where T may be ramified is much more delicate. We will mimic the construction of $\kappa_{F,\mathfrak{r},M}$ locally, and use Proposition 6.1 to show that $(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}}$ can be constructed inside $H^1(F_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}})$. The theorem will follow quickly from this.

Definition 6.6. Fix $\mathfrak{r} \in \mathcal{R}$ and a prime $\mathfrak{q}$ of K not dividing $\mathfrak{pr}$. Fix an inertia and decomposition group $\mathcal{I} \subset \mathcal{D} \subset G_K$ of $\mathfrak{q}$. If L is a finite extension of K, unramified at $\mathfrak{q}$, let S_L denote the set of primes of L above $\mathfrak{q}$ and abbreviate

$$H^i(L_{\mathfrak{q}}, W_M) = \bigoplus_{\mathcal{Q}\in S_L} H^i(L_{\mathcal{Q}}, W_M),$$
$$H^i(L_{\mathfrak{q}}, T^{\mathcal{I}}/MT^{\mathcal{I}}) = \bigoplus_{\mathcal{Q}\in S_L} H^i(L_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}})$$

where for each $\mathcal{Q} \in S_L$, $\mathcal{I}_{\mathcal{Q}}$ is the inertia group of $L_{\mathcal{Q}}$. (Since L/K is unramified at $\mathfrak{q}$, each $\mathcal{I}_{\mathcal{Q}}$ is conjugate to $\mathcal{I}$.) Write $(\,\cdot\,)_{\mathfrak{q}}$ or $\mathrm{res}_{\mathfrak{q}} : H^i(L, W_M) \to H^i(L_{\mathfrak{q}}, W_M)$ for the sum of the restriction maps. Note that $H^i(L_{\mathfrak{q}}, W_M)$ and $H^i(L_{\mathfrak{q}}, T^{\mathcal{I}}/MT^{\mathcal{I}})$ are $\mathrm{Gal}(L/K)$-modules: this can be seen directly (every $\sigma \in \mathrm{Gal}(L/K)$ induces an isomorphism

$$H^i(L_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}}) \xrightarrow{\sim} H^i(L_{\sigma\mathcal{Q}}, \sigma(T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}})) = H^i(L_{\sigma\mathcal{Q}}, T^{\mathcal{I}_{\sigma\mathcal{Q}}}/MT^{\mathcal{I}_{\sigma\mathcal{Q}}})$$

for every $\mathcal{Q}$, and summing these maps over $\mathcal{Q} \in S_L$ gives an automorphism of $H^i(L_{\mathfrak{q}}, T^{\mathcal{I}}/MT^{\mathcal{I}})$ and similarly for $H^i(L_{\mathfrak{q}}, W_M)$), or see Proposition B.5.2.

Write

$$W_M^f = T^{\mathcal{I}}/MT^{\mathcal{I}} \cong ((W^{\mathcal{I}})_{\mathrm{div}})_M \subset (W_M)^{\mathcal{I}} \subset W_M$$

and define

$$\mathbb{W}_M^f = \mathrm{Ind}(W_M^f) = \mathrm{Maps}(G_K, W_M^f) \subset \mathbb{W}_M.$$

As in Appendix B §4, let $\mathrm{Ind}_{\mathcal{D}}(W_M) \subset \mathbb{W}_M$ denote the subgroup of maps satisfying $f(hg) = hf(g)$ for every $h \in \mathcal{D}$, and similarly for $\mathrm{Ind}_{\mathcal{D}}(W_M^f) \subset \mathbb{W}_M^f$.

LEMMA 6.7. *For every $K \subset_{\mathrm{f}} F \subset K_\infty$, with notation as above we have a natural commutative diagram with exact columns*

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
W_M^{G_{F(\mathfrak{r})}} \arrow[r, hook] \arrow[d] & H^0(F(\mathfrak{r})_{\mathfrak{q}}, W_M) \arrow[d] & H^0(F(\mathfrak{r})_{\mathfrak{q}}, W_M^f) \arrow[l, hook'] \arrow[d] \\
\mathbb{W}_M^{G_{F(\mathfrak{r})}} \arrow[r, "\sim"] \arrow[d] & \mathbb{W}_M^{G_{F(\mathfrak{r})}} \arrow[d] & (\mathbb{W}_M^f)^{G_{F(\mathfrak{r})}} \arrow[l] \arrow[d] \\
(\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}} \arrow[r] \arrow[d, "\delta_{F(\mathfrak{r})}"'] & (\mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))^{G_{F(\mathfrak{r})}} \arrow[d, "\delta_{F(\mathfrak{r})_{\mathfrak{q}}}"'] & (\mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f))^{G_{F(\mathfrak{r})}} \arrow[l] \arrow[d, "\delta_{F(\mathfrak{r})_{\mathfrak{q}}, W_M^f}"'] \\
H^1(F(\mathfrak{r}), W_M) \arrow[r, "\mathrm{res}_{\mathfrak{q}}"] \arrow[d] & H^1(F(\mathfrak{r})_{\mathfrak{q}}, W_M) \arrow[d] & H^1(F(\mathfrak{r})_{\mathfrak{q}}, W_M^f) \arrow[l] \arrow[d] \\
0 & 0 & 0
\end{tikzcd}$$

PROOF. The three columns come from $G_{F(\mathfrak{r})}$-cohomology of the short exact sequences

$$0 \longrightarrow W_M \longrightarrow \mathbb{W}_M \longrightarrow \mathbb{W}_M/W_M \longrightarrow 0$$
$$0 \longrightarrow \mathrm{Ind}_{\mathcal{D}}(W_M) \longrightarrow \mathbb{W}_M \longrightarrow \mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M) \longrightarrow 0$$
$$0 \longrightarrow \mathrm{Ind}_{\mathcal{D}}(W_M^f) \longrightarrow \mathbb{W}_M^f \longrightarrow \mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f) \longrightarrow 0$$

respectively (the left-hand column is Proposition 4.5(i)), using Corollary B.4.4 and Proposition B.5.2. The horizontal arrows are the natural ones, and the commutativity follows from the functoriality of all the maps involved. □

We now need the following local analogue of Proposition 4.8.

PROPOSITION 6.8. *Suppose* $\mathbf{c}$ *is an Euler system and* $\mathfrak{r} \in \mathcal{R}$. *There are two families of* $\mathcal{O}[G_K]$*-module maps*

$$\{\mathbf{d}_{F,\mathfrak{q}} : \mathbf{X}_{F(\mathfrak{r})} \to (\mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))^{G_{F(\mathfrak{r})}} : K \subset_{\mathrm{f}} F \subset K_\infty\}$$
$$\{\mathbf{d}^f_{F,\mathfrak{q}} : \mathbf{X}_{F(\mathfrak{r})} \to (\mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f))^{G_{F(\mathfrak{r})}} : K \subset_{\mathrm{f}} F \subset K_\infty\}$$

lifting $\mathbf{c}$, *i.e., such that if* $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset K_\infty$,

(i) *the maps* $\mathbf{d}_{F,\mathfrak{q}}$ *(resp* $\mathbf{d}^f_{F,\mathfrak{q}}$*) are compatible with respect to the norm maps*

$$\mathbf{X}_{F'(\mathfrak{r})} \to \mathbf{X}_{F(\mathfrak{r})}, \quad (\mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))^{G_{F'(\mathfrak{r})}} \to (\mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))^{G_{F(\mathfrak{r})}},$$
$$(\mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f))^{G_{F'(\mathfrak{r})}} \to (\mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f))^{G_{F(\mathfrak{r})}},$$

(ii) *for every $K \subset_{\mathrm{f}} F \subset K_\infty$ and every $\mathfrak{s}$ dividing $\mathfrak{r}$, the compositions*

$$\mathbf{X}_{F(\mathfrak{r})} \xrightarrow{\mathbf{d}_{F,\mathfrak{q}}} (\mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))^{G_{F(\mathfrak{r})}} \xrightarrow{\delta_{F(\mathfrak{r})_\mathfrak{q}}} H^1(F(\mathfrak{r})_\mathfrak{q}, W_M)$$

$$\mathbf{X}_{F(\mathfrak{r})} \xrightarrow{\mathbf{d}^f_{F,\mathfrak{q}}} (\mathbb{W}^f_M/\mathrm{Ind}_{\mathcal{D}}(W^f_M))^{G_{F(\mathfrak{r})}} \xrightarrow{\delta_{F(\mathfrak{r})_\mathfrak{q},W^f_M}} H^1(F(\mathfrak{r})_\mathfrak{q}, W^f_M)$$

both send $x_{F(\mathfrak{s})}$ to $(\mathbf{c}_{F(\mathfrak{s})})_\mathfrak{q}$.

Each $\mathbf{d}_{F,\mathfrak{q}}$ is determined uniquely up to an element of $\mathrm{Hom}_{\mathcal{O}[G_K]}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M)$, and each $\mathbf{d}^f_{F,\mathfrak{q}}$ up to $\mathrm{Hom}_{\mathcal{O}[G_K]}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}^f_M)$, by these two conditions.

Proof. For each $K \subset_{\mathrm{f}} F \subset K_\infty$ we have maps (see Lemma 2.3)

$$\begin{array}{ccccc} x_{F(\mathfrak{s})} & \mapsto & \mathbf{c}_{F(\mathfrak{s})} & \mapsto & (\mathbf{c}_{F(\mathfrak{s})})_\mathfrak{q} \\ \mathbf{X}_{F(\mathfrak{r})} & \longrightarrow & H^1(F(\mathfrak{r}), T) & \longrightarrow & H^1(F(\mathfrak{r})_\mathfrak{q}, T) \\ & & \downarrow & & \downarrow \\ & & H^1(F(\mathfrak{r}), W_M) & \longrightarrow & H^1(F(\mathfrak{r})_\mathfrak{q}, W_M). \end{array} \tag{7}$$

By Proposition 6.1, for every $\mathfrak{s}$ dividing $\mathfrak{r}$ and every $\mathcal{Q} \in S_{F(\mathfrak{r})}$,

$$(\mathbf{c}_{F(\mathfrak{s})})_\mathcal{Q} \in H^1_{\mathrm{ur}}(F(\mathfrak{r})_\mathcal{Q}, T) = H^1(F(\mathfrak{r})^{\mathrm{ur}}_\mathcal{Q}/F(\mathfrak{r})_\mathcal{Q}, T^{\mathcal{I}_\mathcal{Q}}) \subset H^1(F(\mathfrak{r})_\mathcal{Q}, T^{\mathcal{I}_\mathcal{Q}})$$

so the map $\mathbf{X}_{F(\mathfrak{r})} \to H^1(F(\mathfrak{r})_\mathfrak{q}, W_M)$ in (7) factors through a G_K-equivariant map

$$\mathbf{X}_{F(\mathfrak{r})} \to H^1(F(\mathfrak{r})_\mathfrak{q}, W^f_M). \tag{8}$$

To prove the proposition we need to lift these to maps $\mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M)$ and $\mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}^f_M/\mathrm{Ind}_{\mathcal{D}}(W^f_M)$ in the center and right-hand columns, respectively, of the diagram of Lemma 6.7. We will do this by mimicking the proof of Proposition 4.8. We describe the proof only for the right-hand column; the other proof is exactly the same (and see Remark 6.9 below).

Since we have assumed that the decomposition group of $\mathfrak{q}$ in K_∞/K is infinite, we can find a $\mathbf{Z}_p$-extension K'_∞ of K in K_∞ such that K'_∞ has only finitely many primes above $\mathfrak{q}$. Then for each finite extension L of K, $\cup_{K \subset_{\mathrm{f}} F \subset K'_\infty L} H^0(F(\mathfrak{r})_\mathfrak{q}, W_M)$ is a finitely-generated $\mathbf{Z}_p$-module, so by Lemma B.3.2,

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^0(F(\mathfrak{r})_\mathfrak{q}, W_M) = \varprojlim_{K \subset_{\mathrm{f}} L \subset K_\infty} \; \varprojlim_{KL \subset_{\mathrm{f}} F \subset K'_\infty L} H^0(F(\mathfrak{r})_\mathfrak{q}, W_M) = 0$$

(inverse limits with respect to the norm maps). Proposition B.2.7(ii) shows that each $H^1(F(\mathfrak{r})_\mathfrak{q}, W_M)$ is finite, so exactly as in Lemma 4.7 the inverse limit over $K \subset_{\mathrm{f}} F \subset K_\infty$ of the right-hand column of the diagram of Lemma 6.7 is a short exact sequence

$$0 \to \varprojlim_F (\mathbb{W}^f_M)^{G_{F(\mathfrak{r})}} \to \varprojlim_F (\mathbb{W}^f_M/\mathrm{Ind}_{\mathcal{D}}(W^f_M))^{G_{F(\mathfrak{r})}} \to \varprojlim_F H^1(F(\mathfrak{r})_\mathfrak{q}, W^f_M) \to 0.$$

The maps (8) induce a map

$$\mathbf{X}_{\infty,\mathfrak{r}} \longrightarrow \varprojlim_F H^1(F(\mathfrak{r})_\mathfrak{q}, W^f_M),$$

and exactly as in Lemma 4.6, $\varprojlim (\mathbb{W}^f_M)^{G_{F(\mathfrak{r})}}$ is a free $(\mathcal{O}/M\mathcal{O})[[\mathrm{Gal}(K_\infty(\mathfrak{r})/K)]]$-module. As in Proposition 4.8, Proposition 3.4 now shows that this map lifts to a map

$$\mathbf{X}_{\infty,\mathfrak{r}} \longrightarrow \varprojlim_{F} (\mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f))^{G_{F(\mathfrak{r})}}.$$

Also as in Proposition 4.8, Corollary 3.2 shows that this in turn induces maps

$$\mathbf{d}_{F,\mathfrak{q}}^f : \mathbf{X}_{F(\mathfrak{r})} \to (\mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f))^{G_{F(\mathfrak{r})}}$$

having the desired properties. The uniqueness is clear from the diagram of Lemma 6.7. □

REMARK 6.9. To construct the maps $\mathbf{d}_{F,\mathfrak{q}}$ in Proposition 6.8 it is enough to construct *either* the global maps $\mathbf{d}_F$ of Proposition 4.8 or the "unramified" maps $\mathbf{d}_{F,\mathfrak{q}}^f$ of Proposition 6.8 and then map them into $(\mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))^{G_{F(\mathfrak{r})}}$ using the diagram of Lemma 6.7.

In fact, that is how our proof of Theorem 5.1 will proceed. We construct the maps $\mathbf{d}_F$ and $\mathbf{d}_{F,\mathfrak{q}}^f$ lifting our Euler system $\mathbf{c}$. This gives us two different constructions of $\mathbf{d}_{F,\mathfrak{q}}$ and we compare them using the uniqueness assertion of Proposition 6.8.

PROOF OF THEOREM 5.1. Keep the notation from the beginning of this section, so $M \in \mathcal{O}$ is nonzero and we now suppose that $\mathfrak{r} \in \mathcal{R}_{F,M}$. Fix a lift $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M/W_M$ (resp. $\mathbf{d}_{\mathfrak{q}}^f : \mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M^f/\mathrm{Ind}_{\mathcal{D}}(W_M^f)$) of $\mathbf{c}$ as in Proposition 4.8 (resp. Proposition 6.8). Write $\mathbf{d}_{\mathfrak{q}}$ (resp $\mathbf{d}'_{\mathfrak{q}}$) for the image of $\mathbf{d}$ (resp $\mathbf{d}_{\mathfrak{q}}^f$) in $\mathrm{Hom}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}(W_M))$ in the diagram of Lemma 6.7. From the uniqueness portion of Proposition 6.8 it follows that

$$\mathbf{d}_{\mathfrak{q}} - \mathbf{d}'_{\mathfrak{q}} \in \mathrm{image}(\mathrm{Hom}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M^{G_{F(\mathfrak{r})}}))$$

In particular, Lemma 4.2 shows that, in the center column of the diagram of Lemma 6.7,

$$\mathbf{d}_{\mathfrak{q}}(D_{\mathfrak{r},F}x_{F(\mathfrak{r})}) - \mathbf{d}'_{\mathfrak{q}}(D_{\mathfrak{r},F}x_{F(\mathfrak{r})}) \in \mathrm{image}(\mathbb{W}_M^{G_F}) = \ker(\delta_{F_{\mathfrak{q}}}).$$

By definition, $\kappa_{F,\mathfrak{r},M} = \delta_F(\mathbf{d}(D_{\mathfrak{r},F}x_{F(\mathfrak{r})}))$. Therefore we see from the diagram of Lemma 6.7 that $(\kappa_{F,\mathfrak{r},M})_{\mathfrak{q}}$ is equal to the image of $\mathbf{d}_{\mathfrak{q}}^f(D_{\mathfrak{r},F}x_{F(\mathfrak{r})})$ in $H^1(F_{\mathfrak{q}}, W_M)$. In particular we conclude that for every prime $\mathcal{Q}$ of F above $\mathfrak{q}$,

$$(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in \mathrm{image}\big(H^1(F_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}}) \to H^1(F_{\mathcal{Q}}, W_M)\big).$$

By Corollary 6.2(i), we also have that

$$(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in H^1_{\mathrm{ur}}(F(\mathfrak{r})_{\mathcal{Q}}, W_M) = H^1(F(\mathfrak{r})_{\mathcal{Q}}^{\mathrm{ur}}/F(\mathfrak{r})_{\mathcal{Q}}, W_M^{\mathcal{I}_{\mathcal{Q}}})$$

and it follows that

$$(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in \mathrm{image}\big(H^1(F(\mathfrak{r})_{\mathcal{Q}}^{\mathrm{ur}}/F_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}}) \to H^1(F_{\mathcal{Q}}, W_M)\big).$$

Since $\mathrm{Gal}(F_{\mathcal{Q}}^{\mathrm{ur}}/F_{\mathcal{Q}})$ has cohomological dimension one, cohomology of the short exact sequence

$$0 \longrightarrow T^{\mathcal{I}_{\mathcal{Q}}} \xrightarrow{M} T^{\mathcal{I}_{\mathcal{Q}}} \longrightarrow T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}} \longrightarrow 0$$

gives a surjective map

$$H^1_{\mathrm{ur}}(F_{\mathcal{Q}}, T) = H^1(F_{\mathcal{Q}}^{\mathrm{ur}}/F_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}) \twoheadrightarrow H^1(F_{\mathcal{Q}}^{\mathrm{ur}}/F_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}/MT^{\mathcal{I}_{\mathcal{Q}}}).$$

Thus we conclude finally that $(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}}$ belongs to the image of $H^1_{\mathrm{ur}}(F_{\mathcal{Q}},T)$, so by Lemmas I.3.5(ii) and I.3.8(i),

$$(\kappa_{F,\mathfrak{r},M})_{\mathcal{Q}} \in H^1_f(F_{\mathcal{Q}},W_M). \qquad \square$$

7. Local behavior at primes dividing $\mathfrak{r}$

Fix for this section an Euler system $\mathbf{c}$ for T, a nonzero $M \in \mathcal{O}$, a prime $\mathfrak{q} \in \mathcal{R}$, $\mathfrak{r} \in \mathcal{R}$, and $K \subset_{\mathrm{f}} F \subset K_\infty$.

Fix a prime $\mathfrak{Q}$ of $\bar{K}$ above $\mathfrak{q}$ and let $\mathcal{I} \subset \mathcal{D}$ be the inertia and decomposition group, respectively, of $\mathfrak{Q}$ in G_K. Since $K(\mathfrak{q})/K(1)$ is totally ramified at $\mathfrak{q}$, $\mathcal{I}$ projects onto $\Gamma_{\mathfrak{q}}$, so we can choose a lift of $\sigma_{\mathfrak{q}}$ to $\mathcal{I}$ which we will also denote by $\sigma_{\mathfrak{q}}$. With this choice we will view

$$N_{\mathfrak{q}} = \sum_{i=1}^{[K(\mathfrak{q}):K(1)]} \sigma_{\mathfrak{q}}^i, \quad D_{\mathfrak{q}} = \sum_{i=0}^{[K(\mathfrak{q}):K(1)]-1} i\sigma_{\mathfrak{q}}^i \quad \in \mathbf{Z}[\mathcal{I}],$$

but, writing $m = [K(\mathfrak{q}) : K(1)]$, we no longer have $\sigma_{\mathfrak{q}}^m = 1$ in $\mathcal{I}$, so instead of the identity (4) we have

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} = m\sigma_{\mathfrak{q}}^m - N_{\mathfrak{q}} \tag{9}$$

in $\mathbf{Z}[\mathcal{I}]$. Fix also some choice $\mathrm{Fr}_{\mathfrak{q}} \in \mathcal{D}$ of Frobenius for $\mathfrak{Q}$, and fix a lift of the element $N_{F(1)/F}$ of Definition 4.10 to $\mathbf{Z}[G_F]$, so that we can view $D_{\mathfrak{r},F} \in \mathbf{Z}[G_F]$.

LEMMA 7.1. *Suppose $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M/W_M$ is a lifting of $\mathbf{c}$ as in Proposition 4.8, and $\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) \in \mathbb{W}_M$ is a lift of $\mathbf{d}(x_{F(\mathfrak{r})})$. For every $\gamma \in G_K$ and $\sigma, \sigma' \in \mathcal{D}$,*

$$\sigma\sigma'\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) = \sigma'\sigma\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}).$$

PROOF. Let $\mathcal{I}_{F(\mathfrak{r})} = \mathcal{I} \cap G_{F(\mathfrak{r})}$. Since T is unramified at $\mathfrak{q}$, Proposition 6.1 shows that

$$\mathrm{res}_{\mathcal{I}_{F(\mathfrak{r})}}(\gamma\mathbf{c}_{F(\mathfrak{r})}) = 0 \quad \text{in } H^1(\mathcal{I}_{F(\mathfrak{r})}, W_M) = \mathrm{Hom}(\mathcal{I}_{F(\mathfrak{r})}, W_M).$$

Thus every cocycle representing $\gamma\mathbf{c}_{F(\mathfrak{r})}$ vanishes on $\mathcal{I}_{F(\mathfrak{r})}$. In particular by Proposition 4.5(ii),

$$(\sigma - 1)\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) = 0 \quad \text{in } \mathbb{W}_M, \text{ for every } \sigma \in \mathcal{I}_{F(\mathfrak{r})}. \tag{10}$$

Since $\mathcal{D}/\mathcal{I}$ and $\mathrm{Gal}(F(\mathfrak{r})/K)$ are abelian, the commutator subgroup of $\mathcal{D}$ is contained in both $\mathcal{I}$ and $G_{F(\mathfrak{r})}$. In particular if we apply (10) with $\sigma = \sigma^{-1}\sigma'^{-1}\sigma\sigma' \in \mathcal{I}_{F(\mathfrak{r})}$, the lemma follows. $\square$

REMARK 7.2. Suppose in Lemma 7.1 that σ, σ' belong to G_K, but not necessarily to $\mathcal{D}$. Then $\sigma\sigma'\mathbf{d}(x_{F(\mathfrak{r})}) = \sigma'\sigma\mathbf{d}(x_{F(\mathfrak{r})})$ since $\mathbf{d}$ is G_K-equivariant and the action of G_K on $x_{F(\mathfrak{r})}$ factors through an abelian extension of K. However, the action of G_K on $\hat{\mathbf{d}}(x_{F(\mathfrak{r})})$ will *not* in general factor through an abelian extension of K so it is *not* in general true that $\sigma\sigma'\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) = \sigma'\sigma\hat{\mathbf{d}}(x_{F(\mathfrak{r})})$. However, Lemma 7.1 shows that this does hold if $\sigma, \sigma' \in \mathcal{D}$. We will use this repeatedly below.

Note that Lemma 7.1 applies whether or not $\mathfrak{q}$ divides $\mathfrak{r}$.

The following lemma is essentially equivalent to Theorem 5.4, which will follow easily from it.

LEMMA 7.3. *Suppose* $\mathfrak{r} \in \mathcal{R}$, $\mathfrak{q} \in \mathcal{R}_{K,M}$ *does not divide* $\mathfrak{r}$, *and* $K \subset_{\mathrm{f}} F \subset K_\infty$. *Fix a lifting* $\mathbf{d} : \mathbf{X}_{F(\mathfrak{rq})} \to \mathbb{W}_M/W_M$ *of* $\mathbf{c}$ *as in Proposition* 4.8, *and fix liftings* $\hat{\mathbf{d}}(x_{F(\mathfrak{rq})}), \hat{\mathbf{d}}(x_{F(\mathfrak{r})}) \in \mathbb{W}_M$ *of* $\mathbf{d}(x_{F(\mathfrak{rq})})$ *and* $\mathbf{d}(x_{F(\mathfrak{r})})$, *respectively. Then for every* $\gamma \in G_K$,

$$N_\mathfrak{q}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{rq})}) = P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}).$$

PROOF. We will abbreviate $P_\mathfrak{q}(x) = P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;x)$. Note that

$$N_\mathfrak{q}\gamma\mathbf{d}(x_{F(\mathfrak{rq})}) = P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\mathbf{d}(x_{F(\mathfrak{r})})$$

since $\mathbf{d}$ is G_K-equivariant and $N_\mathfrak{q}x_{F(\mathfrak{rq})} = P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})x_{F(\mathfrak{r})}$, so

$$N_\mathfrak{q}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{rq})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) \in W_M.$$

First we show that the image of $N_\mathfrak{q}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{rq})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})})$ in W_M is independent of the choices of $\mathbf{d}$ and $\hat{\mathbf{d}}$. Suppose we replace $\mathbf{d}$ by another choice $\mathbf{d}'$. By Proposition 4.8, $\mathbf{d}' = \mathbf{d} + \mathbf{d}_0$ with $\mathbf{d}_0 \in \mathrm{Hom}_{G_K}(\mathbf{X}_{F(\mathfrak{rq})}, \mathbb{W}_M)$. Therefore if we choose lifts $\hat{\mathbf{d}}'(x_{F(\mathfrak{rq})}), \hat{\mathbf{d}}'(x_{F(\mathfrak{r})}) \in \mathbb{W}_M$ of $\mathbf{d}'(x_{F(\mathfrak{rq})})$ and $\mathbf{d}'(x_{F(\mathfrak{r})})$, they must satisfy

$$\hat{\mathbf{d}}'(x_{F(\mathfrak{rq})}) = \hat{\mathbf{d}}(x_{F(\mathfrak{rq})}) + \mathbf{d}_0(x_{F(\mathfrak{rq})}) + t, \quad \hat{\mathbf{d}}'(x_{F(\mathfrak{r})}) = \hat{\mathbf{d}}(x_{F(\mathfrak{r})}) + \mathbf{d}_0(x_{F(\mathfrak{r})}) + t'$$

where $t, t' \in W_M$. Thus

$$\begin{aligned}(N_\mathfrak{q}\gamma\hat{\mathbf{d}}'(x_{F(\mathfrak{rq})}) &- P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}'(x_{F(\mathfrak{r})})) - (N_\mathfrak{q}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{rq})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}))\\ &= \mathbf{d}_0(\gamma(N_\mathfrak{q}x_{F(\mathfrak{rq})} - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})x_{F(\mathfrak{r})})) + N_\mathfrak{q}\gamma t - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma t'\\ &= N_\mathfrak{q}\gamma t - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma t'\end{aligned}$$

since $\mathbf{d}_0$ is G_K-equivariant. This is zero because $\sigma_\mathfrak{q}$ fixes W_M, $M \mid [K(\mathfrak{q}) : K]$, and $P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})$ annihilates W_M (Lemma 1.2(iv)).

Next we will make a useful choice of $\hat{\mathbf{d}}(x_{F(\mathfrak{r})})$ and $\hat{\mathbf{d}}(x_{F(\mathfrak{rq})})$. Choose $k \in \mathbf{Z}^+$ so that $\mathrm{Fr}_\mathfrak{q}^k$ is the identity on both $F(\mathfrak{rq})$ and W_M, and let k_p be the largest power of p dividing k. Since the decomposition group of $\mathfrak{q}$ in $\mathrm{Gal}(K_\infty/K)$ is infinite, we can fix a finite extension F' of F in K_∞ such that the decomposition group of $\mathfrak{q}$ in $F'(\mathfrak{rq})/F(\mathfrak{rq})$ has order divisible by k_pM. Choose a lift $\mathbf{d} : \mathbf{X}_{F'(\mathfrak{rq})} \to \mathbb{W}_M/W_M$ of $\mathbf{c}$ as in Proposition 4.8.

Let $H \subset \mathrm{Gal}(F'(\mathfrak{rq})/F(\mathfrak{rq}))$ be the subgroup generated by $\mathrm{Fr}_\mathfrak{q}^k$. Fix a subset $B \subset G_{F(\mathfrak{rq})}$ which is a set of coset representatives of $\mathrm{Gal}(F'(\mathfrak{rq})/F(\mathfrak{rq}))/H$. Write

$$\mathbf{N}' = \sum_{i=0}^{|H|-1} \mathrm{Fr}_\mathfrak{q}^{ki}, \quad \mathbf{N}'' = \sum_{\beta \in B} \beta \quad \in \mathbf{Z}[G_{F(\mathfrak{rq})}].$$

The product $\mathbf{N}'\mathbf{N}''$ restricts to the norm from $F'(\mathfrak{rq})$ to $F(\mathfrak{rq})$, so in particular

$$\mathbf{N}'\mathbf{N}''x_{F'(\mathfrak{rq})} = x_{F(\mathfrak{rq})} \quad \text{and} \quad \mathbf{N}'\mathbf{N}''x_{F'(\mathfrak{r})} = x_{F(\mathfrak{r})} \tag{11}$$

in $\mathbf{X}_{F'(\mathfrak{rq})}$.

Choose liftings $\hat{\mathbf{d}}(x_{F'(\mathfrak{rq})}), \hat{\mathbf{d}}(x_{F'(\mathfrak{r})}) \in \mathbb{W}_M$ of $\mathbf{d}(x_{F'(\mathfrak{rq})}), \mathbf{d}(x_{F'(\mathfrak{r})}) \in \mathbb{W}_M/W_M$, respectively, and define

$$\hat{\mathbf{d}}(x_{F(\mathfrak{rq})}) = \gamma^{-1}\mathbf{N}'\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{rq})}), \quad \hat{\mathbf{d}}(x_{F(\mathfrak{r})}) = \gamma^{-1}\mathbf{N}'\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r})}).$$

It follows from (11) that these are lifts of $\mathbf{d}(x_{F(\mathfrak{r}\mathfrak{q})})$ and $\mathbf{d}(x_{F(\mathfrak{r})})$, respectively, to $\mathbb{W}_M$. We will show that with these choices $N_\mathfrak{q}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) = 0$, which will prove the lemma.

Note that $\mathbf{N}'$, $P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})$, and $N_\mathfrak{q}$ all belong to $\mathcal{O}[\mathcal{D}]$ because $\mathrm{Fr}_\mathfrak{q}$ and $\sigma_\mathfrak{q}$ do, so by Lemma 7.1 these elements commute in their action on $\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r}\mathfrak{q})})$ and $\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r})})$. Thus

$$\begin{aligned}
N_\mathfrak{q}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) &- P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \\
&= N_\mathfrak{q}\mathbf{N}'\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r}\mathfrak{q})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{N}'\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r})}) \\
&= \mathbf{N}'(N_\mathfrak{q}\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r}\mathfrak{q})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r})})) \in \mathbf{N}'W_M,
\end{aligned}$$

the final inclusion because $N_\mathfrak{q}\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r}\mathfrak{q})}) - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{N}''\gamma\hat{\mathbf{d}}(x_{F'(\mathfrak{r})}) \in \mathbb{W}_M$ projects to $\mathbf{N}''\gamma\mathbf{d}(N_\mathfrak{q}x_{F'(\mathfrak{r}\mathfrak{q})} - P_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})x_{F'(\mathfrak{r})}) = 0$ in $\mathbb{W}_M/W_M$. Since $\mathrm{Fr}_\mathfrak{q}^k$ fixes W_M,

$$\mathbf{N}'W_M \subset |H|\; W_M.$$

Now observe that H has index dividing k_p in the decomposition group of $\mathfrak{q}$ in $F'(\mathfrak{r}\mathfrak{q})/F(\mathfrak{r}\mathfrak{q})$, so in particular M divides $|H|$. This completes the proof. □

Proof of Theorem 5.4. Keep the notation from the beginning of this section, and suppose now that $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,M}$. Choose $Q_\mathfrak{q} \in \mathcal{O}[x]$ as in Lemma 5.2, so that $Q_\mathfrak{q}(x)(x-1) \equiv P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;x) \pmod{M}$. To prove the theorem we need to show that, for some (or equivalently, for every) choice of cocycles representing $\kappa_{F,\mathfrak{r},M}$ and $\kappa_{F,\mathfrak{r}\mathfrak{q},M}$,

$$Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) = \kappa_{F,\mathfrak{r}\mathfrak{q},M}(\sigma_\mathfrak{q}) \in W_M.$$

Fix $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r}\mathfrak{q})} \to \mathbb{W}_M/W_M$ lifting $\mathbf{c}$ as in Proposition 4.8, and choose liftings $\hat{\mathbf{d}}(x_{F(\mathfrak{r})})$, $\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \in \mathbb{W}_M$ of $\mathbf{d}(x_{F(\mathfrak{r})})$, $\mathbf{d}(x_{F(\mathfrak{r}\mathfrak{q})}) \in \mathbb{W}_M/W_M$, respectively. Lemma 4.12 shows that

$$\begin{aligned}
\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) &= (\mathrm{Fr}_\mathfrak{q}-1)D_{\mathfrak{r},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) \in W_M \\
\kappa_{F,\mathfrak{r}\mathfrak{q},M}(\sigma_\mathfrak{q}) &= (\sigma_\mathfrak{q}-1)D_{\mathfrak{r}\mathfrak{q},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \in W_M.
\end{aligned}$$

Also

$$Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})(\mathrm{Fr}_\mathfrak{q}^{-1}-1)\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) = P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) = 0$$

by Lemma 1.2(iv). Thus, using Lemma 7.1 repeatedly to commute elements of $\mathcal{O}[\mathcal{D}]$, and using (9), we see

$$\begin{aligned}
Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})&\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) - \kappa_{F,\mathfrak{r}\mathfrak{q},M}(\sigma_\mathfrak{q}) \\
&= Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\mathrm{Fr}_\mathfrak{q}^{-1}\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) - \kappa_{F,\mathfrak{r}\mathfrak{q},M}(\sigma_\mathfrak{q}) \\
&= Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\mathrm{Fr}_\mathfrak{q}^{-1}(\mathrm{Fr}_\mathfrak{q}-1)D_{\mathfrak{r},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) - (\sigma_\mathfrak{q}-1)D_\mathfrak{q}D_{\mathfrak{r},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \\
&= -P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})D_{\mathfrak{r},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) + N_\mathfrak{q}D_{\mathfrak{r},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \\
&\qquad - [K(\mathfrak{q}):K(1)]\sigma_\mathfrak{q}^{[K(\mathfrak{q}):K(1)]}D_{\mathfrak{r},F}\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}).
\end{aligned}$$

Since $\mathfrak{q} \in \mathcal{R}_{F,M}$ we have $M \mid [K(\mathfrak{q}):K(1)]$. Thus by Lemma 7.3 we conclude that $Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})\kappa_{F,\mathfrak{r},M}(\mathrm{Fr}_\mathfrak{q}) - \kappa_{F,\mathfrak{r}\mathfrak{q},M}(\sigma_\mathfrak{q}) = 0$ in W_M, as desired. □

8. The congruence

Although we will not need it, we can now prove the following corollary (the "congruence condition" for an Euler system) which was promised in Remark II.1.5. We again abbreviate $P_{\mathfrak{q}}(x) = P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;x)$.

COROLLARY 8.1. *Suppose* $\mathbf{c}$ *is an Euler system for* T, $K \subset_{\mathrm{f}} F \subset K_\infty$, $\mathfrak{q} \in \mathcal{R}$ *is prime, and* $\mathfrak{r}\mathfrak{q} \in \mathcal{R}$. *Then for every prime* $\mathcal{Q}$ *of* $F(\mathfrak{r}\mathfrak{q})$ *dividing* $\mathfrak{q}$,

$$(\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})})_{\mathcal{Q}} = \frac{P_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) - P_{\mathfrak{q}}(\mathbf{N}(\mathfrak{q})\mathrm{Fr}_{\mathfrak{q}}^{-1})}{[K(\mathfrak{q}):K(1)]}(\mathbf{c}_{F(\mathfrak{r})})_{\mathcal{Q}} \quad \in H^1(F(\mathfrak{r}\mathfrak{q})_{\mathcal{Q}}, T).$$

PROOF. Write

$$R(x) = \frac{P_{\mathfrak{q}}(x) - P_{\mathfrak{q}}(\mathbf{N}(\mathfrak{q})x)}{[K(\mathfrak{q}):K(1)]}.$$

Since $[K(\mathfrak{q}):K(1)]$ divides $(\mathbf{N}(\mathfrak{q})-1)$, $R(x) \in \mathcal{O}[x]$.

Keep the notation and setting from the beginning of the previous section, and let

$$c = \mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} - R(\mathrm{Fr}_{\mathfrak{q}}^{-1})\mathbf{c}_{F(\mathfrak{r})} \in H^1(F(\mathfrak{r}\mathfrak{q}), T).$$

For every nonzero $M \in \mathcal{O}$ let $(c)_{\mathcal{Q},M}$ be the image of c in $H^1(F(\mathfrak{r}\mathfrak{q})_{\mathcal{Q}}, W_M)$. By Proposition B.2.3, $H^1(F(\mathfrak{r}\mathfrak{q})_{\mathcal{Q}}, T) = \varprojlim H^1(F(\mathfrak{r}\mathfrak{q})_{\mathcal{Q}}, W_M)$, so to prove the corollary it will suffice to show that $(c)_{\mathcal{Q},M} = 0$ for every M.

Fix an M divisible by $[K(\mathfrak{q}):K(1)]$, and a lifting $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r}\mathfrak{q})} \to \mathbb{W}_M/W_M$ of $\mathbf{c}$ as in Proposition 4.8. Choose elements $\hat{\mathbf{d}}(x_{F(\mathfrak{r})}), \hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \in \mathbb{W}_M$ lifting $\mathbf{d}(x_{F(\mathfrak{r})}), \mathbf{d}(x_{F(\mathfrak{r}\mathfrak{q})}) \in \mathbb{W}_M/W_M$, respectively. Fix a Frobenius element $\mathrm{Fr}_{\mathfrak{q}}$ corresponding to a prime of $\bar{K}$ above $\mathcal{Q}$. Then a Frobenius element for $\mathcal{Q}$ in $G_{F(\mathfrak{r}\mathfrak{q})}$ is given by $\varphi = \mathrm{Fr}_{\mathfrak{q}}^k$ for some k. By Proposition 6.1, $(c)_{\mathcal{Q},M} \in H^1_{\mathrm{ur}}(F(\mathfrak{r}\mathfrak{q})_{\mathcal{Q}}, W_M)$, and by Lemma I.3.2(i) there is an isomorphism

$$\begin{array}{ccc} H^1_{\mathrm{ur}}(F(\mathfrak{r}\mathfrak{q})_{\mathcal{Q}}, W_M) & \xrightarrow{\sim} & W_M/(\varphi-1)W_M \\ (c)_{\mathcal{Q},M} & \mapsto & c(\varphi). \end{array}$$

Proposition 4.5(ii) shows that $\gamma \mapsto (\gamma-1)(\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - R(\mathrm{Fr}_{\mathfrak{q}}^{-1})\hat{\mathbf{d}}(x_{F(\mathfrak{r})})) \in W_M$ is a cocycle representing $(c)_{\mathcal{Q},M}$, so

$$(c)_{\mathcal{Q},M} = 0 \quad \Leftrightarrow \quad (\varphi-1)(\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - R(\mathrm{Fr}_{\mathfrak{q}}^{-1})\hat{\mathbf{d}}(x_{F(\mathfrak{r})})) \in (\varphi-1)W_M.$$

Note that $(\varphi-1)\hat{\mathbf{d}}(x_{F(\mathfrak{r})}), (\varphi-1)\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) \in W_M$ and $N_{\mathfrak{q}}$, $\varphi-1$, $P_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) \in \mathcal{O}[\mathcal{D}]$. Therefore

$$\begin{aligned} [K(\mathfrak{q}):K(1)](\varphi-1)&(\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - R(\mathrm{Fr}_{\mathfrak{q}}^{-1})\hat{\mathbf{d}}(x_{F(\mathfrak{r})})) \\ &= N_{\mathfrak{q}}(\varphi-1)\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - P_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})(\varphi-1)\hat{\mathbf{d}}(x_{F(\mathfrak{r})}) \\ &= (\varphi-1)(N_{\mathfrak{q}}\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - P_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})\hat{\mathbf{d}}(x_{F(\mathfrak{r})})) \end{aligned}$$

the first equality since $\sigma_{\mathfrak{q}}$ fixes W_M and $P_{\mathfrak{q}}(\mathbf{N}(\mathfrak{q})\mathrm{Fr}_{\mathfrak{q}}^{-1})$ annihilates W_M (Lemma 1.2(ii)), and the second by Lemma 7.1. Lemma 7.3 shows that the image of $N_{\mathfrak{q}}\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - P_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})\hat{\mathbf{d}}(x_{F(\mathfrak{r})})$ under the projection $W_M \twoheadrightarrow W_{[K(\mathfrak{q}):K(1)]}$ is zero, and we conclude that

$$[K(\mathfrak{q}):K(1)](\varphi-1)(\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - R(\mathrm{Fr}_{\mathfrak{q}}^{-1})\hat{\mathbf{d}}(x_{F(\mathfrak{r})})) \in [K(\mathfrak{q}):K(1)](\varphi-1)W_M.$$

It follows that $(c)_{\mathcal{Q},M/[K(\mathfrak{q}):K(1)]} = 0$, and since this holds for every M the corollary is proved. □

Example 8.2. Suppose $T = \mathbf{Z}_p(1)$. Then for every $\mathfrak{r} \in \mathcal{R}$ and every prime $\mathcal{Q}$ of $F(\mathfrak{r})$ not dividing p (see Example I.2.1)

$$H^1(F(\mathfrak{r}), T) = (F(\mathfrak{r})^\times)\hat{}, \quad H^1(F(\mathfrak{r})_{\mathcal{Q}}, T) = (F(\mathfrak{r})_{\mathcal{Q}}^\times)\hat{} \cong \Bbbk_{\mathcal{Q}}^\times \otimes \mathbf{Z}_p$$

where $(\,\cdot\,)\hat{}$ denotes the p-adic completion and $\Bbbk_{\mathcal{Q}}$ is the residue field of $F(\mathfrak{r})$ modulo $\mathcal{Q}$. In this case

$$P_{\mathfrak{q}}(x) = \det(1 - \mathrm{Fr}_{\mathfrak{q}}^{-1}x | \mathbf{Z}_p) = 1 - x,$$

so

$$\frac{P_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) - P_{\mathfrak{q}}(\mathbf{N}(\mathfrak{q})\mathrm{Fr}_{\mathfrak{q}}^{-1})}{[K(\mathfrak{q}) : K]} = \frac{\mathbf{N}(\mathfrak{q}) - 1}{[K(\mathfrak{q}) : K]}\mathrm{Fr}_{\mathfrak{q}}^{-1}.$$

Thus viewing $\mathbf{c}_{F(\mathfrak{r})}, \mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} \in (F(\mathfrak{r})^\times)\hat{}$, Corollary 8.1 in this case says

$$\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} / \mathbf{c}_{F(\mathfrak{r})}^{\frac{\mathbf{N}(\mathfrak{q})-1}{[K(\mathfrak{q}):K]}\mathrm{Fr}_{\mathfrak{q}}^{-1}}$$

has order prime to p in $\Bbbk_{\mathcal{Q}}^\times$. (This can be viewed as the "p-part" of a hypothetical congruence

$$\mathbf{c}_{F(\mathfrak{r}\mathfrak{q})} \equiv \mathbf{c}_{F(\mathfrak{r})}^{\frac{\mathbf{N}(\mathfrak{q})-1}{[K(\mathfrak{q}):K]}\mathrm{Fr}_{\mathfrak{q}}^{-1}} \pmod{\mathcal{Q}}.)$$

For the Euler system of cyclotomic units discussed in Chapter III §2, Corollary 8.1 is a reflection of the congruence

$$1 - \zeta_{rq} \equiv 1 - \zeta_r^{\mathrm{Fr}_q^{-1}}$$

modulo every prime above q (which in turn follows from the observation $\zeta_q \equiv 1$).

CHAPTER V

Bounding the Selmer group

In this chapter we will prove Theorems II.2.2 (in §2) and II.2.3 (in §3). For every power M of p we will choose inductively a finite subset Σ of primes in $\mathcal{R}_{K,M}$. As $\mathfrak{r}$ runs through products of primes in Σ, Theorem IV.5.1 shows that the derivative cohomology classes $\kappa_{K,\mathfrak{r},M}$ defined in Chapter IV belong to $\mathcal{S}^{\Sigma\cup\Sigma_p}(K, W_M)$, where Σ_p is the set of primes of K above p, and Theorem IV.5.4 tells us about the singular parts of these classes at primes in Σ. This information and the duality results of Chapter I §7 will allow us to bound the index $[\mathcal{S}_{\Sigma_p}(K, W_M^*) : \mathcal{S}_{\Sigma\cup\Sigma_p}(K, W_M^*)]$. By taking Σ large enough so that $\mathcal{S}_{\Sigma\cup\Sigma_p}(K, W_M^*) = 0$, and letting M go to infinity, we will obtain the bound of Theorem II.2.2.

1. Preliminaries

Keep the notation of Chapter II §1 and §2. Fix an Euler system $\mathbf{c}$ for $(T, \mathcal{K}, \mathcal{N})$ for some $\mathcal{K}$ and $\mathcal{N}$. If M is a power of p we will write $\mathcal{R}_M = \mathcal{R}_{K,M}$ (as defined in Definition IV.1.1), the set of ideals in $\mathcal{R}$ divisible only by primes $\mathfrak{q}$ such that $\mathfrak{q} \nmid \mathcal{N}$, $M \mid [K(\mathfrak{q}) : K]$, $M \mid P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*; 1)$, and $\mathfrak{q}$ splits completely in $K(1)$. If $\mathfrak{r} \in \mathcal{R}_M$ then $\kappa_{\mathfrak{r},M} \in H^1(K, W_M)$ will denote the derivative class $\kappa_{K,\mathfrak{r},M}$ defined in Chapter IV §4.

Recall $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$. If B is an $\mathcal{O}$-module and $b \in B$, define

$$\mathrm{order}(b, B) = \inf\{n \geq 0 : \mathfrak{p}^n b = 0\} \leq \infty,$$

the *exponent* of the smallest power of $\mathfrak{p}$ which annihilates b. Recall that $\ell_{\mathcal{O}}(B)$ denotes the length of B as an $\mathcal{O}$-module, and (Definition II.2.1) $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is the largest integer n such that $\mathbf{c}_K$ is divisible by $\mathfrak{p}^n$ in $H^1(K,T)/H^1(K,T)_{\mathrm{tors}}$. We will suppose that $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is finite, or else there is nothing to prove.

If $M \in \mathcal{O}$ is nonzero, we let $\iota_M : H^1(K, W_M) \to H^1(K, W)$ denote the map induced by the inclusion of W_M in W. If L is an extension of K and $\eta \in H^1(K, W_M^*)$, we write $(\eta)_L$ for the restriction of η to L, and similarly with W_M in place of W_M^*.

LEMMA 1.1. *Suppose M is a power of p and $\mathrm{ord}_{\mathfrak{p}} M \geq \mathrm{ind}_{\mathcal{O}}(\mathbf{c})$. Then*

$$\mathrm{order}(\iota_M(\kappa_{1,M}), H^1(K, W)) = \mathrm{ord}_{\mathfrak{p}} M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}).$$

PROOF. Lemma IV.4.13(i) shows that $\iota_M(\kappa_{1,M})$ is the image of $\mathbf{c}_K$ under the composition

$$H^1(K,T) \to H^1(K, W_M) \to H^1(K, W),$$

and by Lemma I.2.2(iii) the kernel of this composition is $MH^1(K,T) + H^1(K,T)_{\mathrm{tors}}$, so

$$\mathrm{order}(\iota_M(\kappa_{1,M}), H^1(K, W)) = \mathrm{order}(\mathbf{c}_K, H^1(K,T)/(MH^1(K,T) + H^1(K,T)_{\mathrm{tors}}).$$

Since $H^1(K,T)/H^1(K,T)_{\mathrm{tors}}$ is a torsion-free $\mathcal{O}$-module, it follows from the definition (Definition II.2.1) of $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ that

$$\mathrm{order}(\mathbf{c}_K, H^1(K,T)/(MH^1(K,T)+H^1(K,T)_{\mathrm{tors}})) = \mathrm{ord}_{\mathfrak{p}} M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}).$$

This proves the lemma. □

2. Bounding the order of the Selmer group

We divide the proof of Theorem II.2.2 into two main steps. The first step (Lemma 2.3) is to produce inductively a sequence of primes of K with useful properties. The second step (Lemma 2.5) is to show that the Kolyvagin derivative classes we construct with these primes generate a subgroup which has large image when we localize to the singular part of the cohomology groups. Once this is accomplished, we only have to plug this information into Theorem I.7.3, the global duality theorem, and we obtain the desired bound.

Suppose throughout this section that $p > 2$ and that T satisfies hypotheses $\mathrm{Hyp}(K,T)$. Fix a $\tau \in G_K$ as in hypothesis $\mathrm{Hyp}(K,T)$(i), i.e., $\tau \in G_{K(1)(\boldsymbol{\mu}_{p^\infty})}$ and $T/(\tau-1)T$ is free of rank one over $\mathcal{O}$. As a consequence, for every power M of p we have $\mathcal{O}$-module isomorphisms

$$W_M/(\tau-1)W_M \cong \mathcal{O}/M\mathcal{O}, \quad W_M^*/(\tau-1)W_M^* \cong \mathcal{O}/M\mathcal{O}.$$

LEMMA 2.1. *Fix a power M of p. Suppose L is a Galois extension of K such that G_L acts trivially on W_M and on W_M^*. If*

$$\kappa \in H^1(K,W_M), \qquad \eta \in H^1(K,W_M^*)$$

then there is an element $\gamma \in G_L$ satisfying

(i) $\mathrm{order}(\kappa(\gamma\tau), W_M/(\tau-1)W_M)) \geq \mathrm{order}((\kappa)_L, H^1(L,W_M))$,
(ii) $\mathrm{order}(\eta(\gamma\tau), W_M^*/(\tau-1)W_M^*) \geq \mathrm{order}((\eta)_L, H^1(L,W_M^*))$.

PROOF. First observe that for $\gamma \in G_L$, the image of $\kappa(\gamma\tau)$ in $W_M/(\tau-1)W_M$ is well-defined independent of the choice of cocycle representing κ, and

$$\kappa(\gamma\tau) \equiv \kappa(\gamma) + \kappa(\tau) \pmod{(\tau-1)W_M} \tag{1}$$

and similarly for η.

Define

$$B_\kappa = \{\gamma \in G_L : \mathrm{order}(\kappa(\gamma\tau), W_M/(\tau-1)W_M) < \mathrm{order}((\kappa)_L, \mathrm{Hom}(G_L, W_M))\}$$
$$B_\eta = \{\gamma \in G_L : \mathrm{order}(\eta(\gamma\tau), W_M^*/(\tau-1)W_M^*) < \mathrm{order}((\eta)_L, \mathrm{Hom}(G_L, W_M^*))\}.$$

Every $\gamma \in G_L - (B_\kappa \cup B_\eta)$ satisfies the conclusions of the lemma, so we need only show that $B_\kappa \cup B_\eta$ is a proper subset of G_L.

Define a subgroup J of G_L by

$$J = \{\gamma \in G_L : \mathrm{order}(\kappa(\gamma), W_M/(\tau-1)W_M) < \mathrm{order}((\kappa)_L, \mathrm{Hom}(G_L, W_M))\}.$$

By (1), if $\gamma, \gamma' \in B_\kappa$ then $\gamma^{-1}\gamma' \in J$. Therefore B_κ is either empty or is a coset of J.

Write $d = \mathrm{order}((\kappa)_L, \mathrm{Hom}(G_L, W_M))$, and consider the image $\kappa(G_L)$ of κ on G_L. Since $(\kappa)_L \in \mathrm{Hom}(G_L, W_M)^{\mathrm{Gal}(L/K)}$,

$$\gamma(\kappa(h)) = \kappa(\gamma h \gamma^{-1})$$

for every $h \in G_L$, $\gamma \in G_K$, and so $\kappa(G_L)$ is a G_K-stable submodule of $W_{\mathfrak{p}^d}$, not contained in $W_{\mathfrak{p}^{d-1}}$. By hypothesis $\mathrm{Hyp}(K,T)$(ii), $W_{\mathfrak{p}} = T \otimes \Bbbk$ is irreducible so $\mathfrak{p}^{d-1}\kappa(G_L) = W_{\mathfrak{p}}$ and therefore $\kappa(G_L) = W_{\mathfrak{p}^d}$. Since $W_M/(\tau-1)W_M \cong \mathcal{O}/M\mathcal{O}$,

$$\kappa(J) \subset W_{\mathfrak{p}^{d-1}} + (\tau-1)W_M \subsetneqq W_{\mathfrak{p}^d} = \kappa(G_L)$$

and we conclude that J has index at least p in G_L.

In exactly the same way, B_η is either empty or is a coset of a subgroup of G_L of index at least p. Since $p > 2$, $B_\kappa \cup B_\eta$ cannot equal G_L. This completes the proof. □

Remark 2.2. The end of the previous proof is the only place where we need the assumption that $p > 2$ in Theorem II.2.2.

Let

$$\Omega = K(W)K(1)K(\boldsymbol{\mu}_{p^\infty}, {\mathcal{O}_K^\times}^{1/p^\infty})$$

where $K(W)$ denotes the smallest extension of K such that $G_{K(W)}$ acts trivially on W. Note that G_Ω acts trivially on W^* as well.

Lemma 2.3. *Fix a power M of p. Suppose C is a finite subset of $H^1(K, W_M^*)$ and let $k = |C|$.*

Then there is a finite set $\Sigma = \{\mathfrak{q}_1, \dots, \mathfrak{q}_k\}$ of primes of K satisfying the following properties. If $0 \le i \le k$ write $\mathfrak{r}_i = \prod_{j=1}^{i} \mathfrak{q}_j$. For every i, $1 \le i \le k$,

(i) $\mathfrak{q}_i \in \mathcal{R}_M$,

(ii) $\mathrm{Fr}_{\mathfrak{q}_i}$ *is in the conjugacy class of τ in* $\mathrm{Gal}(K(W_M)/K)$,

(iii) $\mathrm{order}((\kappa_{\mathfrak{r}_{i-1},M})_{\mathfrak{q}_i}, H^1_f(K_{\mathfrak{q}_i}, W_M)) \ge \mathrm{order}((\kappa_{\mathfrak{r}_{i-1},M})_\Omega, H^1(\Omega, W_M))$,

(iv) $\{\eta \in C : (\eta)_{\mathfrak{q}} = 0$ *for every* $\mathfrak{q} \in \Sigma\} \subset H^1(\Omega/K, W_M^*)$.

Proof. Number the elements of C so that $C = \{\eta_1, \eta_2, \dots, \eta_k\}$. We will choose the $\mathfrak{q}_i$ inductively to satisfy (i), (ii), (iii), and

$$(\eta)_{\mathfrak{q}_i} \in H^1_f(K_{\mathfrak{q}_i}, W_M^*) \quad \text{for every } \eta \in C, \tag{2}$$

$$\mathrm{order}((\eta_i)_{\mathfrak{q}_i}, H^1_f(K_{\mathfrak{q}_i}, W_M^*)) \ge \mathrm{order}((\eta_i)_\Omega, H^1(\Omega, W_M^*)). \tag{3}$$

Suppose $1 \le i \le k$ and we have chosen $\{\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}\}$ satisfying (i), (ii), (iii), (2), and (3). We need to find $\mathfrak{q}_i$ also satisfying these properties. Define $\mathcal{N}'$ to be the (finite) product of $\mathcal{N}$ and all primes $\mathfrak{q}$ of K such that $\{(\eta)_{\mathfrak{q}} : \eta \in C\} \not\subset H^1_f(K_{\mathfrak{q}}, W_M^*)$. (Recall that $\mathcal{N}$ is divisible by p and all primes where W_M is ramified.)

Let $L = K(W_M)K(1)(\boldsymbol{\mu}_M, (\mathcal{O}_K^\times)^{1/M})$, so L is a finite extension of K contained in Ω, and G_L acts trivially on both W_M and W_M^*. Apply Lemma 2.1 with this L, $\kappa = \kappa_{r_{i-1},M}$ and $\eta = \eta_i$ to produce an element $\gamma \in G_L$. Let L' denote the (finite) extension of L which is the fixed field of

$$\ker((\kappa_{r_{i-1},M})_L) \cap \ker((\eta_i)_L)$$

where we view $(\kappa_{r_{i-1},M})_L \in \mathrm{Hom}(G_L, W_M)$ and $(\eta_i)_L \in \mathrm{Hom}(G_L, W_M^*)$. Let $\mathfrak{q}_i$ be a prime of K not dividing $\mathcal{N}'\mathfrak{r}_{i-1}$, whose Frobenius in L'/K, for some choice of prime above $\mathfrak{q}_i$, is $\gamma\tau$. The Tchebotarev theorem guarantees the existence of infinitely many such primes.

Property (i) holds by Lemma IV.1.3, and (ii) and (2) are immediate from the definition. By Lemma I.4.7(i), evaluating cocycles at $\mathrm{Fr}_{\mathfrak{q}_i}$ induces an isomorphism

$$H^1_f(K_{\mathfrak{q}_i}, W_M) \cong W_M/(\mathrm{Fr}_{\mathfrak{q}_i} - 1)W_M = W_M/(\tau - 1)W_M$$

and similarly for W_M^*, so (iii) and (3) follow from Lemma 2.1(i) and (ii).

It remains only to check (iv). Define $\Sigma = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$, and suppose that for some i, $(\eta_i)_{\mathfrak{q}} = 0$ for every $\mathfrak{q} \in \Sigma$. Then in particular $(\eta_i)_{\mathfrak{q}_i} = 0$, so (3) shows that

$$\eta_i \in \ker(H^1(K, W_M^*) \to H^1(\Omega, W_M^*)) = H^1(\Omega/K, W_M^*). \qquad \square$$

Definition 2.4. Suppose Σ is a finite set of primes in $\mathcal{R}$. For every M we have an exact sequence

$$0 \longrightarrow \mathcal{S}^{\Sigma_p}(K, W_M) \longrightarrow \mathcal{S}^{\Sigma \cup \Sigma_p}(K, W_M) \xrightarrow{\mathrm{loc}^s_{\Sigma, W_M}} \bigoplus_{\mathfrak{q} \in \Sigma} H^1_s(K_{\mathfrak{q}}, W_M) \tag{4}$$

where we recall that

$$H^1_s(K_{\mathfrak{q}}, W_M) = H^1(K_{\mathfrak{q}}, W_M)/H^1_f(K_{\mathfrak{q}}, W_M)$$

and $\mathrm{loc}^s_{\Sigma, W_M}$ is the sum of the localization maps. (in Theorem I.7.3 the map $\mathrm{loc}^s_{\Sigma, W_M}$ was denoted $\mathrm{loc}^s_{\Sigma \cup \Sigma_p, \Sigma_p}$). We define $\mathrm{loc}^s_{\Sigma, W}$ in exactly the same way with W_M replaced by W.

If $\mathfrak{a}$ is an ideal of K let $\Sigma_{\mathfrak{a}}$ denote the set of primes dividing $\mathfrak{a}$. Let

$$\mathfrak{n}_W = \ell_{\mathcal{O}}\left(H^1(\Omega/K, W) \cap \mathcal{S}^{\Sigma_p}(K, W)\right)$$

as in Theorem II.2.2.

Lemma 2.5. *Suppose $\mathfrak{m} = \mathfrak{p}^n$ is a nonzero ideal of $\mathcal{O}$, $k \in \mathbf{Z}^+$, M is a power of p satisfying*

$$\mathrm{ord}_{\mathfrak{p}} M \geq n + (k+1)\mathfrak{n}_W + \mathrm{ind}_{\mathcal{O}}(\mathbf{c}),$$

and

$$\Sigma = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\} \subset \mathcal{R}_M$$

is a finite set of primes of K such that for $1 \leq i \leq k$,

(a) $\mathrm{Fr}_{\mathfrak{q}_i}$ *is in the conjugacy class of τ in* $\mathrm{Gal}(K(W_M)/K)$,

(b) $\mathrm{order}((\kappa_{\mathfrak{r}_{i-1},M})_{\mathfrak{q}_i}, H^1_f(K_{\mathfrak{q}_i}, W_M)) \geq \mathrm{order}((\kappa_{\mathfrak{r}_{i-1},M})_{\Omega}, H^1(\Omega, W_M))$

where $\mathfrak{r}_i = \prod_{j=1}^i \mathfrak{q}_j$. Then the map $\mathrm{loc}^s_{\Sigma, W_{\mathfrak{m}}}$ of (4) satisfies

$$\ell_{\mathcal{O}}\left(\mathrm{coker}(\mathrm{loc}^s_{\Sigma, W_{\mathfrak{m}}})\right) \leq \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + \mathfrak{n}_W.$$

Remark 2.6. Since the proof of Lemma 2.5 is a rather technical calculation, we first give a proof under the mild additional hypotheses

$$W^{G_K} = 0 \quad \text{and} \quad H^1(\Omega/K, W) = 0. \tag{$*$}$$

We will follow this immediately by the general proof; we include the first one only because it makes the important ideas clearer.

PROOF OF LEMMA 2.5 UNDER THE ASSUMPTION $(*)$. Note that by assumption (a) of the lemma, $W_M/(\mathrm{Fr}_{\mathfrak{q}_i}-1)W_M$ is free of rank one over $\mathcal{O}/M\mathcal{O}$ for every i. Therefore we can apply Corollary IV.5.5 with $\mathfrak{q}=\mathfrak{q}_i$ and $\mathfrak{r}=\mathfrak{r}_{i-1}$ to relate $\kappa_{\mathfrak{r}_i,M}$ and $\kappa_{\mathfrak{r}_{i-1},M}$. This will be the key to the proof.

By Lemma I.2.2(i) and $(*)$, all of the maps

$$H^1(K,W_{\mathfrak{m}}) \xrightarrow{\iota_{\mathfrak{m},M}} H^1(K,W_M) \xrightarrow{\iota_M} H^1(K,W) \xrightarrow{(\ )_\Omega} H^1(\Omega,W)$$

are injective. Therefore for $0\le i\le k$ we can define

$$\begin{aligned}\mathfrak{d}_i &= \mathrm{order}(\kappa_{\mathfrak{r}_i,M},H^1(K,W_M)) = \mathrm{order}(\iota_M(\kappa_{\mathfrak{r}_i,M}),H^1(K,W))\\ &\qquad = \mathrm{order}((\iota_M(\kappa_{\mathfrak{r}_i,M}))_\Omega,H^1(\Omega,W)) = \mathrm{order}((\kappa_{\mathfrak{r}_i,M})_\Omega,H^1(\Omega,W_M)).\end{aligned}$$

By Lemma 1.1,

$$\mathfrak{d}_0 = \mathrm{ord}_{\mathfrak{p}}M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) \ge n. \tag{5}$$

For $i\ge 1$,

$$\begin{aligned}\mathfrak{d}_i \ &\ge\ \mathrm{order}((\kappa_{\mathfrak{r}_i,M})_{\mathfrak{q}_i},H^1_s(K_{\mathfrak{q}_i},W_M))\\ &\qquad\qquad =\ \mathrm{order}((\kappa_{\mathfrak{r}_{i-1},M})_{\mathfrak{q}_i},H^1_f(K_{\mathfrak{q}_i},W_M))\ \ge\ \mathfrak{d}_{i-1},\end{aligned}\tag{6}$$

the equality by Corollary IV.5.5, and the inequality on the right by assumption (b) of the lemma. Combining (5) and (6) we see that $\mathfrak{d}_i\ge n$ for every i.

It follows from Lemma I.5.4 and the injectivity of ι_M that the homomorphism $\iota_{\mathfrak{m},M}: H^1(K,W_{\mathfrak{m}})\to H^1(K,W_M)$ sends $\mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K,W_{\mathfrak{m}})$ onto $\mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K,W_M)_{\mathfrak{m}}$. Theorem IV.5.1 shows that $\kappa_{\mathfrak{r}_i,M}\in\mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K,W_M)$, so for each $i\ge 1$ we can choose $\bar\kappa_i\in\mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K,W_{\mathfrak{m}})$ such that $\mathcal{O}\iota_{\mathfrak{m},M}(\bar\kappa_i)=\mathfrak{p}^{\mathfrak{d}_i-n}\kappa_{\mathfrak{r}_i,M}$.

For every $i\le k$ let $A^{(i)}$ denote the $\mathcal{O}$-submodule of $H^1(K,W_{\mathfrak{m}})$ generated by $\{\bar\kappa_1,\dots,\bar\kappa_i\}$, and let $A=A^{(k)}$. Then

$$A^{(i)}\subset\mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K,W_{\mathfrak{m}})\subset\mathcal{S}^{\Sigma\cup\Sigma_p}(K,W_{\mathfrak{m}})$$

so for $i\ge 1$, writing loc^s_Σ for $\mathrm{loc}^s_{\Sigma,W_{\mathfrak{m}}}$, restriction to $\mathfrak{q}_i$ induces a surjective map

$$\mathrm{loc}^s_\Sigma(A^{(i)})/\mathrm{loc}^s_\Sigma(A^{(i-1)}) \twoheadrightarrow \mathcal{O}(\bar\kappa_i)_{\mathfrak{q}_i}\subset H^1_s(K_{\mathfrak{q}_i},W_{\mathfrak{m}}).$$

Hence for every $i\ge 1$, (6) shows that

$$\begin{aligned}\ell_{\mathcal{O}}(\mathrm{loc}^s_\Sigma(A^{(i)})/\mathrm{loc}^s_\Sigma(A^{(i-1)})) &\ge \mathrm{order}((\bar\kappa_i)_{\mathfrak{q}_i},H^1_s(K_{\mathfrak{q}_i},W_{\mathfrak{m}}))\\ &\ge \mathrm{order}((\kappa_{\mathfrak{r}_i,M})_{\mathfrak{q}_i},H^1_s(K_{\mathfrak{q}_i},W_M)) - (\mathfrak{d}_i-n)\\ &\ge n+\mathfrak{d}_{i-1}-\mathfrak{d}_i.\end{aligned}$$

Using the filtration

$$\mathrm{loc}^s_\Sigma(A)=\mathrm{loc}^s_\Sigma(A^{(k)})\supset\mathrm{loc}^s_\Sigma(A^{(k-1)})\supset\cdots\supset\mathrm{loc}^s_\Sigma(A^{(1)})\supset\mathrm{loc}^s_\Sigma(A^{(0)})=0$$

we conclude, using (5) and the trivial estimate $\mathfrak{d}_k\le\mathrm{ord}_{\mathfrak{p}}M$, that

$$\begin{aligned}\ell_{\mathcal{O}}(\mathrm{loc}^s_\Sigma(\mathcal{S}^{\Sigma\cup\Sigma_p}(K,W_{\mathfrak{m}}))) &\ge \ell_{\mathcal{O}}(\mathrm{loc}^s_\Sigma(A))\\ &\ge \sum_{i=1}^{k}(n+\mathfrak{d}_{i-1}-\mathfrak{d}_i) = kn+\mathfrak{d}_0-\mathfrak{d}_k \ge kn-\mathrm{ind}_{\mathcal{O}}(\mathbf{c}).\end{aligned}$$

For every prime $\mathfrak{q} \in \mathcal{R}_M$, $H^1_s(K_\mathfrak{q}, W_\mathfrak{m}) = W_\mathfrak{m}^{\mathrm{Fr}_\mathfrak{q}=1}$ by Lemma I.4.7(i), so

$$\ell_\mathcal{O}(\oplus_{\mathfrak{q}\in\Sigma} H^1_s(K_\mathfrak{q}, W_\mathfrak{m})) = k\ell_\mathcal{O}(W_\mathfrak{m}^{\tau=1}) = k\ell_\mathcal{O}(W_\mathfrak{m}/(\tau-1)W_\mathfrak{m}) = kn.$$

Thus

$$\ell_\mathcal{O}(\mathrm{coker}(\mathrm{loc}^s_\Sigma)) \le \mathrm{ind}_\mathcal{O}(\mathbf{c})$$

as desired. □

Proof of Lemma 2.5 in general. Recall that ι_M is the natural map from $H^1(K, W_M)$ to $H^1(K, W)$. For $0 \le i \le k$ define

$$\mathfrak{d}'_i = \mathrm{order}(\iota_M(\kappa_{\mathfrak{r}_i,M}), H^1(K, W)),$$
$$\mathfrak{d}_i = \mathrm{order}((\kappa_{\mathfrak{r}_i,M})_\Omega, H^1(\Omega, W_M)).$$

By Lemma 1.1,

$$\mathfrak{d}'_0 = \mathrm{ord}_\mathfrak{p} M - \mathrm{ind}_\mathcal{O}(\mathbf{c}) \ge n + (k+1)\mathfrak{n}_W. \tag{7}$$

Since $\mathfrak{p}^{\mathfrak{d}_i}(\kappa_{\mathfrak{r}_i,M})_\Omega = 0$,

$$\mathfrak{p}^{\mathfrak{d}_i}\iota_M(\kappa_{\mathfrak{r}_i,M}) \subset H^1(\Omega/K, W).$$

By Theorem IV.5.1, $\mathfrak{p}^{\mathfrak{d}_i}\iota_M(\kappa_{\mathfrak{r}_i,M}) \in \mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K, W)$. The primes dividing $\mathfrak{r}_i$ are unramified in Ω/K and satisfy $H^1_f(K_\mathfrak{q}, W) = H^1_{\mathrm{ur}}(K_\mathfrak{q}, W)$ (Lemma I.3.5(iv)), so we conclude that

$$\mathfrak{p}^{\mathfrak{d}_i}\iota_M(\kappa_{\mathfrak{r}_i,M}) \in H^1(\Omega/K, W) \cap \mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K, W) = H^1(\Omega/K, W) \cap \mathcal{S}^{\Sigma_p}(K, W). \tag{8}$$

Therefore for every i, $\mathfrak{p}^{\mathfrak{d}_i+\mathfrak{n}_W}\iota_M(\kappa_{\mathfrak{r}_i,M}) = 0$, so

$$\mathfrak{n}_W + \mathfrak{d}_i \ge \mathfrak{d}'_i. \tag{9}$$

Suppose $i \ge 1$. If $\mathcal{I}_{\mathfrak{q}_i}$ is an inertia group of $\mathfrak{q}_i$, then (using Lemmas I.3.8(ii), I.3.5(iv) and I.3.2(ii)) we have a diagram

$$\begin{array}{ccccc}
H^1_s(K_{\mathfrak{q}_i}, W_M) & = & H^1(K_{\mathfrak{q}_i}, W_M)/H^1_{\mathrm{ur}}(K_{\mathfrak{q}_i}, W_M) & \subset & \mathrm{Hom}(\mathcal{I}_{\mathfrak{q}_i}, W_M) \\
\downarrow{\scriptstyle \iota_M} & & \downarrow & & \cap \\
H^1_s(K_{\mathfrak{q}_i}, W) & = & H^1(K_{\mathfrak{q}_i}, W)/H^1_{\mathrm{ur}}(K_{\mathfrak{q}_i}, W) & \subset & \mathrm{Hom}(\mathcal{I}_{\mathfrak{q}_i}, W).
\end{array}$$

Therefore the map $\iota_M : H^1_s(K_{\mathfrak{q}_i}, W_M) \to H^1_s(K_{\mathfrak{q}_i}, W)$ is injective. This gives the first equality of

$$\begin{aligned}\mathfrak{d}'_i \ \ge\ \mathrm{order}(\iota_M(\kappa_{\mathfrak{r}_i,M})_{\mathfrak{q}_i}, H^1_s(K_{\mathfrak{q}_i}, W)) \ &=\ \mathrm{order}((\kappa_{\mathfrak{r}_i,M})_{\mathfrak{q}_i}, H^1_s(K_{\mathfrak{q}_i}, W_M)) \\ &=\ \mathrm{order}((\kappa_{\mathfrak{r}_{i-1},M})_{\mathfrak{q}_i}, H^1_f(K_{\mathfrak{q}_i}, W_M)) \ \ge\ \mathfrak{d}_{i-1},\end{aligned} \tag{10}$$

the second equality comes from Corollary IV.5.5 and assumption (a) of the lemma, and the final inequality comes from assumption (b). Combining this inequality with (7) and (9) we conclude by induction that

$$\mathfrak{d}_i \ge \mathfrak{d}'_0 - (i+1)\mathfrak{n}_W \ge n.$$

For every $i \le k$ let $A^{(i)}$ denote the $\mathcal{O}$-submodule of $H^1(K, W)$ generated by

$$\{\mathfrak{p}^{\mathfrak{d}_j - n}\iota_M(\kappa_{\mathfrak{r}_j,M}) : 0 \le j \le i\},$$

and $A = A^{(k)}$. By Theorem IV.5.1,

$$A^{(i)} \subset \mathcal{S}^{\Sigma_{p\mathfrak{r}_i}}(K, W) \tag{11}$$

so for $i \geq 1$ restriction to $\mathfrak{q}_i$ induces a surjective map

$$\mathrm{loc}^s_{\Sigma,W}(A^{(i)})/\mathrm{loc}^s_{\Sigma,W}(A^{(i-1)}) \twoheadrightarrow \mathfrak{p}^{\mathfrak{d}_i - n}(\kappa_{\mathfrak{r}_i,M})_{\mathfrak{q}_i} \subset H^1_s(K_{\mathfrak{q}_i}, W).$$

For every $i \geq 1$, (10) shows that

$$\mathrm{order}((\mathfrak{p}^{\mathfrak{d}_i - n}\kappa_{\mathfrak{r}_i,M})_{\mathfrak{q}_i}, H^1_s(K_{\mathfrak{q}_i}, W_M)) \geq \mathfrak{d}_{i-1} - \mathfrak{d}_i + n,$$

so using the filtration

$$\mathrm{loc}^s_{\Sigma,W}(A) = \mathrm{loc}^s_{\Sigma,W}(A^{(k)}) \supset \mathrm{loc}^s_{\Sigma,W}(A^{(k-1)}) \supset \cdots \supset \mathrm{loc}^s_{\Sigma,W}(A^{(1)}) \supset \mathrm{loc}^s_{\Sigma,W}(A^{(0)})$$

we conclude that

$$\ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma,W}(A)) \geq \sum_{i=1}^{k}(\mathfrak{d}_{i-1} - \mathfrak{d}_i + n) = kn + \mathfrak{d}_0 - \mathfrak{d}_k \geq kn + \mathfrak{d}_0 - \mathrm{ord}_{\mathfrak{p}} M. \tag{12}$$

Since $\mathfrak{m} = \mathfrak{p}^n$, (8) shows that

$$\mathfrak{m}A \subset H^1(\Omega/K, W) \cap \mathcal{S}^{\Sigma_p}(K, W). \tag{13}$$

Let $A_{\mathfrak{m}}$ denote the submodule of A killed by $\mathfrak{m}$. By (11) and Lemma I.5.4,

$$A_{\mathfrak{m}} \subset \mathcal{S}^{\Sigma \cup \Sigma_p}(K, W)_{\mathfrak{m}} = \iota_{\mathfrak{m}}(\mathcal{S}^{\Sigma \cup \Sigma_p}(K, W_{\mathfrak{m}})). \tag{14}$$

From the exact diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker(\mathrm{loc}^s_{\Sigma,W}) \cap A_{\mathfrak{m}} \arrow[r] \arrow[d] & A_{\mathfrak{m}} \arrow[r] \arrow[d] & \mathrm{loc}^s_{\Sigma,W}(A_{\mathfrak{m}}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker(\mathrm{loc}^s_{\Sigma,W}) \cap A \arrow[r] & A \arrow[r] \arrow[d] & \mathrm{loc}^s_{\Sigma,W}(A) \arrow[r] & 0 \\
 & & \mathfrak{m}A \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

we see that

$$\begin{aligned} &\ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma,W}(A_{\mathfrak{m}})) \\ &\quad = \ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma,W}(A)) + \ell_{\mathcal{O}}((\ker(\mathrm{loc}^s_{\Sigma,W}) \cap A)/(\ker(\mathrm{loc}^s_{\Sigma,W}) \cap A_{\mathfrak{m}})) - \ell_{\mathcal{O}}(\mathfrak{m}A). \end{aligned} \tag{15}$$

By (11) with $i = 0$,

$$A^{(0)} = \mathfrak{p}^{\mathfrak{d}_0 - n}\iota_M(\kappa_{1,M}) \subset \ker(\mathrm{loc}^s_{\Sigma,W}).$$

Since $A^{(0)}$ is a cyclic $\mathcal{O}$-module, we conclude using (7) that

$$\begin{aligned} \ell_{\mathcal{O}}((\ker(\mathrm{loc}^s_{\Sigma,W}) \cap A)/(\ker(\mathrm{loc}^s_{\Sigma,W}) \cap A_{\mathfrak{m}})) &\geq \ell_{\mathcal{O}}(A^{(0)}) - \ell_{\mathcal{O}}(A^{(0)} \cap A_{\mathfrak{m}}) \\ &\geq (\mathfrak{d}'_0 - (\mathfrak{d}_0 - n)) - n \\ &= \mathrm{ord}_{\mathfrak{p}} M - \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) - \mathfrak{d}_0. \end{aligned}$$

Combining this with (14), (15), (12), and (13) yields

$$\begin{aligned}\ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma,W_{\mathfrak{m}}}(\mathcal{S}^{\Sigma\cup\Sigma_p}(K,W_{\mathfrak{m}}))) &\geq \ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma,W}(A_{\mathfrak{m}}))\\ &\geq (kn+\mathfrak{d}_0-\mathrm{ord}_{\mathfrak{p}}M)+(\mathrm{ord}_{\mathfrak{p}}M-\mathrm{ind}_{\mathcal{O}}(\mathbf{c})-\mathfrak{d}_0)-\mathfrak{n}_W\\ &= kn-\mathrm{ind}_{\mathcal{O}}(\mathbf{c})-\mathfrak{n}_W.\end{aligned}$$

For every prime $\mathfrak{q}\in\mathcal{R}_M$, $H^1_s(K_{\mathfrak{q}},W_{\mathfrak{m}})=W_{\mathfrak{m}}^{\mathrm{Fr}_{\mathfrak{q}}=1}$ by Lemma I.4.7(i), so

$$\ell_{\mathcal{O}}(\oplus_{\mathfrak{q}\in\Sigma}H^1_s(K_{\mathfrak{q}},W_{\mathfrak{m}}))=k\ell_{\mathcal{O}}(W_{\mathfrak{m}}^{\tau=1})=k\ell_{\mathcal{O}}(W_{\mathfrak{m}}/(\tau-1)W_{\mathfrak{m}})=kn.$$

Thus

$$\begin{aligned}\ell_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma,W_{\mathfrak{m}}}))&=\ell_{\mathcal{O}}(\oplus_{\mathfrak{q}\in\Sigma}H^1_s(K_{\mathfrak{q}},W_{\mathfrak{m}}))-\ell_{\mathcal{O}}(\mathrm{loc}^s_{\Sigma,W_{\mathfrak{m}}}(\mathcal{S}^{\Sigma\cup\Sigma_p}(K,W_{\mathfrak{m}})))\\ &\leq \mathrm{ind}_{\mathcal{O}}(\mathbf{c})+\mathfrak{n}_W\end{aligned}$$

as desired. □

Proof of Theorem II.2.2. Fix a nonzero ideal $\mathfrak{m}=\mathfrak{p}^n$ of $\mathcal{O}$. Let C be the image of $\mathcal{S}_{\Sigma_p}(K,W^*_{\mathfrak{m}})$ (which is finite by Lemma I.5.7(i)) in $H^1(K,W^*_M)$ where M is a power of p large enough so that

$$\mathrm{ord}_{\mathfrak{p}}M>n+(|\mathcal{S}_{\Sigma_p}(K,W^*_{\mathfrak{m}})|+1)\mathfrak{n}_W+\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$$

(if $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$ is infinite then there is nothing to prove). Apply Lemma 2.3 with this group C, let Σ be a set of primes of K produced by that lemma, and apply Lemma 2.5 with this set Σ.

Combining the inequality of Lemma 2.5 with Theorem I.7.3(iii) shows that

$$\ell_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}(K,W^*_{\mathfrak{m}})/\mathcal{S}_{\Sigma\cup\Sigma_p}(K,W^*_{\mathfrak{m}}))\leq\mathfrak{n}_W+\mathrm{ind}_{\mathcal{O}}(\mathbf{c}).$$

Therefore

$$\ell_{\mathcal{O}}(\iota_{\mathfrak{m}}(\mathcal{S}_{\Sigma_p}(K,W^*_{\mathfrak{m}})))\leq\ell_{\mathcal{O}}(\iota_{\mathfrak{m}}(\mathcal{S}_{\Sigma\cup\Sigma_p}(K,W^*_{\mathfrak{m}})))+\mathfrak{n}_W+\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$$

for every $\mathfrak{m}$. By Lemma 2.3(iv), $\iota_{\mathfrak{m}}(\mathcal{S}_{\Sigma\cup\Sigma_p}(K,W^*_{\mathfrak{m}}))\subset H^1(\Omega/K,W^*)\cap\mathcal{S}_{\Sigma_p}(K,W^*)$, and

$$\mathcal{S}_{\Sigma_p}(K,W^*)=\varinjlim_{\mathfrak{m}}\iota_{\mathfrak{m}}(\mathcal{S}_{\Sigma_p}(K,W^*_{\mathfrak{m}})),$$

so

$$\ell_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}(K,W^*))\leq\mathrm{ind}_{\mathcal{O}}(\mathbf{c})+\mathfrak{n}_W+\ell_{\mathcal{O}}(H^1(\Omega/K,W^*)\cap\mathcal{S}_{\Sigma_p}(K,W^*))$$

which is Theorem II.2.2. □

3. Bounding the exponent of the Selmer group

The proof of Theorem II.2.3 is similar to that of Theorem II.2.2; it is easier in that one can work with a single prime $\mathfrak{q}$ instead of a finite set of primes, but more difficult in that one must keep track of extra "error terms".

The idea is as follows. Given $\eta\in\mathcal{S}_{\Sigma_p}(K,W^*_M)$, we use Lemma 3.1 below to choose a prime $\mathfrak{q}$ such that

- $H^1_f(K_{\mathfrak{q}},W^*_M)$ and $H^1_s(K_{\mathfrak{q}},W_M)$ are "almost" isomorphic to $\mathcal{O}/M\mathcal{O}$,
- $\mathrm{order}((\kappa_{\mathfrak{q},M})_{\mathfrak{q}},H^1_s(K_{\mathfrak{q}},W_M))$ is approximately $\mathrm{ord}_{\mathfrak{p}}M-\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$
- $\mathrm{order}((\eta)_{\mathfrak{q}},H^1_f(K_{\mathfrak{q}},W^*_M))$ is approximately $\mathrm{order}(\eta,H^1(K,W^*_M))$

Since the Kolyvagin derivative class $\kappa_{\mathfrak{q},M}$ belongs to $\mathcal{S}^{\Sigma_{p\mathfrak{q}}}(K, W_M)$, the duality Theorem I.7.3 shows that $\mathrm{order}((\kappa_{\mathfrak{q},M})_{\mathfrak{q}}, H^1_s(K_{\mathfrak{q}}, W_M)) + \mathrm{order}((\eta)_{\mathfrak{q}}, H^1_f(K_{\mathfrak{q}}, W^*_M))$ is "approximately" bounded by $\mathrm{ord}_{\mathfrak{p}} M$, and so we deduce that $\mathrm{order}(\eta, H^1(K, W^*_M))$ is "approximately" bounded by $\mathrm{ind}_{\mathcal{O}}(\mathbf{c})$. Since $\eta \in \mathcal{S}_{\Sigma_p}(K, W^*_M)$ is arbitrary, if we can bound all the error terms independently of M, this will prove Theorem II.2.3. In the remainder of this section we sketch the details of this argument.

Keep the notation of §1 and §2. Suppose the Euler system $\mathbf{c}$ satisfies the hypotheses $\mathrm{Hyp}(K, V)$, and fix a $\tau \in G_K$ as in hypothesis $\mathrm{Hyp}(K, V)$(i). We now allow $p = 2$.

Let a be the least positive integer such that $\mathfrak{p}^a$ annihilates the maximal G_K-stable subgroup of $(\tau - 1)W$ and of $(\tau - 1)W^*$. Hypothesis $\mathrm{Hyp}(K, V)$(ii) ensures that a is finite, since any divisible G_K-stable subgroup of $(\tau - 1)W$ would be the image of a G_K-stable subgroup of $(\tau - 1)V$, which must be zero.

We have the following variant of Lemma 2.1.

LEMMA 3.1. *Fix a power M of p. Suppose L is a Galois extension of K such that G_L acts trivially on W_M and on W^*_M. If*

$$\kappa \in H^1(K, W_M), \qquad \eta \in H^1(K, W^*_M)$$

then there is an element $\gamma \in G_L$ satisfying

(i) $\mathrm{order}(\kappa(\gamma\tau), W_M/(\tau - 1)W_M) \geq \mathrm{order}((\kappa)_L, H^1(L, W_M)) - a - 1$,
(ii) $\mathrm{order}(\eta(\gamma\tau), W^*_M/(\tau - 1)W^*_M) \geq \mathrm{order}((\eta)_L, H^1(L, W^*_M)) - a - 1$.

PROOF. The proof is identical to that of Lemma 2.1, once we note that a G_K-submodule of W_M which projects to zero in $W_M/(\tau - 1)W_M$ is killed by $\mathfrak{p}^a$, and similarly for W^*_M. The extra '1' takes care of the case $p = 2$. □

Let $\Omega = K(W)K(1)K(\boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})$ as in §2.

LEMMA 3.2. *If $T \neq \mathcal{O}$ and $T \neq \mathcal{O}(1)$ then $H^1(\Omega/K, W)$ and $H^1(\Omega/K, W^*)$ are finite.*

PROOF. This is Corollary C.2.2 applied with $F = K$. □

PROOF OF THEOREM II.2.3. If $T = \mathcal{O}(1)$ then by the example of Chapter I §6.1,

$$\mathcal{S}_{\Sigma_p}(K, W^*) \subset \mathrm{Hom}(A_K, \mathbf{D}),$$

where A_K is the ideal class group of K, so $\mathcal{S}_{\Sigma_p}(K, W^*)$ is finite. The theorem assumes that $T \neq \mathcal{O}$, so by Lemma 3.2 we may assume from now on that $H^1(\Omega/K, W)$ and $H^1(\Omega/K, W^*)$ are finite. Let

$$n = \max\{\ell_{\mathcal{O}}(H^1(\Omega/K, W)), \ell_{\mathcal{O}}(H^1(\Omega/K, W^*))\}.$$

Suppose M is a power of p and $\eta \in \mathcal{S}_{\Sigma_p}(K, W^*_M)$. Apply Lemma 3.1 with $L = K(W_M)K(1)(\boldsymbol{\mu}_M, (\mathcal{O}_K^\times)^{1/M}) \subset \Omega$, this η, and with $\kappa = \kappa_{1,M} \in H^1(K, W_M)$, and let $\gamma \in G_L$ be an element satisfying the conclusions of that lemma. Then since

$H^1(\Omega/K, W)$ is the kernel of the restriction map $H^1(K, W) \to H^1(\Omega, W)$,

$$\begin{aligned}
\operatorname{order}(\kappa_{1,M}(\gamma\tau), W_M/(\tau-1)W_M)) &\geq \operatorname{order}(\iota_M(\kappa_{1,M})_\Omega, H^1(\Omega, W)) - a - 1 \\
&\geq \operatorname{order}(\iota_M(\kappa_{1,M}), H^1(K, W)) - a - 1 - n \\
&= \operatorname{ord}_{\mathfrak{p}} M - \operatorname{ind}_{\mathcal{O}}(\mathbf{c}) - a - 1 - n \qquad (16)
\end{aligned}$$

by Lemma 1.1. Similarly

$$\operatorname{order}(\eta(\gamma\tau), W_M^*/(\tau-1)W_M^*) \geq \operatorname{order}(\eta, H^1(K, W_M^*)) - a - 1 - n. \qquad (17)$$

Let L' denote the fixed field of

$$\ker((\kappa_{1,M})_L) \cap \ker((\eta)_L),$$

and, using the Tchebotarev theorem, choose a prime $\mathfrak{q}$ of K, not dividing $\mathcal{N}$, whose Frobenius in L'/K, for some choice of prime above $\mathfrak{q}$, is $\gamma\tau$. By Lemma IV.1.3, $\mathfrak{q} \in \mathcal{R}_M$.

As in the proof of Lemma 2.3, we conclude from (16) and (17) that

$$\operatorname{order}((\kappa_{1,M})_{\mathfrak{q}}, H^1_f(K_{\mathfrak{q}}, W_M)) \geq \operatorname{ord}_{\mathfrak{p}} M - \operatorname{ind}_{\mathcal{O}}(\mathbf{c}) - a - 1 - n$$

and

$$\operatorname{order}((\eta)_{\mathfrak{q}}, H^1_f(K_{\mathfrak{q}}, W_M^*)) \geq \operatorname{order}(\eta, H^1(K, W_M^*)) - a - 1 - n. \qquad (18)$$

Let $b = \ell_{\mathcal{O}}(W^{\tau=1}/(W^{\tau=1})_{\mathrm{div}})$, where $(W^{\tau=1})_{\mathrm{div}}$ is the maximal divisible submodule of $W^{\tau=1}$. By Theorem IV.5.4 and Corollary A.2.6,

$$\begin{aligned}
\operatorname{order}((\kappa_{\mathfrak{q},M})_{\mathfrak{q}}, H^1_s(K_{\mathfrak{q}}, W_M)) &\geq \operatorname{order}((\kappa_{1,M})_{\mathfrak{q}}, H^1_f(K_{\mathfrak{q}}, W_M)) - 2b \\
&\geq \operatorname{ord}_{\mathfrak{p}} M - \operatorname{ind}_{\mathcal{O}}(\mathbf{c}) - a - 1 - n - 2b.
\end{aligned}$$

By Lemma I.4.7(i),

$$\ell_{\mathcal{O}}(H^1_s(K_{\mathfrak{q}}, W_M)) = \ell_{\mathcal{O}}((W_M)^{\tau=1}) = \ell_{\mathcal{O}}((W^{\tau=1})_M) \leq \operatorname{ord}_{\mathfrak{p}} M + b.$$

Thus, applying Theorem I.7.3(iii) with $\Sigma = \Sigma_{p\mathfrak{q}}$, $\Sigma_0 = \Sigma_p$, and $\eta \in \mathcal{S}_{\Sigma_p}(K, W_M^*)$, we conclude that

$$\begin{aligned}
\operatorname{order}((\eta)_{\mathfrak{q}}, H^1_f(K_{\mathfrak{q}}, W_M^*)) &\leq \ell_{\mathcal{O}}(\operatorname{coker}(\operatorname{loc}^s_{\Sigma_{p\mathfrak{q}},\Sigma_p})) \\
&\leq \ell_{\mathcal{O}}(H^1_s(K_{\mathfrak{q}}, W_M)) - \operatorname{order}((\kappa_{\mathfrak{q},M})_{\mathfrak{q}}, H^1_s(K_{\mathfrak{q}}, W_M)) \\
&\leq \operatorname{ind}_{\mathcal{O}}(\mathbf{c}) + a + 1 + n + 3b
\end{aligned}$$

since $\kappa_{\mathfrak{q},M} \in \mathcal{S}^{\Sigma_{p\mathfrak{q}}}(K, W_M)$. Combining this with (18) shows

$$\operatorname{order}(\eta, H^1(K, W_M^*)) \leq 2 + 2a + 3b + 2n + \operatorname{ind}_{\mathcal{O}}\mathbf{c}.$$

This holds for every M and every $\eta \in \mathcal{S}_{\Sigma_p}(K, W_M^*)$. Since $\mathcal{S}_{\Sigma_p}(K, W^*)$ is the direct limit of the $\mathcal{S}_{\Sigma_p}(K, W_M^*)$, if $\mathfrak{m} = \mathfrak{p}^{2+2a+3b+2n+\operatorname{ind}_{\mathcal{O}}\mathbf{c}}$ then we conclude that $\mathfrak{m}\mathcal{S}_{\Sigma_p}(K, W^*) = 0$.

As is well-known, this implies that $\mathcal{S}_{\Sigma_p}(K, W^*)$ is finite: Lemma I.5.4 shows that

$$\mathcal{S}_{\Sigma_p}(K, W^*) = \mathcal{S}_{\Sigma_p}(K, W^*)_{\mathfrak{m}} \subset \mathcal{S}(K, W^*)_{\mathfrak{m}} = \iota_{\mathfrak{m}}(\mathcal{S}(K, W^*_{\mathfrak{m}}))$$

and the latter is finite by Lemma I.5.7(i). $\square$

CHAPTER VI

Twisting

In this chapter we extend the methods of Chapter II §4 and show how to twist Euler systems by characters of infinite order. This will be used in Chapter VII when we prove Theorems II.3.2, II.3.3, and II.3.4: Theorem 4.1 shows that without loss of generality we may twist T by a character of $\mathrm{Gal}(K_\infty/K)$, and Lemma 1.3 allows us to choose a particular twist that avoids certain complications.

We keep the setting of Chapter II: K is a number field, T is a p-adic representation of G_K, and K_∞ is an abelian extension of K satisfying

$$\mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^d.$$

Let $\Gamma = \mathrm{Gal}(K_\infty/K)$, and recall that Λ is the Iwasawa algebra

$$\Lambda = \mathcal{O}[[\Gamma]] = \varprojlim_{K \subset_f F \subset K_\infty} \mathcal{O}[\mathrm{Gal}(F/K)],$$

a complete local noetherian unique factorization domain. The characteristic ideal $\mathrm{char}(B)$ of a finitely-generated Λ-module B was defined in Chapter II §3.

1. Twisting representations

Definition 1.1. Suppose $\rho : G_K \to \mathcal{O}^\times$ is a continuous character, possibly of infinite order. As in Example I.1.2 we will write $\mathcal{O}_\rho$ for a free, rank-one $\mathcal{O}$ module with G_K acting via ρ, and if B is a G_K-module we will abbreviate

$$B \otimes \rho = B \otimes_{\mathcal{O}} \mathcal{O}_\rho.$$

Then $B \otimes \rho$ is isomorphic to B as an $\mathcal{O}$-module but not (in general) as a G_K-module.

If $\rho : \Gamma \to \mathcal{O}^\times$ define

$$\mathrm{Tw}_\rho : \Lambda \xrightarrow{\sim} \Lambda$$

to be the $\mathcal{O}$-linear isomorphism induced by $\gamma \mapsto \rho(\gamma)\gamma$ for $\gamma \in \Gamma$.

Lemma 1.2. *If B is a finitely-generated torsion Λ-module and $\rho : \Gamma \to \mathcal{O}^\times$ is a character, then $B \otimes \rho$ is a finitely-generated torsion Λ-module and*

(i) $\mathrm{Tw}_\rho(\mathrm{char}(B \otimes \rho)) = \mathrm{char}(B)$,
(ii) $\mathrm{Tw}_\rho(\mathrm{Ann}_\Lambda(B \otimes \rho)) = \mathrm{Ann}_\Lambda(B)$.

Proof. If $f \in \Lambda$ and $\xi_\rho \in \mathcal{O}_\rho$ then

$$f \cdot (b \otimes \xi_\rho) = (\mathrm{Tw}_\rho(f)b) \otimes \xi_\rho.$$

The lemma follows easily from this, along with (for (i)) the fact that twisting preserves the heights of ideals of Λ. □

LEMMA 1.3. (i) *Suppose B is G_K-module, free of finite rank over $\mathcal{O}$, and $J_1, \ldots, J_k$ are subgroups of G_K whose projections to Γ are infinite. Then the set*

$$\{\rho \in \mathrm{Hom}(\Gamma, \mathcal{O}^\times) : (B \otimes \rho)^{J_i^{p^n}} = 0 \text{ for } 1 \leq i \leq k \text{ and every } n \geq 0\}$$

contains an open dense subset of $\mathrm{Hom}(\Gamma, \mathcal{O}^\times)$.

(ii) *Suppose B is a finitely-generated torsion Λ-module. Then the set*

$$\{\rho \in \mathrm{Hom}(\Gamma, \mathcal{O}^\times) : (B \otimes \rho) \otimes_\Lambda \mathcal{O}[\mathrm{Gal}(F/K)] \text{ is finite for every } K \subset_{\mathrm{f}} F \subset K_\infty\}$$

is dense in $\mathrm{Hom}(\Gamma, \mathcal{O}^\times)$.

PROOF. Consider (i) first. Recall that Φ is the field of fractions of $\mathcal{O}$, and let $\bar{\Phi}$ denote an algebraic closure. For each i fix an element $\gamma_i \in J_i$ whose projection to Γ has infinite order, and define

$$\begin{aligned} R_i &= \{\text{eigenvalues of } \gamma_i \text{ acting on } B \otimes \bar{\Phi}\}, \\ P_i &= \{x \in \mathcal{O}^\times : xR_i \cap \boldsymbol{\mu}_{p^\infty} \neq \emptyset\}, \\ Z_i &= \{\rho \in \mathrm{Hom}(\Gamma, \mathcal{O}^\times) : \rho(\gamma_i) \notin P_i\}. \end{aligned}$$

Each R_i is finite, and $\boldsymbol{\mu}_{p^\infty} \cap \mathcal{O}^\times$ is finite, so each P_i is finite and thus $Z = \cap_i Z_i$ is an open dense subset of $\mathrm{Hom}(\Gamma, \mathcal{O}^\times)$. We will show that Z is contained in the set of (i).

Suppose $\zeta \in \boldsymbol{\mu}_{p^\infty}$. Then

$$\begin{aligned} &\zeta \text{ is an eigenvalue of } \gamma_i \text{ acting on } (B \otimes \rho) \otimes \bar{\Phi} \\ &\qquad \Leftrightarrow \rho^{-1}(\gamma_i)\zeta \text{ is an eigenvalue of } \gamma_i \text{ acting on } B \otimes \bar{\Phi} \\ &\qquad \Leftrightarrow \zeta \in \rho(\gamma_i) R_i \\ &\qquad \Rightarrow \rho(\gamma_i) \in P_i \end{aligned}$$

Therefore if $\rho \in Z_i$ and $n \geq 0$ then $\gamma_i^{p^n}$ does not have 1 as an eigenvalue on $(B \otimes \rho) \otimes \Phi$. It follows that for for $1 \leq i \leq k$, $n \geq 0$, and $\rho \in Z$,

$$(B \otimes \rho)^{J_i^{p^n}} \otimes \Phi = ((B \otimes \rho) \otimes \Phi)^{J_i^{p^n}} = 0$$

and since B has no p-torsion, $(B \otimes \rho)^{J_i^{p^n}} = 0$.

Let $U \subset \mathrm{Hom}(\Gamma, \mathcal{O}^\times)$ be the set defined in (ii). We will show that U contains a countable intersection of dense open sets, so the Baire Category Theorem shows that U is dense. Since B is a quotient of a finite direct sum of cyclic modules, it is enough to prove this when $B = \Lambda/f\Lambda$ with a nonzero $f \in \Lambda$.

Suppose $B = \Lambda/f\Lambda$, so $B \otimes \rho \cong \Lambda/\mathrm{Tw}_{\rho^{-1}}(f)\Lambda$. If $K \subset_{\mathrm{f}} F \subset K_\infty$ then

$$\begin{aligned} &\Lambda/\mathrm{Tw}_{\rho^{-1}}(f)\Lambda \otimes_\Lambda \mathcal{O}[\mathrm{Gal}(F/K)] \text{ is finite } \Leftrightarrow \\ &\qquad \rho^{-1}\chi(f) \neq 0 \text{ for every character } \chi : \mathrm{Gal}(F/K) \to \bar{\Phi}. \end{aligned} \tag{1}$$

Let $\mathcal{X}$ be the set of characters of finite order of Γ into $\bar{\Phi}$. For every $\chi \in \mathcal{X}$ let

$$Y_\chi = \{\rho \in \mathrm{Hom}(\Gamma, \mathcal{O}^\times) : \rho^{-1}\chi(f) \neq 0\}.$$

Since $f \neq 0$, each Y_χ is open and dense in $\mathrm{Hom}(\Gamma, \mathcal{O}^\times)$, and (1) shows that $U = \cap_{\chi \in \mathcal{X}} Y_\chi$. Since $\mathcal{X}$ is countable, this concludes the proof. □

2. Twisting cohomology groups

For every extension L of K, write $H^1_\infty(L,T) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(FL,T)$, and if $\mathbf{c}$ is an Euler system let $\mathbf{c}_{L,\infty} = \{\mathbf{c}_{LF}\}_{K \subset_{\mathrm{f}} F \subset K_\infty} \in H^1_\infty(L,T)$.

PROPOSITION 2.1. *Suppose $K \subset_{\mathrm{f}} L$ and $\rho : \mathrm{Gal}(LK_\infty/K) \to \mathcal{O}^\times$ is a character. The natural map on cocycles induces G_K-isomorphisms*

(i) $H^1_\infty(L,T) \otimes \rho \xrightarrow{\sim} H^1_\infty(L, T \otimes \rho)$

(ii) $\mathcal{S}_\Sigma(LK_\infty, W) \otimes \rho \xrightarrow{\sim} \mathcal{S}_\Sigma(LK_\infty, W \otimes \rho)$

if Σ is a finite set of primes of K containing all primes above p.

PROOF. Let $L_\infty = LK_\infty$, and write $L_\infty = \cup L_n$ where $[L_n : L]$ is finite and $\mathrm{Gal}(L_\infty/L_n)$ is in the kernel of $\mathrm{Gal}(LK_\infty/K) \xrightarrow{\rho} (\mathcal{O}/p^n\mathcal{O})^\times$. Since $\mathcal{O}_\rho/p^n\mathcal{O}_\rho$ is a trivial G_{L_n}-module, the natural map on cocycles induces G_K-equivariant isomorphisms

$$H^1(L_n, T/p^nT) \otimes \rho \xrightarrow{\sim} H^1(L_n, (T/p^nT) \otimes \rho). \tag{2}$$

Combining these isomorphisms with Lemma B.3.1 gives a sequence of isomorphisms

$$\begin{aligned} H^1_\infty(L,T) \otimes \rho &= \varprojlim_n H^1(L_n, T/p^nT) \otimes \rho \\ &\xrightarrow{\sim} \varprojlim_n H^1(L_n, (T \otimes \rho)/p^n(T \otimes \rho)) = H^1_\infty(L, T \otimes \rho). \end{aligned}$$

This proves (i).

The isomorphisms (2) induce

$$\varinjlim_n H^1(L_n, W) \otimes \rho \xrightarrow{\sim} \varinjlim_n H^1(L_n, W \otimes \rho)$$

and, for every place w of L_n

$$H^1(L_{n,w}, W_{p^n}) \otimes \rho \xrightarrow{\sim} H^1(L_{n,w}, W_{p^n} \otimes \rho). \tag{3}$$

We need to show that if w does not divide p, then the isomorphisms (3) induce

$$\varinjlim_n H^1_f(L_{n,w}, W) \otimes \rho \xrightarrow{\sim} \varinjlim_n H^1_f(L_{n,w}, W \otimes \rho).$$

Since all primes above p are in Σ, this will prove (ii).

Fix a place w of LK_∞ not dividing p, and let $\mathcal{I}$ denote an decomposition group of w in G_L. Since K_∞/K is unramified outside p, $\rho(\mathcal{I}) = 1$, and $\mathcal{I}$ is also an inertia group of w in G_{L_n} for every n.

By Lemma I.3.2(i), for every n we have

$$H^1_{\mathrm{ur}}(L_{n,w}, W_{p^n}) \cong W^{\mathcal{I}}_{p^n}/(\mathrm{Fr}_n - 1)W^{\mathcal{I}}_{p^n}$$

where Fr_n is a Frobenius of w in G_{L_n}. By Lemma I.3.5(iii), $H^1_f(L_{n,w}, W_{p^n})$ is the inverse image of $((W^{\mathcal{I}})_{\mathrm{div}} + (\mathrm{Fr}_n - 1)W^{\mathcal{I}})_{p^n}$ under this isomorphism, and we define the subgroup $H^1_F(L_{n,w}, W_{p^n}) \subset H^1_f(L_{n,w}, W_{p^n})$ to be the inverse image of $((W^{\mathcal{I}})_{\mathrm{div}})_{p^n} + (\mathrm{Fr}_n - 1)W^{\mathcal{I}}_{p^n}$. Then

$$\varinjlim_n H^1_F(L_{n,w}, W_{p^n}) = \varinjlim_n H^1_f(L_{n,w}, W_{p^n}) = \varinjlim_n H^1_f(L_{n,w}, W)$$

and similarly with W replaced by $W \otimes \rho$. The isomorphism (3) induces an isomorphism

$$H^1_F(L_{n,w}, W_{p^n}) \otimes \rho \xrightarrow{\sim} H^1_F(L_{n,w}, W_{p^n} \otimes \rho)$$

so this concludes the proof of (ii). $\square$

REMARK 2.2. Note that Proposition 2.1 does not assert the existence of an isomorphism, or even a map, from $H^1(L,T)$ to $H^1(L, T \otimes \rho)$.

3. Twisting Euler systems

DEFINITION 3.1. Suppose $\mathbf{c}$ is an Euler system for (T, K_∞), more specifically (in the notation of Definition II.1.1) for $(T, \mathcal{K}, \mathcal{N})$, where $K_\infty \subset \mathcal{K}$ and $\mathcal{N}$ is divisible by p and the primes where T is ramified. Suppose $\rho : \mathrm{Gal}(\mathcal{K}/K) \to \mathcal{O}^\times$ is a character which factors through a finite extension of K_∞. (We can always ensure this latter property by taking K_∞ to be the compositum of all $\mathbf{Z}_p$-extensions of K in $\mathcal{K}$.) Let L be finite extension of K in $\mathcal{K}$, and $L_\infty = LK_\infty$, such that

(i) ρ factors through $\mathrm{Gal}(L_\infty/K)$,

(ii) L_∞/K is ramified only at primes dividing $\mathcal{N}$, ∞, and the conductor of ρ.

(For example, L_∞ could be the fixed field of $\ker(\rho) \cap G_{K_\infty}$, and L a finite extension of K such that $L_\infty = LK_\infty$.) Fix a generator ξ_ρ of $\mathcal{O}_\rho$. We define a collection of cohomology classes $\mathbf{c}^\rho$

$$\{\mathbf{c}^\rho_F \in H^1(F, T \otimes \rho) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$$

as follows. If $K \subset_{\mathrm{f}} F \subset \mathcal{K}$ let $\mathbf{c}^\rho_F$ be the image of $\mathbf{c}_{FL,\infty} \otimes \xi_\rho \in H^1_\infty(FL, T) \otimes \rho$ under the composition

$$H^1_\infty(FL, T) \otimes \rho \xrightarrow{\sim} H^1_\infty(FL, T \otimes \rho) \longrightarrow H^1(FL, T \otimes \rho) \xrightarrow{\mathrm{Cor}_{FL/F}} H^1(F, T \otimes \rho)$$

where the first map is the isomorphism of Proposition 2.1 and the second is the natural projection from H^1_∞ to H^1.

REMARK 3.2. This definition is independent of our choice of L. For, suppose L' is another such choice satisfying the properties above. We may as well suppose that $L \subset L'$. If $K \subset_{\mathrm{f}} F \subset \mathcal{K}$, then FL'/FL is unramified outside $\mathcal{N}$, ∞, and the conductor of ρ. Those primes which divide the conductor of ρ but do not divide p are already ramified in FL/K, so the Euler system distribution relation shows that $\mathrm{Cor}_{FL'/FL}(\mathbf{c}_{FL'}) = \mathbf{c}_{FL}$.

REMARK 3.3. Let $\xi_{\rho,n}$ denote the image of the generator ξ_ρ in $\mathcal{O}_\rho/p^n\mathcal{O}_\rho$. An examination of the proof of Proposition 2.1 shows that for every F, with L_n as in that proof, we have

$$\mathbf{c}_{FL_n} \otimes \xi_{\rho,n} \in H^1(FL_n, (T \otimes \rho)/p^n(T \otimes \rho))$$

and then

$$\begin{aligned}\mathbf{c}^\rho_F = \lim_{n\to\infty} \mathrm{Cor}_{FL_n/F}(\mathbf{c}_{FL_n} \otimes \xi_{\rho,n})& \\ \in \varprojlim_n H^1(F, (T \otimes \rho)/p^n(T \otimes \rho)) &= H^1(F, T \otimes \rho).\end{aligned}$$

REMARK 3.4. When ρ is a character of finite order, this definition of $\mathbf{c}^\rho$ agrees with the one given in Definition II.4.1. (Just take L to be the fixed field of $\ker(\rho)$.)

THEOREM 3.5. *Suppose* $\mathbf{c}$ *is an Euler system for* $(T,\mathcal{K},\mathcal{N})$ *where* $K_\infty \subset \mathcal{K}$, *and* $\rho : \mathrm{Gal}(\mathcal{K}/K) \to \mathcal{O}^\times$ *is a character which factors through a finite extension of* K_∞. *Then the collection of classes* $\{\mathbf{c}_F^\rho \in H^1(F, T\otimes\rho)\}$ *defined above is an Euler system for* $(T\otimes\rho,\mathcal{K},\mathfrak{f}\mathcal{N})$ *where* $\mathfrak{f}$ *is the non-archimedean, non-p part of the conductor of* ρ.

PROOF. Suppose $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$. We have a commutative diagram

$$\begin{tikzcd}
H^1_\infty(F'L,T)\otimes\rho \arrow[r, "\sim"] \arrow[d, "\mathrm{Cor}\otimes 1"'] & H^1_\infty(F'L,T\otimes\rho) \arrow[r, "\mathrm{Cor}"] \arrow[d, "\mathrm{Cor}"'] & H^1(F',T\otimes\rho) \arrow[d, "\mathrm{Cor}_{F'/F}"'] \\
H^1_\infty(FL,T)\otimes\rho \arrow[r, "\sim"] & H^1_\infty(FL,T\otimes\rho) \arrow[r, "\mathrm{Cor}"] & H^1(F,T\otimes\rho)
\end{tikzcd}$$

Since $\mathbf{c}$ is an Euler system,

$$\mathrm{Cor}_{F'LK_\infty/FLK_\infty}(\mathbf{c}_{F'L,\infty}) = \Big(\prod_{\mathfrak{q}\in S} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})\Big)\mathbf{c}_{FL,\infty}$$

where

$$\begin{aligned} S &= \{\mathfrak{q} \text{ of } K : \mathfrak{q} \text{ ramifies in } F'L/K \text{ but not in } FL/K, \text{ and } \mathfrak{q}\nmid\mathcal{N}\} \\ &= \{\mathfrak{q} \text{ of } K : \mathfrak{q} \text{ ramifies in } F'/K \text{ but not in } F/K, \text{ and } \mathfrak{q}\nmid\mathfrak{f}\mathcal{N}\}, \end{aligned}$$

the last equality because the conductor of L/K is divisible by $\mathfrak{f}$ and divides $\mathfrak{f}\mathcal{N}\infty$ times a power of p. Therefore

$$\begin{aligned} (\mathrm{Cor}_{F'LK_\infty/FLK_\infty}(\mathbf{c}_{F'L,\infty}))\otimes\xi_\rho &= (\prod_{\mathfrak{q}\in S} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{c}_{FL,\infty})\otimes\xi_\rho \\ &= \prod_{\mathfrak{q}\in S} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\rho(\mathrm{Fr}_\mathfrak{q})\mathrm{Fr}_\mathfrak{q}^{-1})(\mathbf{c}_{FL,\infty}\otimes\xi_\rho) \end{aligned}$$

and so, using the diagram above

$$\mathrm{Cor}_{F'/F}(\mathbf{c}^\rho_{F'}) = \prod_{\mathfrak{q}\in S} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\rho(\mathrm{Fr}_\mathfrak{q})\mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{c}^\rho_F.$$

Since

$$\det(1-\mathrm{Fr}_\mathfrak{q}^{-1}x|(T\otimes\rho)^*) = \det(1-\rho(\mathrm{Fr}_\mathfrak{q})\mathrm{Fr}_\mathfrak{q}^{-1}x|T^*) = P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\rho(\mathrm{Fr}_\mathfrak{q})x),$$

this shows that $\mathbf{c}^\rho$ is an Euler system for $(T\otimes\rho,\mathcal{K},\mathfrak{f}\mathcal{N})$. □

LEMMA 3.6. *Suppose* $\mathbf{c}$ *is an Euler system for* $(T,\mathcal{K},\mathcal{N})$ *where* $K_\infty\subset\mathcal{K}$, *and* $\rho,\rho' : \mathrm{Gal}(\mathcal{K}/K)\to\mathcal{O}^\times$ *are characters which factor through a finite extension of* K_∞. *Let* $\mathfrak{f}_\rho$, $\mathfrak{f}_{\rho'}$, $\mathfrak{f}_{\rho\rho'}$ *be the non-archimedean, non-p part of the conductors of* ρ, ρ', *and* $\rho\rho'$. *Fix generators of* $\mathcal{O}_\rho$, $\mathcal{O}_{\rho'}$, *and* $\mathcal{O}_{\rho\rho'} = \mathcal{O}_\rho\otimes\mathcal{O}_{\rho'}$ *so that* $\xi_{\rho\rho'} = \xi_\rho\otimes\xi_{\rho'}$.

If every divisor of $\mathfrak{f}_\rho\mathfrak{f}_{\rho'}$ *divides* $\mathfrak{f}_{\rho\rho'}\mathcal{N}$, *then* $(\mathbf{c}^\rho)^{\rho'} = \mathbf{c}^{\rho\rho'}$. *In particular, if* $\mathfrak{f}_\rho \mid \mathcal{N}$ *then* $(\mathbf{c}^\rho)^{\rho^{-1}} = \mathbf{c}$.

PROOF. Let L_ρ be a finite extension of K satisfying (i) and (ii) of Definition 3.1 for ρ, and similarly for $L_{\rho'}$.

Our assumption on the conductors of ρ, ρ', and $\rho\rho'$ ensures that the compositum $L_\rho L_{\rho'}$ satisfies Definition 3.1(i) and (ii) for $\rho\rho'$. The lemma now follows easily from the definitions of $\mathbf{c}^\rho$, $\mathbf{c}^{\rho'}$, and $\mathbf{c}^{\rho\rho'}$ (and Remark 3.2). $\square$

4. Twisting theorems

Recall that $\Gamma = \mathrm{Gal}(K_\infty/K)$.

THEOREM 4.1. *If $\rho : \Gamma \to \mathcal{O}^\times$ is a character then Theorems* II.3.2, II.3.3, *and* II.3.4 *for T and $\mathbf{c}$ are equivalent to Theorems* II.3.2, II.3.3, *and* II.3.4, *respectively, for $T \otimes \rho$ and $\mathbf{c}^\rho$, where $\mathbf{c}^\rho$ is the Euler system for $T \otimes \rho$ given by Theorem* 3.5.

PROOF. The hypotheses $\mathrm{Hyp}(K_\infty, T)$, $\mathrm{Hyp}(K_\infty, V)$, and $\mathrm{Hyp}(K_\infty/K)$ depend only on the action of G_{K_∞} on T, so they are not affected by twisting by characters of Γ.

Write

$$X_\infty^{(T)} = \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*), \mathbf{D}), \quad X_\infty^{(T\otimes\rho)} = \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K_\infty, (W\otimes\rho)^*), \mathbf{D}).$$

Since $(W \otimes \rho)^* = W^* \otimes \rho^{-1}$, Proposition 2.1(ii) shows that $X_\infty^{(T\otimes\rho)} \cong X_\infty^{(T)} \otimes \rho$, so by Lemma 1.2(i)

$$\mathrm{Tw}_\rho(\mathrm{char}(X_\infty^{(T\otimes\rho)})) = \mathrm{char}(X_\infty^{(T)}).$$

The argument of Lemma 1.2 also shows that

$$\mathrm{Tw}_\rho(\mathrm{ind}_\Lambda(\mathbf{c}^\rho)) = \mathrm{ind}_\Lambda(\mathbf{c}).$$

The theorem follows from these equalities. $\square$

5. Examples and applications

Recall that $\varepsilon_{\mathrm{cyc}} : G_K \to \mathbf{Z}_p^\times \subset \mathcal{O}^\times$ is the cyclotomic character, and let $\omega : G_K \to (\mathbf{Z}_p^\times)_{\mathrm{tors}}$ be the Teichmüller character giving the action of G_K on $\boldsymbol{\mu}_p$ (if p is odd) or $\boldsymbol{\mu}_4$ (if $p = 2$).

5.1. Tate twists. Suppose $\boldsymbol{\mu}_{p^\infty} \subset \mathcal{K}$, so that $\varepsilon_{\mathrm{cyc}}$ is a character of $\mathrm{Gal}(\mathcal{K}/K)$. If T is a p-adic representation of G_K, then for every integer n we write $T(n)$ for the Tate twist $T \otimes \varepsilon_{\mathrm{cyc}}^n$. By Theorem 3.5, an Euler system $\mathbf{c}$ for $(T, \mathcal{K}, \mathcal{N})$ gives an Euler system $\mathbf{c}^{\varepsilon_{\mathrm{cyc}}^n}$ for $(T(n), \mathcal{K}, \mathcal{N})$, and by Lemma 3.6 $(\mathbf{c}^{\varepsilon_{\mathrm{cyc}}^n})^{\varepsilon_{\mathrm{cyc}}^m} = \mathbf{c}^{\varepsilon_{\mathrm{cyc}}^{n+m}}$ for every n and m.

Now take K_∞ to be the cyclotomic $\mathbf{Z}_p$-extension of K. Then $\varepsilon_{\mathrm{cyc}}$ does not necessarily factor through $\mathrm{Gal}(K_\infty/K)$, but $\omega^{-1}\varepsilon_{\mathrm{cyc}}$ does. Thus if $\mathbf{c}$ is an Euler system for (T, K_∞), Theorem 4.1 shows that for every n, Theorems II.3.2, II.3.3, and II.3.4 for T and $\mathbf{c}$ are equivalent to those same theorems for $T \otimes \omega^{-n}\varepsilon_{\mathrm{cyc}}^n$ and $\mathbf{c}^{\omega^{-n}\varepsilon_{\mathrm{cyc}}^n}$.

5.2. Cyclotomic fields. In Chapter III, §2 and §4, we used cyclotomic units and Stickelberger elements, respectively, to construct Euler systems $\mathbf{c}_{\mathrm{cyc}}$ for $\mathbf{Z}_p(1)$ and $\mathbf{c}_{\mathrm{St}}$ for $\mathbf{Z}_p$.

EXERCISE. Both $\mathbf{c}_{\mathrm{St}}^{\varepsilon_{\mathrm{cyc}}}$ and $\mathbf{c}_{\mathrm{cyc}}$ are Euler systems for $\mathbf{Z}_p(1)$. Determine the relation between them.

5.3. Elliptic curves with complex multiplication. Let K be an imaginary quadratic field, K_∞ the $\mathbf{Z}_p^2$-extension of K, and suppose E is an elliptic curve defined over K with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. Fix a prime $\mathfrak{p}$ of K above p, and let $\mathcal{O}$ be the completion of $\mathcal{O}_K$ at $\mathfrak{p}$. Fix a generator of $\mathfrak{p}\mathcal{O}$ and let $T_\mathfrak{p}(E)$ denote the $\mathfrak{p}$-adic Tate module of E, which is a free, rank-one $\mathcal{O}$-module. Let ψ be the canonical character

$$\psi : G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}_K}(E_{\mathfrak{p}^\infty}) \cong \mathcal{O}^\times.$$

Then $T_\mathfrak{p}(E) \cong \mathcal{O}_\psi$.

Let $\mathbf{c}_{\mathrm{ell}}$ denote the Euler system of elliptic units for $\mathcal{O}(1)$ (over K) of Chapter III §3. The character $\psi\varepsilon_{\mathrm{cyc}}^{-1}$ factors through a finite extension of K_∞, so by Theorem 3.5 we get an Euler system $\mathbf{c}_{E,\mathfrak{p}} = \mathbf{c}_{\mathrm{ell}}^{\psi\varepsilon_{\mathrm{cyc}}^{-1}}$ for $\mathcal{O}(1) \otimes \psi\varepsilon_{\mathrm{cyc}}^{-1} = \mathcal{O}_\psi \cong T_\mathfrak{p}(E)$. In particular we get an element

$$\mathbf{c}_{E,\mathfrak{p},K} \in H^1(K, T_\mathfrak{p}(E)).$$

Let $V_\mathfrak{p} = T_\mathfrak{p} \otimes K_\mathfrak{p}$. As usual (see Example I.6.4), if v divides p we define

$$H^1_f(K_v, V_\mathfrak{p}(E)) = \mathrm{image}(E(K_v) \otimes \mathbf{Q}_p \hookrightarrow H^1(K_v, V_\mathfrak{p}(E))).$$

As in Example I.6.4,

$$H^1_f(K_v, V_\mathfrak{p}(E)) = H^1(K_v, V_\mathfrak{p}(E)) = 0$$

for all $v \neq \mathfrak{p}$. It follows that $H^1(K, T_\mathfrak{p}(E)) = \mathcal{S}^{\{\mathfrak{p}\}}(K, T_\mathfrak{p}(E))$, so in particular

$$\mathbf{c}_{E,\mathfrak{p},K} \in \mathcal{S}^{\{\mathfrak{p}\}}(K, T_\mathfrak{p}(E)).$$

There is an exact sequence

$$0 \longrightarrow E(K) \otimes \mathbf{Z}_p \longrightarrow \mathcal{S}(K, T_\mathfrak{p}(E)) \longrightarrow \varprojlim Ш(E_{/K})_{\mathfrak{p}^n} \longrightarrow 0$$

so if the $\mathfrak{p}$-part of the Tate-Shafarevich group $Ш(E_{/K})$ is finite (and this is known to be true if E is defined over $\mathbf{Q}$ and the L-function $L(E_{/\mathbf{Q}}, s)$ of E vanishes to order at most one at $s = 1$) then $\mathcal{S}(K, T_\mathfrak{p}(E)) = E(K) \otimes \mathbf{Z}_p$.

One can show that

$$\mathbf{c}_{E,\mathfrak{p},K} \in \mathcal{S}(K, T_\mathfrak{p}(E)) \;\Leftrightarrow\; L(E_{/K}, 1) = 0.$$

If $L(E_{/K}, 1) = 0$ then one can further compute the p-adic height of $\mathbf{c}_{E,\mathfrak{p},K}$ in terms of the derivative of the $\mathfrak{p}$-adic L-function of E at $s = 1$. See [**Ru7**] for the details of these computations.

CHAPTER VII

Iwasawa theory

In this chapter we use the cohomology classes constructed in Chapter IV, along with the duality results of Chapter I §7, to prove Theorems II.3.2, II.3.3 and II.3.4. The proofs follow generally along the same lines as as the proof of Theorem II.2.2 given in Chapter V, except that where in Chapter V we dealt with $\mathcal{O}$-modules, we must now deal with $\mathcal{O}[\mathrm{Gal}(F/K)]$-modules for $K \subset_{\mathrm{f}} F \subset K_\infty$. This makes the algebra much more complicated.

In §1 we give the proof of Theorems II.3.3 and II.3.4, assuming Theorem II.3.2 and two propositions (Propositions 1.4 and 1.6), whose proofs will be given in the following sections.

We keep the notation of Chapter II. In particular $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $\Lambda = \mathcal{O}[[\Gamma]]$. If $K \subset_{\mathrm{f}} F \subset K_\infty$ and M is a power of p, then let $\Lambda_F = \mathcal{O}[\mathrm{Gal}(F/K)]$ and

$$\Lambda_{F,M} = \Lambda_F/M\Lambda_F = (\mathcal{O}/M\mathcal{O})[\mathrm{Gal}(F/K)].$$

We assume throughout this chapter that we have a p-adic representation T of G_K and an Euler system $\mathbf{c}$ for (T, K_∞) such that $\mathbf{c}_{K,\infty} = \{\mathbf{c}_F\}_F \notin H^1_\infty(K,T)_{\mathrm{tors}}$ (or else there is nothing to prove). We assume that hypotheses $\mathrm{Hyp}(K_\infty, V)$ are satisfied, and we fix once and for all a $\tau \in G_K$ as in hypothesis $\mathrm{Hyp}(K_\infty,V)$(i): i.e., τ fixes $K(1)$, K_∞, $\boldsymbol{\mu}_{p^\infty}$, and $(\mathcal{O}_K^\times)^{1/p^\infty}$, and $\dim_\Phi(V/(\tau-1)V) = 1$.

1. Outline

Since τ fixes $\boldsymbol{\mu}_{p^\infty}$, we also have $\dim_\Phi(V^*/(\tau-1)V^*) = 1$.

Definition 1.1. Fix an isomorphism

$$\theta^* : W^*/(\tau-1)W^* \xrightarrow{\sim} \mathbf{D}.$$

Recall that $\Omega = K(1)(W, \boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})$. Define $\Omega_\infty = K_\infty\Omega$ and let $\Omega_\infty^{\langle\tau\rangle}$ be the fixed field of τ in Ω_∞.

There is a natural evaluation homomorphism

$$\mathrm{Ev}^* : G_{\Omega_\infty^{\langle\tau\rangle}} \to \mathrm{Hom}(H^1(K_\infty, W^*), \mathbf{D}),$$

defined by

$$\mathrm{Ev}^*(\sigma)([c]) = \theta^*(c(\sigma))$$

for every $\sigma \in G_{\Omega_\infty^{\langle\tau\rangle}}$ and every cocycle c representing a class in $[c] \in H^1(K_\infty, W^*)$. This is well-defined because $c(\sigma)$ is well-defined modulo $(\sigma-1)W^*$, and if $\sigma \in G_{\Omega_\infty^{\langle\tau\rangle}}$ then σ acts on W^* through $\mathrm{Gal}(\Omega_\infty/\Omega_\infty^{\langle\tau\rangle})$ which is (topologically) generated by τ, so $(\sigma-1)W^* \subset (\tau-1)W^* = \ker(\theta^*)$. Similarly, the cocycle relation shows that Ev^* is a homomorphism.

If B maps to $H^1(K_\infty, W^*)$ (for example, if B is a subgroup of $H^1(F, W_M^*)$ where $K \subset_{\mathrm{f}} F \subset K_\infty$ and $M \in \mathcal{O}$) then we will also write Ev^* or Ev_B^* for the induced map

$$G_{\Omega_\infty^{\langle\tau\rangle}} \longrightarrow \mathrm{Hom}(B, \mathbf{D}).$$

For example, $\mathrm{Ev}^*_{\mathcal{S}_{\Sigma_p}(K_\infty, W^*)}$ maps $G_{\Omega_\infty^{\langle\tau\rangle}}$ to $X_\infty = \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*), \mathbf{D})$.

DEFINITION 1.2. Define a positive integer a_τ by

$$a_\tau = [W^{\tau=1} : (W^{\tau=1})_{\mathrm{div}}] \cdot \max\{|Z|, |Z^*|\}$$

where $(W^{\tau=1})_{\mathrm{div}}$ is the maximal divisible subgroup of $W^{\tau=1}$, and Z (resp. Z^*) is the unique maximal G_{K_∞}-stable submodule of $(\tau-1)W$ (resp. $(\tau-1)W^*$).

LEMMA 1.3. (i) *a_τ is finite.*
(ii) *If T and τ satisfy hypotheses* $\mathrm{Hyp}(K_\infty, T)$ *then $a_\tau = 1$.*

PROOF. If the submodule Z (resp. Z^*) of Definition 1.2 is infinite, then it gives rise to a proper G_{K_∞}-stable submodule of V (resp. V^*). But hypothesis $\mathrm{Hyp}(K_\infty, V)$ asserts that V is irreducible, and it follows that V^* is as well, so this is impossible. Thus $|Z|$ and $|Z^*|$ are finite, and $[W^{\tau=1} : (W^{\tau=1})_{\mathrm{div}}]$ is finite simply because W has finite $\mathbf{Z}_p$-corank. This proves (i).

Similarly, if hypotheses $\mathrm{Hyp}(K_\infty, T)$ hold, then the irreducibility of $T/\mathfrak{p}T$ (where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$) shows that Z and Z^* must be zero, and Proposition A.2.5 shows that $W^{\tau=1} = (W^{\tau=1})_{\mathrm{div}}$. This proves (ii). □

Suppose that Theorem II.3.2 holds (the proof will be given in §4), so X_∞ is a finitely-generated torsion Λ-module. By Theorem VI.4.1, if $\rho : \Gamma \to \mathcal{O}^\times$ is a character then Theorems II.3.2, II.3.3, and II.3.4 for T and $\mathbf{c}$ are equivalent to Theorems II.3.2, II.3.3, and II.3.4 for $T \otimes \rho$ and the twisted Euler system $\mathbf{c}^\rho$ of Chapter VI §3, respectively. Thus by Lemma VI.1.3(ii) applied to the Λ-module $X_\infty \oplus \Lambda/\mathrm{char}(X_\infty)$, twisting T and $\mathbf{c}$ if necessary we may assume that

$$X_\infty \otimes \Lambda_F \text{ and } \Lambda_F/\mathrm{char}(X_\infty)\Lambda_F \text{ are finite for every } K \subset_{\mathrm{f}} F \subset K_\infty. \tag{1}$$

As discussed in Chapter II §3, since X_∞ is a torsion Λ-module we can fix an injective pseudo-isomorphism

$$\bigoplus_{i=1}^{r} \Lambda/f_i\Lambda \to X_\infty, \tag{2}$$

where the nonzero elements $f_1, \ldots, f_r \in \Lambda$ satisfy $f_{i+1} \mid f_i$ for $1 \le i \le r-1$. The sequence of principal ideals (elementary divisors) $f_1\Lambda, \ldots, f_r\Lambda$ is uniquely determined by these conditions, and the characteristic ideal of X_∞ is

$$\mathrm{char}(X_\infty) = \prod_{i=1}^{r} f_i\Lambda. \tag{3}$$

Assume for the rest of this section that, in addition to hypotheses $\mathrm{Hyp}(K_\infty, V)$, hypothesis $\mathrm{Hyp}(K_\infty/K)$ is satisfied as well.

PROPOSITION 1.4. *There are elements $z_1, \ldots, z_r \in X_\infty$ and ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_r \subset \Lambda$ such that for $1 \le k \le r$*

(i) $z_k \in \mathrm{Ev}^*(\tau G_{\Omega_\infty})$,

(ii) $a_\tau \mathfrak{g}_k \subset f_k\Lambda$ *and, if* $k < r$, $\mathfrak{g}_k \subset \mathfrak{g}_{k+1}$,

(iii) *there is a split exact sequence*

$$0 \longrightarrow \sum_{i=1}^{k-1} \Lambda z_i \longrightarrow \sum_{i=1}^{k} \Lambda z_i \longrightarrow \Lambda/\mathfrak{g}_k \longrightarrow 0$$

so $\sum_{i=1}^k \Lambda z_i \cong \oplus_{i=1}^k \Lambda/\mathfrak{g}_i$ *and* $\sum_{i=1}^k \Lambda z_i$ *is a direct summand of* $\sum_{i=1}^r \Lambda z_i$,

(iv) $a_\tau(X_\infty/\sum_{i=1}^r \Lambda z_i)$ *is pseudo-null.*

The proof of Proposition 1.4 will be given in §6. Using (2) it is easy to find $\{z_i\}$, with $\mathfrak{g}_i = f_i\Lambda$, satisfying (ii), (iii), and (iv), but condition (i) will be essential for our purposes.

Definition 1.5. Fix a sequence $z_1, \ldots, z_r \in X_\infty$ as in Proposition 1.4 and define

$$Z_\infty = \sum_{i=1}^r \Lambda z_i \subset X_\infty.$$

If $0 \le k \le r$, a *Selmer sequence* $\boldsymbol{\sigma}$ of length k is a k-tuple $(\sigma_1, \ldots, \sigma_k)$ of elements of τG_{Ω_∞} satisfying

$$\mathrm{Ev}^*(\sigma_i) - z_i \in \mathcal{M} Z_\infty$$

for $1 \le i \le k$, where we recall that $\mathcal{M}$ is the maximal ideal of Λ. (When $k = 0$, the empty sequence is a Selmer sequence.) Note that by Proposition 1.4(i), Selmer sequences exist, for example with all the above differences equal to zero.

Suppose M is a power of p. Let $\Omega_M = K(1)(\boldsymbol{\mu}_M, (\mathcal{O}_K^\times)^{1/M}, W_M)$, and if $K \subset_{\mathrm{f}} F \subset K_\infty$ let $L_{F,M} \supset F\Omega_M$ be the fixed field of the subgroup

$$\bigcap_{c \in \mathcal{S}_{\Sigma_p}(F, W_M^*)} \ker((c)_{F\Omega_M}) \quad \subset \ G_{F\Omega_M}.$$

The restriction of $\mathcal{S}_{\Sigma_p}(F, W_M^*)$ to $F\Omega_M$ is a finite (Lemma I.5.7) subgroup of $\mathrm{Hom}(G_{F\Omega_M}, W_M^*)$, so $L_{F,M}$ is a finite abelian extension of $F\Omega_M$. It is not difficult to check, although we do not absolutely need it, that $L_{F,M}/K$ is Galois and unramified outside primes above p, ∞, and primes where T is ramified.

For $0 \le k \le r$ we call a k-tuple $(\mathcal{Q}_1, \ldots, \mathcal{Q}_k)$ of primes of F a *Kolyvagin sequence* (for F and M) if there is a Selmer sequence $\boldsymbol{\sigma}$ of length k such that for $1 \le i \le k$, the prime of K below $\mathcal{Q}_i$ belongs to the set $\mathcal{R}$ of Chapter II §1, and

$$\mathrm{Fr}_{\mathcal{Q}_i} = \sigma_i \quad \text{on } L_{F,M}$$

(all primes in $\mathcal{R}$ are unramified in $L_{F,M}/K$). If $\boldsymbol{\pi}$ is a Kolyvagin sequence of length k we will write $\mathfrak{q}_i$ for the prime of K below $\mathcal{Q}_i$ and we define

$$\mathfrak{r}(\boldsymbol{\pi}) = \prod_{i=1}^k \mathfrak{q}_i.$$

By Lemma IV.1.3, $\mathfrak{r}(\boldsymbol{\pi})$ belongs to the set $\mathcal{R}_{F,M}$ defined in Definition IV.1.1.

Let $\Pi(k, F, M)$ be the set of all Kolyvagin sequences of length k for F and M. When $k = 0$, $\Pi(k, F, M)$ has a single element, the empty sequence (independent of

F and M). Define an ideal in $\Lambda_{F,M}$

$$\Psi(k,F,M) = \sum_{\boldsymbol{\pi}\in\Pi(k,F,M)} \sum_{\psi} \psi(\kappa_{F,\mathfrak{r}(\boldsymbol{\pi}),M}) \quad \subset \Lambda_{F,M}$$

where the inner sum is over $\psi \in \mathrm{Hom}_\Lambda(\Lambda_{F,M}\kappa_{F,\mathfrak{r}(\boldsymbol{\pi}),M}, \Lambda_{F,M})$ and $\kappa_{F,\mathfrak{r}(\boldsymbol{\pi}),M}$ is the Euler system derivative class constructed in Chapter IV §4. In other words, $\Psi(k,F,M)$ is the ideal of $\Lambda_{F,M}$ generated by all homomorphic images of modules $\Lambda_{F,M}\kappa_{F,\mathfrak{r}(\boldsymbol{\pi}),M}$ as $\boldsymbol{\pi}$ runs through $\Pi(k,F,M)$.

PROPOSITION 1.6. *There is an element $h \in \Lambda$ relatively prime to* $\mathrm{char}(X_\infty)$*, and for every $K \subset_{\mathrm{f}} F \subset K_\infty$ there is a power N_F of p, such that if $K \subset_{\mathrm{f}} F \subset K_\infty$, $M \geq N_F$ is a power of p, and $0 \leq k < r$, then*

$$ha_\tau^5 \Psi(k,F,MN_F)\Lambda_{F,M} \subset f_{k+1}\Psi(k+1,F,M).$$

Proposition 1.6 is the key to the proofs of Theorems II.3.3 and II.3.4; it will be proved in §7. We now show how to use Proposition 1.6 to complete the proof of Theorems II.3.3 and II.3.4. Recall that if Σ is a set of places of K, then K_Σ denotes the maximal extension of K in $\bar{K}$ which is unramified outside Σ.

COROLLARY 1.7. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, Σ is a set of places of K containing all primes above p, all primes where T is ramified, and all infinite places, and $h \in \Lambda$ satisfies Proposition* 1.6*. If $\psi \in \mathrm{Hom}_\Lambda(H^1(K_\Sigma/F,T),\Lambda_F)$, then*

$$h^r a_\tau^{5r}\psi(\mathbf{c}_F) \in \mathrm{char}(X_\infty)\Lambda_F.$$

PROOF. Note that $\mathbf{c}_F \in H^1(K_\Sigma/F,T)$ by Corollary B.3.5.

Suppose $0 \leq k < r$ and $M \geq N_F$ is a power of p, where N_F is as in in Proposition 1.6. Proposition 1.6 shows that

$$ha_\tau^5\Psi(k,F,MN_F^{r-k})\Lambda_{F,M} \subset f_{k+1}\Psi(k+1,F,MN_F^{r-k-1})\Lambda_{F,M},$$

so by induction, writing $M' = MN_F^r$ and using (3), we conclude that

$$\begin{aligned} h^r a_\tau^{5r}\Psi(0,F,M')\Lambda_{F,M} &\subset \Big(\prod_{i=1}^r f_i\Big)\Psi(r,F,M) \\ &\subset \Big(\prod_{i=1}^r f_i\Big)\Lambda_{F,M} = \mathrm{char}(X_\infty)\Lambda_{F,M} \end{aligned} \tag{4}$$

By Lemma IV.4.13(1), $\kappa_{F,1,M'}$ is the image of $\mathbf{c}_F$ under the injection

$$H^1(K_\Sigma/F,T)/M'H^1(K_\Sigma/F,T) \hookrightarrow H^1(K_\Sigma/F,W_{M'}) \hookrightarrow H^1(F,W_{M'}).$$

Let $\bar\psi$ denote the composition

$$\Lambda_{F,M'}\kappa_{F,1,M'} \hookrightarrow H^1(K_\Sigma/F,T)/M'H^1(K_\Sigma/F,T) \xrightarrow{\psi} \Lambda_{F,M'} \to \Lambda_{F,M}$$

induced by the inverse of this inclusion and by ψ. By definition $\bar\psi(\kappa_{F,1,M'}) \in \Psi(0,F,M')\Lambda_{F,M}$, so (4) shows

$$h^r a_\tau^{5r}\bar\psi(\kappa_{F,1,M}) \in \mathrm{char}(X_\infty)\Lambda_{F,M}.$$

Since this holds for every sufficiently large M, and $\bar\psi(\kappa_{F,1,M}) = \psi(\mathbf{c}_F) \pmod{M}$, this completes the proof of the corollary. $\square$

LEMMA 1.8. *Suppose G is a finite abelian group, R is a principal ideal domain, and B is finitely generated $R[G]$-module with no R-torsion. If $f \in R[G]$ is not a zero-divisor, $b \in B$, and*

$$\{\psi(b) : \psi \in \mathrm{Hom}_{R[G]}(B, R[G])\} \subset fR[G],$$

then $b \in fB$.

PROOF. Let $B' = Rb + fB$. Since f is not a zero-divisor, we have a commutative diagram

$$\begin{array}{ccccc}
\mathrm{Hom}_{R[G]}(B', fR[G]) & \xleftarrow{f} & \mathrm{Hom}_{R[G]}(B', R[G]) & \xrightarrow{\sim} & \mathrm{Hom}_R(B', R) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_{R[G]}(fB, fR[G]) & \xleftarrow{f} & \mathrm{Hom}_{R[G]}(fB, R[G]) & \xrightarrow{\sim} & \mathrm{Hom}_R(fB, R)
\end{array}$$

in which the horizontal maps are all isomorphisms (see for example Lemma IV.3.3 for the isomorphisms on the right).

Suppose $\bar{\varphi} \in \mathrm{Hom}_{R[G]}(fB, fR[G])$. Since B has no R-torsion, $\bar{\varphi}$ extends uniquely to a map $\varphi : B \to R[G]$, and by our assumption, the restriction of φ belongs to $\mathrm{Hom}_{R[G]}(B', fR[G])$. Thus all the vertical maps in the diagram above are isomorphisms. Since B' and fB are free R-modules, the surjectivity of the right-hand map shows that $B' = fB$, which proves the lemma. □

Let $\mathrm{ind}_\Lambda(\mathbf{c})$ be as in Definition II.3.1.

THEOREM 1.9. *With notation and assumptions as above,*

$$\mathrm{char}(X_\infty) \textit{ divides } a_\tau^{5r}\mathrm{ind}_\Lambda(\mathbf{c}).$$

PROOF. Suppose $h \in \Lambda$ satisfies Proposition 1.6. Let Σ be a finite set of places of K containing all primes above p, all primes where T is ramified, and all infinite places. If $K \subset_{\mathrm{f}} F \subset K_\infty$, Corollary 1.7 and Lemma 1.8 applied with $B = H^1(K_\Sigma/F, T)/H^1(K_\Sigma/F, T)_{\mathrm{tors}}$ and $b = h^r a_\tau^{5r}\mathbf{c}_F$ show (note that $H^1(K_\Sigma/F, T)$ is finitely generated over $\mathbf{Z}_p$ by Proposition B.2.7) that

$$h^r a_\tau^{5r}\mathbf{c}_F \in \mathrm{char}(X_\infty)(H^1(K_\Sigma/F, T)/H^1(K_\Sigma/F, T)_{\mathrm{tors}}).$$

It follows from Lemma I.2.2(ii) that if $K \subset_{\mathrm{f}} F \subset K_\infty$, $H^1(F, T)_{\mathrm{tors}}$ is annihilated by the annihilator in Λ of $W^{G_{K_\infty}}$, so $\varprojlim (H^1(F, T)_{\mathrm{tors}}) \subset H^1_\infty(K, T)_{\mathrm{tors}}$ (where the latter group is the Λ-torsion submodule), and we deduce that

$$h^r a_\tau^{5r}\mathbf{c}_{K,\infty} \in \mathrm{char}(X_\infty)(H^1_\infty(K, T)/H^1_\infty(K, T)_{\mathrm{tors}}).$$

Therefore if $\phi \in \mathrm{Hom}_\Lambda(H^1_\infty(K, T), \Lambda)$ then

$$h^r a_\tau^{5r}\phi(\mathbf{c}_{K,\infty}) \in \mathrm{char}(X_\infty).$$

Since h is relatively prime to (the principal ideal) $\mathrm{char}(X_\infty)$, it follows that

$$a_\tau^{5r}\phi(\mathbf{c}_{K,\infty}) \in \mathrm{char}(X_\infty).$$

This completes the proof. □

Proof of Theorems II.3.3 and II.3.4. Lemma 1.3(i) shows that a_τ is a (finite) positive integer, so Theorem II.3.4 is immediate from Theorem 1.9. If in addition hypotheses $\mathrm{Hyp}(K_\infty, T)$ are satisfied then $a_\tau = 1$ by Lemma 1.3(ii), and Theorem II.3.3 follows as well. $\square$

2. Galois groups and the evaluation map

Keep the notation of the previous section.

Definition 2.1. Define $q_\tau(x) = \det(1 - \tau^{-1}x|T^*)/(x-1)$. Our assumptions on τ ensure that

$$q_\tau(x) = \det(1 - \tau x|T)/(x-1) \in \mathcal{O}[x].$$

and that, by Lemma A.2.4(ii) (applied with $\sigma = \tau^{-1}$)

$$q_\tau(\tau^{-1}) : V/(\tau - 1)V \xrightarrow{\sim} V^{\tau=1}$$

is an isomorphism of 1-dimensional vector spaces.

The $\mathbf{D}(1)$-dual of the isomorphism θ^* of Definition 1.1 is an isomorphism

$$\mathcal{O}(1) \xrightarrow{\sim} T^{\tau=1}.$$

The inverse of this isomorphism, together with the generator ξ of $\mathcal{O}(1)$ chosen in Definition IV.4.1, gives an isomorphism

$$\theta : (W^{\tau=1})_{\mathrm{div}} \xrightarrow{\sim} \mathbf{D}.$$

Define $\bar{\theta}$ to be the (surjective, by Lemma A.2.4) composition

$$\bar{\theta} : W/(\tau-1)W \xrightarrow{q_\tau(\tau^{-1})} (W^{\tau=1})_{\mathrm{div}} \xrightarrow{\theta} \mathbf{D}.$$

We also fix once and for all an extension of θ

$$\theta : W^{\tau=1} \to \mathbf{D}.$$

This extension is not in general unique, but the difference between any two choices lies in $\mathrm{Hom}(W^{\tau=1}/(W^{\tau=1})_{\mathrm{div}}, \mathbf{D})$ which is killed by a_τ.

Definition 2.2. Recall the evaluation homomorphism

$$\mathrm{Ev}^* : G_{\Omega_\infty^{\langle\tau\rangle}} \to \mathrm{Hom}(H^1(K_\infty, W^*), \mathbf{D})$$

of Definition 1.1. Similarly we define

$$\mathrm{Ev} : G_{\Omega_\infty^{\langle\tau\rangle}} \to \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D})$$

by

$$\mathrm{Ev}(\sigma)([c]) = \bar{\theta}(c(\sigma))$$

for every $\sigma \in G_{\Omega_\infty^{\langle\tau\rangle}}$ and every cocycle c representing a class $[c] \in H^1(K_\infty, W)$. If B maps to $H^1(K_\infty, W)$ (for example, if B is a subgroup of $H^1(F, W_M)$ where $K \subset_{\mathrm{f}} F \subset K_\infty$ and $M \in \mathcal{O}$) then we will also write Ev or Ev_B for the induced map

$$G_{\Omega_\infty^{\langle\tau\rangle}} \longrightarrow \mathrm{Hom}(B, \mathbf{D}).$$

DEFINITION 2.3. Suppose $K \subset_{\mathfrak{f}} F \subset K_\infty$ and M is a power of p. Define

$$\mathcal{R}_{F,M,\tau} = \{\mathfrak{r} \in \mathcal{R} : \text{for every prime } \mathfrak{q} \text{ dividing } \mathfrak{r}, \mathrm{Fr}_{\mathfrak{q}} \text{ belongs to the conjugacy class of } \tau \text{ in } \mathrm{Gal}(F\Omega_M/K)\}$$

where $\Omega_M = K(1)(\boldsymbol{\mu}_M, (\mathcal{O}_K^\times)^{1/M}, W_M)/K)$ as in Definition 1.5. By Lemma IV.1.3, $\mathcal{R}_{F,M,\tau} \subset \mathcal{R}_{F,M}$ where $\mathcal{R}_{F,M}$ is the set defined in DefinitionIV.1.1.

Suppose $\mathfrak{q} \in \mathcal{R}_{F,M,\tau}$. Let $\mathfrak{Q}$ be a prime of $\bar{K}$ above $\mathfrak{q}$ such that $\mathrm{Fr}_{\mathfrak{Q}} = \tau$ on $F\Omega_M$, and write $\mathrm{Fr}_{\mathfrak{q}} = \mathrm{Fr}_{\mathfrak{Q}}$. Recall the generator $\sigma_{\mathfrak{q}}$ of $\mathrm{Gal}(K(\mathfrak{q})/K)$ given by Definition IV.4.1, and fix a lift of $\sigma_{\mathfrak{q}}$ to the inertia group $\mathcal{I}_{\mathfrak{Q}}$ of $\mathfrak{Q}$ in G_K. By Lemma I.4.7(i) (which applies thanks to Lemma IV.1.2(i)), evaluation at $\sigma_{\mathfrak{q}}$ induces an isomorphism

$$H^1_s(F_{\mathfrak{Q}}, W_M) \xrightarrow{\sim} W_M^{\mathrm{Fr}_{\mathfrak{q}}=1} = W_M^{\tau=1}$$

and we define another evaluation map $\mathrm{Ev}_{\mathfrak{q}} : H^1(F, W)_M \to \mathbf{D}$ by

$$\mathrm{Ev}_{\mathfrak{q}}(c) = \theta(c(\sigma_{\mathfrak{q}})).$$

As above, if B maps to $H^1(F, W)_M$ we will also write $\mathrm{Ev}_{\mathfrak{q}}$ or $\mathrm{Ev}_{\mathfrak{q},B}$ for the induced map $B \to M^{-1}\mathcal{O}/\mathcal{O} \xrightarrow{\sim} \mathcal{O}/M\mathcal{O}$.

LEMMA 2.4. *Suppose $K \subset_{\mathfrak{f}} F \subset K_\infty$, M is a power of p, and B is a Λ_F-module. Recall that $\Lambda_{F,M} = \Lambda_F/M\Lambda_F$. The map*

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{O}}(B, \mathcal{O}/M\mathcal{O}) & \longrightarrow & \mathrm{Hom}_\Lambda(B, \Lambda_{F,M}) \\ \psi & \mapsto & \tilde{\psi}, \end{array}$$

defined by

$$\tilde{\psi}(b) = \sum_{\eta \in \mathrm{Gal}(F/K)} \psi(\eta b)\eta^{-1}$$

is an $\mathcal{O}$-module isomorphism. If $\psi \in \mathrm{Hom}_{\mathcal{O}}(B, \mathcal{O}/M\mathcal{O})$ and $\sigma \in \mathrm{Gal}(F/K)$ then

$$\widetilde{\sigma\psi} = \sigma^{-1}\tilde{\psi}$$

so this bijection is not in general a $\Lambda_{F,M}$-module homomorphism.

PROOF. The map $\mathrm{Hom}_\Lambda(B, \Lambda_{F,M}) \to \mathrm{Hom}_{\mathcal{O}}(B, \mathcal{O}/M\mathcal{O})$ induced by composition with $\sum_{\eta \in \mathrm{Gal}(F/K)} a_\eta \eta \mapsto a_1$ is a 2-sided inverse of the map in question, so it is an isomorphism. The second identity is easily checked. (Note that σ acts on $\psi \in \mathrm{Hom}_{\mathcal{O}}(B, \mathcal{O}/M\mathcal{O})$ by $(\sigma\psi)(b) = \psi(\sigma^{-1}b)$ and on $\tilde{\psi} \in \mathrm{Hom}_\Lambda(B, \Lambda_{F,M})$ by $(\sigma\tilde{\psi})(b) = \sigma(\tilde{\psi}(b))$.) $\square$

DEFINITION 2.5. Suppose $K \subset_{\mathfrak{f}} F \subset K_\infty$ and M is a power of p. If B maps to $H^1(F, W)_M$ and $\gamma \in G_{\Omega_\infty^{(\tau)}}$, we will write $\widetilde{\mathrm{Ev}}(\gamma) = \widetilde{\mathrm{Ev}}_B(\gamma) \in \mathrm{Hom}_\Lambda(B, \Lambda_{F,M})$ and $\widetilde{\mathrm{Ev}}_{\mathfrak{q}} = \widetilde{\mathrm{Ev}}_{\mathfrak{q},B} \in \mathrm{Hom}_\Lambda(B, \Lambda_{F,M})$ for the images of $\mathrm{Ev}_B(\gamma)$ and $\mathrm{Ev}_{\mathfrak{q},B}$ under the map of Lemma 2.4. Thus

$$(\widetilde{\mathrm{Ev}}_B(\gamma))(b) = \sum_{\eta \in \mathrm{Gal}(F/K)} (\mathrm{Ev}(\gamma))(\eta b)\eta^{-1}, \quad \widetilde{\mathrm{Ev}}_{\mathfrak{q},B}(b) = \sum_{\eta \in \mathrm{Gal}(F/K)} \mathrm{Ev}_{\mathfrak{q}}(\eta b)\eta^{-1}.$$

The next two results, Theorems 2.6 and 2.7, are crucial for the proof of Theorem II.3.2 and Proposition 1.6. They are restatements of Theorems IV.5.4 and I.7.3(ii), respectively, in the language of these evaluation maps.

THEOREM 2.6. *Suppose* $\mathbf{c}$ *is an Euler system,* $K \subset_{\mathrm{f}} F \subset K_\infty$*,* M *is a power of* p*,* $\mathfrak{r} \in \mathcal{R}_{F,M}$*,* $\mathfrak{q} \in \mathcal{R}_{F,M,\tau}$ *is a prime not dividing* $\mathfrak{r}$*, and* $\kappa_{F,\mathfrak{r},M}$ *is the derivative class constructed in Chapter* IV §4. *Then*

$$\widetilde{\mathrm{Ev}}(\mathrm{Fr}_\mathfrak{q})(\kappa_{F,\mathfrak{r},M}) = \widetilde{\mathrm{Ev}}_\mathfrak{q}(\kappa_{F,\mathfrak{r}\mathfrak{q},M}).$$

PROOF. Suppose $\rho \in G_K$. Theorem IV.5.4 applied to the Euler system $\{\rho\mathbf{c}_{F(\mathfrak{r})}\}$ shows that, with $Q_\mathfrak{q}(x)$ as in Lemma IV.5.2,

$$\begin{aligned}\mathrm{Ev}(\mathrm{Fr}_\mathfrak{q})(\rho\kappa_{F,\mathfrak{r},M}) &= \theta \circ q_\tau(\tau^{-1})((\rho\kappa_{F,\mathfrak{r},M})(\mathrm{Fr}_\mathfrak{q}))\\ &= \theta \circ Q_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})((\rho\kappa_{F,\mathfrak{r},M})(\mathrm{Fr}_\mathfrak{q}))\\ &= \theta((\rho\kappa_{F,\mathfrak{r}\mathfrak{q},M})(\sigma_\mathfrak{q}))\\ &= \mathrm{Ev}_\mathfrak{q}(\rho\kappa_{F,\mathfrak{r}\mathfrak{q},M}).\end{aligned}$$

(Note that one consequence of Theorem IV.5.4 is that $(\rho\kappa_{F,\mathfrak{r}\mathfrak{q},M})(\sigma_\mathfrak{q}) \in W_{\mathrm{div}}^{\tau=1}$, so $\mathrm{Ev}_\mathfrak{q}(\rho\kappa_{F,\mathfrak{r}\mathfrak{q},M})$ does not depend on any choice made in extending θ from $W_{\mathrm{div}}^{\tau=1}$ to $W^{\tau=1}$.) The theorem follows immediately. □

NOTATION. If B is a G_K-module, v is a place of K, and $K \subset_{\mathrm{f}} F \subset K_\infty$ we will abbreviate

$$\begin{aligned}&F_v = F \otimes_K K_v = \oplus_{w|v} F_w,\\ &H^1(F_v, B) = \oplus_{w|v} H^1(F_w, B),\\ &H^1_f(F_v, B) = \oplus_{w|v} H^1_f(F_w, B),\\ &c_v = \oplus_{w|v} c_w \in H^1(F_v, B) \text{ for every } c \in H^1(F, B).\end{aligned}$$

There is a natural action of $\mathrm{Gal}(F/K)$ on $H^1(F_v, B)$. Concretely, every $\sigma \in \mathrm{Gal}(F/K)$ induces an isomorphism

$$H^1(F_w, B) \xrightarrow{\sim} H^1(F_{\sigma w}, B)$$

for every w, and summing these maps over w lying above v gives an automorphism of $H^1(F_v, B)$; see also Proposition B.5.2. In applying Theorem I.7.3 over the base field F instead of K, all of the maps are $\mathrm{Gal}(F/K)$-homomorphisms.

THEOREM 2.7. *Suppose* $K \subset_{\mathrm{f}} F \subset K_\infty$*,* M *is a power of* p*,* $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,M}$ *and* $\mathfrak{q}$ *is a prime in* $\mathcal{R}_{F,M,\tau}$*. Let* $\Sigma_{p\mathfrak{r}}$ *and* $\Sigma_{p\mathfrak{r}\mathfrak{q}}$ *denote the set of primes of* K *dividing* $p\mathfrak{r}$ *and* $p\mathfrak{r}\mathfrak{q}$*, respectively. Then*

$$a_\tau \widetilde{\mathrm{Ev}}_\mathfrak{q}(\mathcal{S}^{\Sigma_{p\mathfrak{r}\mathfrak{q}}}(F, W_M))\, \mathrm{Ev}^*_{\mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F, W_M^*)}(\mathrm{Fr}_\mathfrak{q}) = 0.$$

PROOF. Note that $\widetilde{\mathrm{Ev}}_\mathfrak{q}(\mathcal{S}^{\Sigma_{p\mathfrak{r}\mathfrak{q}}}(F, W_M)) \subset \Lambda_{F,M}$ and $\mathrm{Ev}^*_{\mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F, W_M^*)}(\mathrm{Fr}_\mathfrak{q})$ belongs to the $\Lambda_{F,M}$-module $\mathrm{Hom}(\mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F, W_M^*), \mathbf{D})$.

Suppose $c \in \mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F, W_M^*)$ and $d \in \mathcal{S}^{\Sigma_{p\mathfrak{r}\mathfrak{q}}}(F, W_M)$. Theorem I.7.3(ii), applied with $\Sigma = \Sigma_{p\mathfrak{r}\mathfrak{q}}$ and $\Sigma_0 = \Sigma_{p\mathfrak{r}}$, shows that $\langle c, d\rangle_\mathfrak{q} = 0$, where $\langle\ ,\ \rangle_\mathfrak{q} = \sum_{\mathfrak{Q}|\mathfrak{q}} \langle\ ,\ \rangle_\mathfrak{q}$ is the sum of the local pairings of Theorem I.4.1 at primes above $\mathfrak{q}$.

Let $\mathfrak{Q}$ be the prime above $\mathfrak{q}$ corresponding to our choice of $\mathrm{Fr}_\mathfrak{q}$ and $\sigma_\mathfrak{q}$. Consider the diagram

$$\begin{array}{ccccc}
H^1_f(F_\mathfrak{Q}, W_M^*) & \times & H^1_s(F_\mathfrak{Q}, W_M) & \xrightarrow{\langle\ ,\ \rangle_\mathfrak{Q}} & \mathcal{O}/M\mathcal{O} \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle \pm 1\otimes\xi} \\
W_M^*/(\tau-1)W_M^* & \times & (W_M)^{\tau=1} & \xrightarrow{\langle\ ,\ \rangle_{W_M}} & \mathcal{O}(1)/M\mathcal{O}(1) \\
{\scriptstyle \theta^*}\downarrow & & {\scriptstyle \theta}\downarrow & & \downarrow{\scriptstyle a_\tau\otimes\xi^{-1}} \\
\mathcal{O}/M\mathcal{O} & \times & \mathcal{O}/M\mathcal{O} & \xrightarrow{a_\tau} & \mathcal{O}/M\mathcal{O}
\end{array}$$

where the upper part (including the ambiguity of sign) comes from Lemma I.4.7 (so the upper left and upper center vertical maps are isomorphisms given by evaluation at $\mathrm{Fr}_\mathfrak{q}$ and $\sigma_\mathfrak{q}$, respectively), ξ is the chosen generator of $\mathbf{Z}_p(1)$ from which we defined $\sigma_\mathfrak{q}$, $\langle\ ,\ \rangle_{W_M}$ is induced by the natural pairing $W_M^* \times W_M \to \mathcal{O}(1)$, and the pairing on the bottom is $(x, y) \mapsto a_\tau xy$. Since a_τ annihilates $(W^{\tau=1})/(W^{\tau=1})_{\mathrm{div}}$, it follows from Definitions 1.1 and 2.1 of θ^* and θ that the bottom commutes. In other words,

$$a_\tau\langle c, d\rangle_\mathfrak{Q} = \pm a_\tau \theta((d)(\sigma_\mathfrak{q}))\theta^*((c)(\mathrm{Fr}_\mathfrak{q})) = \pm a_\tau \mathrm{Ev}_\mathfrak{q}(d)\mathrm{Ev}^*(\mathrm{Fr}_\mathfrak{q})(c).$$

Therefore

$$\begin{aligned}
(a_\tau \widetilde{\mathrm{Ev}}_\mathfrak{q}(d)\mathrm{Ev}^*(\mathrm{Fr}_\mathfrak{q}))(c) &= a_\tau \sum_{\rho\in\mathrm{Gal}(F/K)} \mathrm{Ev}_\mathfrak{q}(\rho d)(\mathrm{Ev}^*(\mathrm{Fr}_\mathfrak{q}))^{\rho^{-1}}(c) \\
&= a_\tau \sum_{\rho\in\mathrm{Gal}(F/K)} \mathrm{Ev}_\mathfrak{q}(\rho d)\mathrm{Ev}^*(\mathrm{Fr}_\mathfrak{q})(\rho c) \\
&= \pm a_\tau \sum_{\rho\in\mathrm{Gal}(F/K)} \langle \rho c, \rho d\rangle_\mathfrak{Q} \\
&= \pm a_\tau \sum_{\rho\in\mathrm{Gal}(F/K)} \langle c, d\rangle_{\mathfrak{Q}^\rho} = \pm a_\tau \langle c, d\rangle_\mathfrak{q} = 0. \qquad \square
\end{aligned}$$

COROLLARY 2.8. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$, M is a power of p, $\mathfrak{r} \in \mathcal{R}_{F,M}$, and $\gamma \in \tau G_{\Omega_\infty}$. Then*

$$a_\tau \widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,\mathfrak{r},M})\ \mathrm{Ev}^*_{\mathcal{S}_{\Sigma_p\mathfrak{r}}(F,W_M^*)}(\gamma) = 0.$$

PROOF. Fix a finite Galois extension L of $F(\boldsymbol{\mu}_M, (\mathcal{O}_K^\times)^{1/M}, W_M)$ such that the restrictions to L of $\kappa_{F,\mathfrak{r},M}$ and of $\mathcal{S}_{\Sigma_p}(F, W_M^*)$ are zero (by Lemma I.5.7 $\mathcal{S}_{\Sigma_p}(F, W_M^*)$ is finite, so such an extension exists). Let $\mathcal{N}$ be the ideal of Definition II.1.1 corresponding to $\mathbf{c}$. Choose a prime $\mathfrak{q}$ of K prime to $\mathfrak{r}\mathcal{N}$ (and a prime $\mathfrak{Q}$ of $\bar{K}$ above $\mathfrak{q}$) such that $\mathrm{Fr}_\mathfrak{q} = \gamma$ on L.

By Lemma IV.1.3, $\mathfrak{q} \in \mathcal{R}_{F,M,\tau}$. Thus Theorems 2.6 and IV.5.1 show

$$\widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,\mathfrak{r},M}) = \widetilde{\mathrm{Ev}}_\mathfrak{q}(\kappa_{F,\mathfrak{r}\mathfrak{q},M}) \in \widetilde{\mathrm{Ev}}_\mathfrak{q}(\mathcal{S}^{\Sigma_{p\mathfrak{r}\mathfrak{q}}}(F, W_M)),$$

and the corollary follows from Theorem 2.7. $\square$

3. The kernel and cokernel of the restriction map

Let $\mathcal{N}$ be the ideal of Definition II.1.1 corresponding to $\mathbf{c}$. By Lemma VI.1.3(i) applied to $T \oplus T^*$, we may twist T by a character of Γ if necessary to assume that, in addition to (1), for every prime λ of K dividing $\mathcal{N}$, the decomposition group of λ in G_K contains an element γ_λ with the property that

$$T^{\gamma_\lambda^{p^n}=1} = (T^*)^{\gamma_\lambda^{p^n}=1} = 0 \quad \text{for every } n \geq 0. \tag{5}$$

(Recall that by Proposition VI.2.1 and Theorem VI.3.5, each of the Theorems II.3.2, II.3.4, and II.3.3 holds for T if and only if it holds for a twist of T.) In particular, if $K \subset_{\mathrm{f}} F \subset K_\infty$ and λ is a prime of F dividing $\mathcal{N}$, then W^{G_F}, $(W^*)^{G_F}$, $W^{G_{F_\lambda}}$ and $(W^*)^{G_{F_\lambda}}$ are finite.

Definition 3.1. We define several ideals of Λ which will play a role in the proofs below. If B is a Λ-module, $\mathrm{Ann}_\Lambda(B)$ will denote the annihilator in Λ of B. Define

$$\mathcal{A}_{\mathrm{glob}} = \begin{cases} \mathrm{Ann}_\Lambda(W^{G_{K_\infty}}) & \text{if } \mathrm{rank}_{\mathbf{Z}_p}\Gamma > 1, \\ \mathrm{Ann}_\Lambda(W^{G_{K_\infty}}/(W^{G_{K_\infty}})_{\mathrm{div}}) & \text{if } \Gamma = \mathbf{Z}_p, \end{cases}$$

If v is a place of K and w is an extension of v to $\bar{K}$, let D_v denote the decomposition group of v in Γ, $\mathcal{I}_w$ the inertia group of w in G_K, and

$$K_{\infty,w} = \cup_{K \subset_{\mathrm{f}} F \subset K_\infty} F_w.$$

Define

$$\mathcal{A}_v = \begin{cases} \mathrm{Ann}_{\mathcal{O}[[D_v]]}(W^{G_{K_{\infty,w}}}) & \text{if } v \mid p \text{ and } \mathrm{rank}_{\mathbf{Z}_p} D_v > 1, \\ \mathrm{Ann}_{\mathcal{O}[[D_v]]}(W^{G_{K_{\infty,w}}}/(W^{G_{K_{\infty,w}}})_{\mathrm{div}}) & \text{if } v \mid p \text{ and } D_v = \mathbf{Z}_p, \\ \mathrm{Ann}_{\mathcal{O}[[D_v]]}(W^{\mathcal{I}_v}/(W^{\mathcal{I}_v})_{\mathrm{div}}) & \text{if } v \nmid p, \end{cases}$$

$$\mathcal{A}_{\mathcal{N}} = \prod_{v \mid \mathcal{N}} \mathcal{A}_v \Lambda.$$

We define $\mathcal{A}^*_{\mathrm{glob}}$, $\mathcal{A}^*_v$, and $\mathcal{A}^*_{\mathcal{N}}$ in exactly the same way with W replaced by W^*.

Lemma 3.2. *The ideals $\mathcal{A}_{\mathrm{glob}}$, $\mathcal{A}_{\mathcal{N}}$, $\mathcal{A}^*_{\mathrm{glob}}$, and $\mathcal{A}^*_{\mathcal{N}}$ defined above have height at least two in Λ.*

Proof. This is clear from the definitions of these ideals. □

Lemma 3.3. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$ and $i \geq 1$.*

(i) *$H^i(K_\infty/F, W^{G_{K_\infty}})$ is finite and annihilated by $\mathcal{A}_{\mathrm{glob}}$.*
(ii) *$H^i(K_\infty/F, (W^*)^{G_{K_\infty}})$ is finite and annihilated by $\mathcal{A}^*_{\mathrm{glob}}$.*
(iii) *If v is a prime of K above p and w is a prime of K_∞ above v, then $H^i(K_{\infty,w}/F_w, (W^*)^{G_{K_{\infty,w}}})$ is finite and annihilated by $\mathcal{A}^*_v$.*

Proof. Let $W' = W^{G_{K_\infty}}$, $(W^*)^{G_{K_\infty}}$, or $(W^*)^{G_{K_{\infty,w}}}$ and let $G = \mathrm{Gal}(K_\infty/F)$, $\mathrm{Gal}(K_\infty/F)$, or $\mathrm{Gal}(K_{\infty,w}/F_w)$, respectively. By (5), there is a $\gamma \in G_{F_w} \subset G_F$ such that $T^{\gamma=1} = (T^*)^{\gamma=1} = 0$. Let $\bar{\gamma} \in \Gamma$ denote the restriction of γ to K_∞.

Since Γ is abelian, the annihilator of W' annihilates $H^i(G, W')$ for every i. If $f(x) = \det(1 - \gamma x | T \oplus T^*) \in \mathcal{O}[x]$, then the Cayley-Hamilton theorem shows that $f(\bar{\gamma}^{-1})$ annihilates W', so in particular $f(\bar{\gamma}^{-1})$ annihilates $H^i(G, W')$.

But G acts trivially on $H^i(G, W')$, so it follows that $f(1)$ annihilates $H^i(G, W')$. Our hypothesis on γ ensures that $f(1) \neq 0$, so it follows without difficulty (since G is finitely generated and W' is co-finitely generated) that $H^i(G, W')$ is finite.

This proves the finiteness in all cases, and the annihilation when $\mathrm{rank}_{\mathbf{Z}_p}(G) > 1$. Suppose now $G \cong \mathbf{Z}_p$, and use the exact sequences

$$H^i(G, W'_{\mathrm{div}}) \longrightarrow H^i(G, W') \longrightarrow H^i(G, W'/W'_{\mathrm{div}}) \longrightarrow H^{i+1}(G, W'_{\mathrm{div}}).$$

If $i > 1$ then $H^i(G, W'_{\mathrm{div}}) = 0$ because G has cohomological dimension 1, and if σ is a topological generator of G then

$$H^1(G, W'_{\mathrm{div}}) \cong W'_{\mathrm{div}}/(\sigma - 1)W'_{\mathrm{div}} = 0$$

because $W'_{\mathrm{div}}/(\sigma - 1)W'_{\mathrm{div}}$ is a quotient of $W'_{\mathrm{div}}/(\bar{\gamma} - 1)W'_{\mathrm{div}}$. Thus for every $i > 0$

$$H^i(G, W') \cong H^i(G, W'/W'_{\mathrm{div}})$$

so we see that the annihilator of W'/W'_{div} annihilates $H^i(G, W')$ in this case as well. □

PROPOSITION 3.4. *Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$ and M is a power of p.*

(i) *The kernel of the restriction map*

$$H^1(F, W) \longrightarrow H^1(K_\infty, W)^{G_F}$$

is finite and is annihilated by $\mathcal{A}_{\mathrm{glob}}$.

(ii) *The kernel of the natural map*

$$H^1(F, W_M) \longrightarrow H^1(F, W)_M$$

is finite, bounded independently of M, and annihilated by $\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})$.

(iii) *The cokernel of the restriction map*

$$\mathcal{S}_{\Sigma_p}(F, W^*) \longrightarrow \mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}$$

is finite and is annihilated by $\mathcal{A}^*_{\mathrm{glob}}\mathcal{A}^*_{\mathcal{N}}$.

(iv) *If $\mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}$ is finite, then there is a power M_F of p such that if $M \geq M_F$ is a power of p, then $\mathcal{A}^*_{\mathrm{glob}}\mathcal{A}^*_{\mathcal{N}}$ annihilates the cokernel of the natural map*

$$\mathcal{S}_{\Sigma_p}(F, W^*_M) \longrightarrow \mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}.$$

(v) *The cokernel of the natural map*

$$\mathcal{S}_{\Sigma_p}(F, W^*_M) \longrightarrow \mathcal{S}_{\Sigma_p}(F, W^*)_M$$

is finite and bounded independently of M.

PROOF. The inflation-restriction exact sequence shows that the kernel of the restriction map in (i) is $H^1(K_\infty/F, W^{G_{K_\infty}})$, so (i) follows from Lemma 3.3(i). Lemma I.2.2(i) shows that the kernel of the map in (ii) is W^{G_F}/MW^{G_F}, which in turn is a quotient of a quotient of $W^{G_F}/(W^{G_F})_{\mathrm{div}}$, and (ii) follows.

Let res_{K_∞} denote the restriction map from $H^1(F, W^*)$ to $H^1(K_\infty, W^*)^{G_F}$. As in (i), the inflation-restriction exact sequence and Lemma 3.3(ii) show that $\mathcal{A}^*_{\mathrm{glob}}$ annihilates the cokernel of res_{K_∞} and hence of

$$\mathrm{res}_{K_\infty}^{-1}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}) \xrightarrow{\mathrm{res}_{K_\infty}} \mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}$$

as well. Since K_∞/F is unramified outside primes above p,

$$\mathrm{res}_{K_\infty}^{-1}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}) \subset \mathcal{S}^{\Sigma_p\mathcal{N}}(F, W^*)$$

and we have an exact sequence

$$0 \longrightarrow \mathcal{S}_{\Sigma_p}(F, W^*) \longrightarrow \mathrm{res}_{K_\infty}^{-1}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F})$$
$$\longrightarrow \oplus_{w|p} H^1(F_{w,\infty}/F_w, (W^*)^{G_{F_{w,\infty}}}) \oplus \oplus_{w|\mathcal{N}, w\nmid p} H^1_{\mathrm{ur}}(F_w, W^*)/H^1_f(F_w, W^*).$$

Now (iii) follows from Lemmas 3.3(ii) and I.3.5(iii).

Suppose further that $\mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}$ is finite. Since

$$\mathcal{S}_{\Sigma_p}(F, W^*) = \varinjlim \mathcal{S}_{\Sigma_p}(F, W^*_M),$$

we can choose M_F so that the image of $\mathcal{S}_{\Sigma_p}(F, W^*_{M_F})$ in $H^1(K_\infty, W^*)$ contains the image of $\mathrm{res}_{K_\infty}(\mathcal{S}_{\Sigma_p}(F, W^*))$. With this choice (iv) follows from (iii).

By Lemma I.5.4, the map $\mathcal{S}^{\Sigma_p}(F, W^*_M) \to \mathcal{S}^{\Sigma_p}(F, W^*)_M$ is surjective. Thus the cokernel in (v) is isomorphic to a subquotient of

$$\oplus_{w|p} \ker\left(H^1(F_w, W^*_M) \to H^1(F_w, W^*)\right).$$

For each w dividing p, Lemma I.2.2(i) shows that the above kernel is

$$(W^*)^{G_{F_w}}/M(W^*)^{G_{F_w}},$$

which is a quotient of the finite group $(W^*)^{G_{F_w}}/((W^*)^{G_{F_w}})_{\mathrm{div}}$ and hence is bounded independently of M. This proves (v). □

Definition 3.5. If $\eta \in \Lambda$, we will denote by $\eta^\bullet$ the image of η under the involution of Λ induced by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma$. Similarly if $\mathcal{A}$ is an ideal of Λ we will write $\mathcal{A}^\bullet$ for the ideal which is the image of $\mathcal{A}$ under this involution.

We will use repeatedly below that if B is a Λ-module and $\mathcal{A}$ is an ideal of Λ which annihilates B, then $\mathcal{A}^\bullet$ annihilates $\mathrm{Hom}(B, \mathbf{D})$.

Recall that $\Omega_\infty = K_\infty(1)(W, \boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})$.

Lemma 3.6. (i) *If* $c \in H^1(K_\infty, W)$ *and* $\mathrm{Ev}(\gamma)(c) = 0$ *for every* $\gamma \in G_{\Omega_\infty}$, *then* $a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))c = 0$,

(ii) $a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet\ \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}) \subset \mathcal{O}\mathrm{Ev}(G_{\Omega_\infty})$,

(iii) $a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W^*))^\bullet\ X_\infty \subset \mathcal{O}\mathrm{Ev}^*(G_{\Omega_\infty})$.

Proof. Unwinding the definition, we see that the dual of Ev on G_{Ω_∞} is given by the composition

$$H^1(K_\infty, W) \xrightarrow{\mathrm{res}_{\Omega_\infty}} \mathrm{Hom}(G_{\Omega_\infty}, W)^{G_{K_\infty}}$$
$$\longrightarrow \mathrm{Hom}(G_{\Omega_\infty}, W/(\tau-1)W) \xrightarrow{\bar\theta} \mathrm{Hom}(G_{\Omega_\infty}, \mathbf{D}). \quad (6)$$

The kernel of the first map is $H^1(\Omega_\infty/K_\infty, W)$. The kernel of the second map is

$$\mathrm{Hom}(G_{\Omega_\infty}, W)^{G_{K_\infty}} \cap \mathrm{Hom}(G_{\Omega_\infty}, (\tau-1)W).$$

If ψ belongs to this intersection, then $\psi(G_{\Omega_\infty})$ is a G_{K_∞}-stable submodule of $(\tau-1)W$. The kernel of $\bar\theta$ is $W^{q(\tau)=0}/(\tau-1)W$, which has the same order as $W^{\tau=1}/W^{\tau=1}_{\mathrm{div}}$ by Proposition A.2.5 (applied with $\sigma = \tau^{-1}$). Thus the product of the kernels of the second and third maps is annihilated by a_τ.

The assertion that $\mathrm{Ev}(\gamma)(c) = 0$ for every $\gamma \in G_{\Omega_\infty}$ is equivalent to saying that c maps to zero under (6), so this proves (i). Applying $\mathrm{Hom}_{\mathcal{O}}(\,\cdot\,, \mathbf{D})$ to (6) yields

$$G_{\Omega_\infty} \otimes \mathcal{O} \xrightarrow{\mathrm{Ev}} \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D})$$

and (ii) follows. The proof of (iii) is the same (except that in that case the third map of the analogue of (6) is induced by θ^*, which is injective). □

LEMMA 3.7. *Suppose $\Gamma \cong \mathbf{Z}_p$, and either K is imaginary quadratic or K is totally real and Leopoldt's conjecture holds for K.*

(i) *If G_{K_∞} acts trivially on T then $X_\infty/\mathrm{Ann}_\Lambda(T)X_\infty$ is finite.*
(ii) *If G_{K_∞} acts trivially on $T(-1) = T \otimes \mathcal{O}_{\varepsilon_{\mathrm{cyc}}^{-1}}$ then $X_\infty/\mathrm{Ann}_\Lambda(T(-1))X_\infty$ is finite.*

PROOF. Since we have assumed ($\mathrm{Hyp}(K_\infty, V)$) that V is an irreducible G_{K_∞}-representation, the situations (i) and (ii) can only arise if $\mathrm{rank}_{\mathcal{O}} T = 1$ and T is a twist of $\mathcal{O}$ or $\mathcal{O}(1)$, respectively, by a character of Γ.

Suppose ρ is a character of Γ. If we replace T by its twist $T \otimes \rho$, then W^* is replaced by $W^* \otimes \rho^{-1}$, Proposition VI.2.1(ii) shows that $\mathcal{S}_{\Sigma_p}(K_\infty, W^*)$ is replaced by $\mathcal{S}_{\Sigma_p}(K_\infty, W^*) \otimes \rho^{-1}$, so X_∞ is replaced by $X_\infty \otimes \rho$. Also $\mathrm{Ann}_\Lambda(T)$ is replaced by $\mathrm{Tw}_{\rho^{-1}}(\mathrm{Ann}_\Lambda(T))$ by Lemma VI.1.2(ii) (where $\mathrm{Tw}_\rho : \Lambda \to \Lambda$ is the map of Definition VI.1.1 induced by $\gamma \mapsto \rho^{-1}(\gamma)\gamma$ on Γ), and similarly for $\mathrm{Ann}_\Lambda(T(-1))$. It follows easily that $X_\infty/\mathrm{Ann}_\Lambda(T)X_\infty$ and $X_\infty/\mathrm{Ann}_\Lambda(T(-1))X_\infty$ remain unchanged as $\mathcal{O}$-modules. Thus both assertions of the lemma are invariant under twisting by characters of Γ, so we may assume that $T = \mathcal{O}$ for (i) and $T = \mathcal{O}(1)$ for (ii) (although because of this twist we can not assume (5) for this proof). Then in both cases we are trying to show that $X_\infty/\mathcal{J}X_\infty$ is finite, where $\mathcal{J}$ denotes the augmentation ideal of Λ. We may as well suppose that $\mathcal{O} = \mathbf{Z}_p$.

Suppose first that $T = \mathbf{Z}_p(1)$. Then $W^* = \mathbf{Q}_p/\mathbf{Z}_p$ and $H^1(K_\infty, W^*) = \mathrm{Hom}(G_{K_\infty}, \mathbf{Q}_p/\mathbf{Z}_p)$, so by the example of Chapter I §6.1, $X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$, where L_∞ is the maximal abelian p-extension of K_∞ such that all primes are unramified and all primes above p split completely in L_∞/K_∞. A standard Iwasawa theory argument ([**Iw3**] §3.1) now shows that $X_\infty/\mathcal{J}X_\infty = \mathrm{Gal}(L/K_\infty)$ where L is the maximal abelian extension of K in L_∞, and that this Galois group is finitely generated.

If K is totally real and Leopoldt's conjecture holds for K, then K has no extension with Galois group $\mathbf{Z}_p^2$, so L/K_∞ is finite. If K is imaginary quadratic then K has a unique extension with Galois group $\mathbf{Z}_p^2$, but no prime above p is infinitely split in this extension, so again L/K_∞ is finite. This proves the lemma in this case.

Now suppose $T = \mathbf{Z}_p$, so $W^* = \boldsymbol{\mu}_{p^\infty}$. By Proposition 3.4(iii), the map

$$\mathcal{S}_{\Sigma_p}(K, \boldsymbol{\mu}_{p^\infty}) \longrightarrow \mathcal{S}_{\Sigma_p}(K_\infty, \boldsymbol{\mu}_{p^\infty})^{G_K} = \mathrm{Hom}(X_\infty/\mathcal{J}X_\infty, \mathbf{Q}_p/\mathbf{Z}_p)$$

has finite cokernel (note that even though (5) does not hold for W, it is satisfied for W^* so Proposition 3.4(iii) holds). Since Leopoldt's conjecture holds for K, Corollary I.6.4 shows that $\mathcal{S}_{\Sigma_p}(K, \boldsymbol{\mu}_{p^\infty})$ is finite. This completes the proof. □

4. Proof of Theorem II.3.2

In this section we will prove Theorem II.3.2. The general idea is that if $\mathbf{c} \notin H^1_\infty(K,T)_{\mathrm{tors}}$, then we can use Corollary 2.8 to construct a nonzero annihilator of X_∞, and hence X_∞ is Λ-torsion.

LEMMA 4.1. *X_∞ is a finitely generated Λ module.*

PROOF. Let $\mathcal{J}$ denote the augmentation ideal in Λ. Then $X_\infty/\mathcal{J}X_\infty = \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K_\infty,W^*)^{G_K},\mathbf{D})$. Thus by Nakayama's Lemma, to prove the lemma we need only show that $\mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K_\infty,W^*)^{G_K},\mathbf{D})$ is finitely generated over $\mathcal{O}$.

By Proposition 3.4(iii), the cokernel of the restriction map

$$\mathcal{S}_{\Sigma_p}(K,W^*) \longrightarrow \mathcal{S}_{\Sigma_p}(K_\infty,W^*)^{G_K}$$

is finite, and by Lemma I.5.7(iii), $\mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K,W^*),\mathbf{D})$ is finitely generated. This proves the lemma. $\square$

LEMMA 4.2. *Suppose X_∞ is not a torsion Λ-module. Define*

$$J = \{\gamma \in \tau G_{\Omega_\infty} : \mathrm{Ev}^*(\gamma) \notin (X_\infty)_{\mathrm{tors}}\}$$

Then the subgroup of G_K generated by J contains an open subgroup of G_{Ω_∞}.

PROOF. By Corollary C.2.2 (applied with $F = K_\infty$), $H^1(\Omega_\infty/K_\infty,W^*)$ is a torsion Λ-module. Therefore if X_∞ is not a torsion Λ-module, Lemma 3.6(iii) shows that there is a $\gamma_0 \in G_{\Omega_\infty}$ such that $\mathrm{Ev}^*(\gamma_0) \notin (X_\infty)_{\mathrm{tors}}$. Then either τ or $\tau\gamma_0$ belongs to J, so J is nonempty.

Since X_∞ is finitely generated by Lemma 4.1, $(X_\infty)_{\mathrm{tors}}$ is a closed submodule of X_∞. The map Ev^* is continuous, so $J = (\mathrm{Ev}^*)^{-1}(X_\infty - (X_\infty)_{\mathrm{tors}}) \cap \tau G_{\Omega_\infty}$ is open in τG_{Ω_∞}, and the lemma follows. $\square$

PROOF OF THEOREM II.3.2. Let $\mathbf{c}$ be the Euler system of Theorem II.3.2. We will show, under the assumption that X_∞ is not a torsion Λ-module, that $\mathbf{c}_{K,\infty} \in H^1_\infty(K,T)_{\mathrm{tors}}$.

Suppose that X_∞ is not a torsion Λ-module. Fix a γ in the set J of Lemma 4.2, i.e., $\gamma \in \tau G_{\Omega_\infty}$ such that $\mathrm{Ev}^*(\gamma) \notin (X_\infty)_{\mathrm{tors}}$.

Suppose $K \subset_{\mathrm{f}} F \subset K_\infty$ and M is a power of p. Let $\kappa_{F,M} = \kappa_{F,1,M}$ be the derivative class constructed in Chapter IV §4. By Lemma IV.4.13(i), $\kappa_{F,M}$ is the image of $\mathbf{c}_F$ under the injection

$$H^1(F,T)/MH^1(F,T) \hookrightarrow H^1(F,W_M).$$

By Corollary 2.8,

$$a_\tau \widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,M})\,\mathrm{Ev}^*_{\mathcal{S}_{\Sigma_p}(F,W^*_M)}(\gamma) = 0.$$

Since by definition the map $\widetilde{\mathrm{Ev}}(\gamma)$ factors through restriction to K_∞, and for every $F \subset_{\mathrm{f}} F'$

$$(\kappa_{F,M})_{F'} = (\mathrm{Cor}_{F'/F}\kappa_{F',M})_{F'} = \sum_{\rho\in\mathrm{Gal}(F'/F)} \rho\kappa_{F',M},$$

it follows that the restriction of $\widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F',M}) \in \Lambda_{F',M}$ to F is $\widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,M}) \in \Lambda_{F,M}$. Thus $\varprojlim_{F,M} \widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,M}) \in \Lambda$ and

$$a_\tau \varprojlim_{F,M} \widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,M})\ \mathrm{Ev}^*(\gamma) = 0.$$

Since $\mathrm{Ev}^*(\gamma) \notin (X_\infty)_{\mathrm{tors}}$ it follows that $\varprojlim \widetilde{\mathrm{Ev}}(\gamma)(\kappa_{F,M}) = 0$. Since this holds for every $\gamma \in J$, Lemma 4.2 shows that it holds for every γ in an open subgroup of G_{Ω_∞}. Since an open subgroup has finite index, and Λ is torsion-free, we conclude that for every F, every M, and *every* $\gamma \in G_{\Omega_\infty}$,

$$\mathrm{Ev}(\gamma)(\kappa_{F,M}) = 0. \tag{7}$$

We will show that this is not compatible with the assumption that $\mathbf{c}_{K,\infty} = \{\mathbf{c}_F\}_F \notin H^1_\infty(K,T)_{\mathrm{tors}}$.

Write $(\kappa_{F,M})_{K_\infty}$ for the image of $\kappa_{F,M}$ in $H^1(K_\infty, W)$. By Proposition 3.6(i), it follows from (7) that

$$a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))(\kappa_{F,M})_{K_\infty} = 0.$$

But Proposition 3.4(i) and (ii) show that the kernel of the map $H^1(F, W_M) \to H^1(K_\infty, W)$ is finite and bounded independently of M, so we conclude that there is an integer $m > 0$, independent of M, such that

$$m\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))\kappa_{F,M} = 0.$$

Since $\kappa_{F,M}$ is the image of $\mathbf{c}_F$ under the injection

$$H^1(F,T)/MH^1(F,T) \hookrightarrow H^1(F, W_M)$$

(Lemma IV.4.13(i)), it follows that $m\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))\mathbf{c}_F$ is divisible in $H^1(F,T)$, and hence by Proposition B.2.4

$$m\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))\mathbf{c}_F = 0.$$

Using Lemma I.2.2(ii) to control the torsion in $H^1(F,T)$ we see that for every $K \subset_{\mathrm{f}} F \subset K_\infty$

$$\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))\mathbf{c}_F = 0.$$

But this annihilator of $\mathbf{c}_F$ is independent of F, and by Corollary C.2.2 applied with $F = K_\infty$, it is nonzero as well. Thus $\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W)) \subset \Lambda$ is a nonzero annihilator of $\mathbf{c}_{K,\infty} \in H^1_\infty(K,T)$. This contradicts the assumption that $\mathbf{c}_{K,\infty} \notin H^1_\infty(K,T)_{\mathrm{tors}}$, and completes the proof. □

5. Galois equivariance of the evaluation maps

For the proofs of Propositions 1.4 and 1.6 in the following sections, it would be convenient if G_{Ω_∞} were a Λ-module and Ev and Ev^* were Λ-module homomorphisms. Unfortunately this makes no sense, since G_{Ω_∞} is not a Λ-module. We will get around this be defining an action of a subring of Λ on a quotient of G_{Ω_∞}, and Ev and Ev^* will behave well with respect to this action.

Proposition 5.1. *There is a subgroup* Γ_0 *of finite index in* Γ, *characters* $\chi, \chi^* : \Gamma_0 \to \mathcal{O}^\times$, *an abelian extension* L *of* Ω_∞, *and an action of* $\mathbf{Z}_p[[\Gamma_0]]$ *on* $\mathrm{Gal}(L/\Omega_\infty)$ *such that*

(i) Ev *and* Ev^* *on* G_{Ω_∞} *factor through* $\mathrm{Gal}(L/\Omega_\infty)$,

(ii) *if* $\eta \in \Gamma_0$ *and* $\gamma \in \mathrm{Gal}(L/\Omega_\infty)$ *then*

$$\mathrm{Ev}(\gamma^\eta) = \chi(\eta)\eta(\mathrm{Ev}(\gamma)), \quad \mathrm{Ev}^*(\gamma^\eta) = \chi^*(\eta)\eta(\mathrm{Ev}^*(\gamma)).$$

Proof. Let L be the maximal abelian p-extension of

$$K_\infty(\boldsymbol{\mu}_{p^\infty}, W) = K_\infty(\boldsymbol{\mu}_{p^\infty}, W^*) = K_\infty(W, W^*).$$

Then $\Omega_\infty \subset L$, and every cocycle in $H^1(K_\infty, W)$ or $H^1(K_\infty, W^*)$ vanishes on G_L, so (i) is satisfied.

Consider the diagram of fields in Figure 2. By Proposition C.1.7, there is a

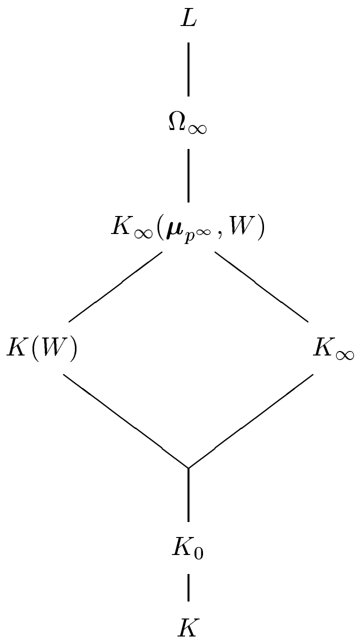

Figure 2

finite extension K_0 of K in $K(W) \cap K_\infty$ such that the center of $\mathrm{Gal}(K(W)/K)$ maps onto $\mathrm{Gal}(K(W) \cap K_\infty/K_0)$. Define

$$\Gamma_0 = \mathrm{Gal}(K_\infty/K_0).$$

Fix once and for all a set of independent topological generators $\{\gamma_1, \ldots, \gamma_d\}$ of Γ_0, and for every i fix a lift $\tilde{\gamma}_i \in \mathrm{Gal}(K_\infty(\boldsymbol{\mu}_{p^\infty}, W)/K_0)$ of γ_i such that the restriction of $\tilde{\gamma}_i$ to $K(W)$ belongs to the center of $\mathrm{Gal}(K(W)/K)$. Since $K_\infty(\boldsymbol{\mu}_{p^\infty}, W)$ is the compositum of $K(W)$ with an abelian extension of K, each $\tilde{\gamma}_i$ belongs to the center of $\mathrm{Gal}(K_\infty(\boldsymbol{\mu}_{p^\infty}, W)/K)$, so these choices extend by multiplicativity to define a homomorphism

$$\Gamma_0 \longrightarrow \mathrm{Gal}(K_\infty(\boldsymbol{\mu}_{p^\infty}, W)/K_0),$$

whose image lies in the center of $\mathrm{Gal}(K_\infty(\boldsymbol{\mu}_{p^\infty}, W)/K)$, which is a section for the projection map $\mathrm{Gal}(K_\infty(\boldsymbol{\mu}_{p^\infty}, W)/K_0) \to \Gamma_0$. We will denote this map by $\gamma \mapsto \tilde{\gamma}$, and we will use this map to define an action of Γ_0 on $\mathrm{Gal}(L/\Omega_\infty)$: for $\gamma \in \mathrm{Gal}(L/\Omega_\infty)$ and $\eta \in \Gamma_0$, define

$$\gamma^\eta = \tilde{\eta}\gamma\tilde{\eta}^{-1}.$$

This definition extends to give an action of $\mathbf{Z}_p[[\Gamma_0]]$ on $\mathrm{Gal}(L/\Omega_\infty)$. It is not canonical, since it depends on our choice of the $\tilde{\gamma}_i$.

By Lemma C.1.6, since V is assumed irreducible, every element of the center of $\mathrm{Gal}(K(W)/K)$ acts on W by a scalar in $\mathcal{O}^\times$. Thus the choice above defines a character

$$\chi : \Gamma_0 \to \mathcal{O}^\times, \qquad \chi(\eta) = \tilde{\eta} \in \mathrm{Aut}(W).$$

Similarly, if $\eta \in \Gamma_0$ then $\tilde{\eta}$ belongs to the center of $\mathrm{Gal}(K(W^*)/K)$ so we get a second character

$$\chi^* : \Gamma_0 \to \mathcal{O}^\times, \qquad \chi^*(\eta) = \tilde{\eta} \in \mathrm{Aut}(W^*).$$

Suppose $c \in H^1(K_\infty, W)$, $\gamma \in \mathrm{Gal}(L/\Omega_\infty)$, and $\eta \in \Gamma_0$. Since $\mathrm{Ev}(\gamma) \in \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D})$,

$$(\eta\mathrm{Ev}(\gamma))(c) = \mathrm{Ev}(\gamma)(\eta^{-1}c) = \bar{\theta}((\eta^{-1}c)(\gamma)) = \bar{\theta}(\tilde{\eta}^{-1}(c(\gamma^\eta))) = \chi(\eta^{-1})\mathrm{Ev}(\gamma^\eta)(c).$$

In other words

$$\mathrm{Ev}(\gamma^\eta) = \chi(\eta)\eta(\mathrm{Ev}(\gamma)),$$

and similarly with Ev^* and χ^*. This proves (ii). □

Recall the involution $\eta \mapsto \eta^\bullet$ of Λ given by Definition 3.5

PROPOSITION 5.2. *Suppose X' is a Λ-submodule of X_∞ and X_∞/X' is pseudo-null. Then there is an ideal $\mathcal{A}_0$ of height at least two in Λ such that for every $K \subset_{\mathrm{f}} F \subset K_\infty$,*

$$\mathcal{A}_0 a_\tau \mathrm{Ann}_\Lambda(W^{G_{K_\infty}})^\bullet \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet \mathrm{Hom}(H^1(F, W_M), \mathbf{D}) \subset \mathcal{O}\mathrm{Ev}((\mathrm{Ev}^*)^{-1}(X') \cap G_{\Omega_\infty}).$$

In other words, if

$$\psi \in \mathcal{A}_0 a_\tau \mathrm{Ann}_\Lambda(W^{G_{K_\infty}})^\bullet \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet \mathrm{Hom}(H^1(F, W_M), \mathbf{D})$$

then there are $\gamma_1, \ldots, \gamma_k \in G_{\Omega_\infty}$ and $c_1, \ldots, c_k \in \mathcal{O}$ such that $\mathrm{Ev}^*(\gamma_i) \in X'$ for every i and

$$\sum_{i=1}^k c_i \mathrm{Ev}_{H^1(F,W)}(\gamma_i) = \psi.$$

Proof. The general proof is quite tedious. However, there is a simple proof when $\Gamma \cong \mathbf{Z}_p$. In that case X_∞/X' is finite, so $(\mathrm{Ev}^*)^{-1}(X') \cap G_{\Omega_\infty}$ has finite index in G_{Ω_∞}, so by Proposition 3.6(ii), $\mathcal{O}\mathrm{Ev}((\mathrm{Ev}^*)^{-1}(X') \cap G_{\Omega_\infty})$ contains a subgroup of finite index (not *a priori* a Λ-submodule) of

$$a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}).$$

But every subgroup of finite index contains a submodule of finite index, and hence there is a $j \geq 0$ such that

$$\mathcal{M}^j a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}) \\ \subset \mathcal{O}\mathrm{Ev}((\mathrm{Ev}^*)^{-1}(X') \cap G_{\Omega_\infty})$$

where we recall that $\mathcal{M}$ is the maximal ideal of Λ. By Proposition 3.4(i) and (ii), $\mathcal{A}^\bullet_{\mathrm{glob}} \mathrm{Ann}_\Lambda(W^{G_{K_\infty}})^\bullet$ annihilates the cokernel of the map $\mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}) \to \mathrm{Hom}(H^1(F, W_M), \mathbf{D})$, so the proposition is satisfied with $\mathcal{A}_0 = \mathcal{M}^j \mathcal{A}^\bullet_{\mathrm{glob}}$ (which has height at least two by Lemma 3.2).

We now turn to the general case. Let Γ_0, L, χ, and χ^* be as in Proposition 5.1. We define

$$\mathrm{Tw}_\chi : \mathcal{O}[[\Gamma_0]] \to \mathcal{O}[[\Gamma_0]] \quad \text{by} \quad \gamma \mapsto \chi(\gamma)\gamma$$

and similarly for Tw_{χ^*}, and then Proposition 5.1 shows that for every $\eta \in \mathbf{Z}_p[[\Gamma_0]]$ and $\gamma \in \mathrm{Gal}(L/\Omega_\infty)$

$$\mathrm{Ev}(\gamma^\eta) = \mathrm{Tw}_\chi(\eta)(\mathrm{Ev}(\gamma)), \quad \mathrm{Ev}^*(\gamma^\eta) = \mathrm{Tw}_{\chi^*}(\eta)(\mathrm{Ev}^*(\gamma)). \tag{8}$$

Note that a pseudo-null Λ-module is also pseudo-null as a $\mathbf{Z}_p[[\Gamma_0]]$-module, and conversely if $\mathcal{A}$ is an ideal of $\mathbf{Z}_p[[\Gamma_0]]$ of height at least two then $\mathcal{A}\Lambda$ is an ideal of Λ of height at least two.

Define

$$\mathcal{A} = \mathrm{Tw}_{\chi^*}^{-1}(\mathrm{Ann}_{\mathcal{O}[[\Gamma_0]]}(X_\infty/X')) \cap \mathbf{Z}_p[[\Gamma_0]].$$

Since X_∞/X' is assumed to be a pseudo-null Λ-module, $\mathcal{A}$ is an ideal of height at least two in $\mathbf{Z}_p[[\Gamma_0]]$. By (8),

$$\mathrm{Ev}^*(\mathcal{A}\mathrm{Gal}(L/\Omega_\infty)) = \mathrm{Tw}_{\chi^*}(\mathcal{A})\mathrm{Ev}^*(G_{\Omega_\infty}) \subset X',$$

and by (8) and Proposition 3.6(ii), for every $K \subset_{\mathrm{f}} F \subset K_\infty$

$$\mathcal{O}\mathrm{Ev}(\mathcal{A}\mathrm{Gal}(L/\Omega_\infty)) = \mathcal{O}\mathrm{Tw}_\chi(\mathcal{A})\mathrm{Ev}(G_{\Omega_\infty}) \\ \supset \mathrm{Tw}_\chi(\mathcal{A}) a_\tau \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}).$$

By Proposition 3.4(i), (ii), the image of the composition

$$\mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}) \longrightarrow \mathrm{Hom}(H^1(F, W), \mathbf{D}) \longrightarrow \mathrm{Hom}(H^1(F, W_M), \mathbf{D})$$

contains

$$\mathcal{A}^\bullet_{\mathrm{glob}} \mathrm{Ann}_\Lambda(W^{G_{K_\infty}})^\bullet \mathrm{Hom}(H^1(F, W_M), \mathbf{D}).$$

Combining these inclusions proves the proposition, with $\mathcal{A}_0 = \mathcal{A}^\bullet_{\mathrm{glob}} \mathrm{Tw}_\chi(\mathcal{A})$, which has height at least two by Lemma 3.2. $\square$

6. Proof of Proposition 1.4

Proposition 1.4 is very easy to prove in the following (fairly common; see the examples of Chapter III) special case. Suppose that hypotheses $\mathrm{Hyp}(K_\infty, T)$ are satisfied (so $a_\tau = 1$ by Lemma 1.3(ii)), $\mathcal{O} = \mathbf{Z}_p$, and $H^1(\Omega_\infty/K_\infty, W^*) = 0$. Use (2) to choose a sequence $z_1, \ldots, z_r \in X_\infty$ such that $\oplus \Lambda z_i \cong \oplus \Lambda/f_i\Lambda$. By Lemma 3.6(iii), under our assumptions we have

$$\mathrm{Ev}^*(\tau G_{\Omega_\infty}) = \mathrm{Ev}^*(\tau) + \mathrm{Ev}^*(G_{\Omega_\infty}) = \mathrm{Ev}^*(\tau) + X_\infty = X_\infty,$$

so Proposition 1.4 holds with these z_i and with $\mathfrak{g}_i = f_i\Lambda$.

The rest of this section is devoted to the proof of Proposition 1.4 in the general case, which unfortunately is more complicated.

We say that two ideals $\mathcal{A}$ and $\mathcal{B}$ of Λ are relatively prime if $\mathcal{A} + \mathcal{B}$ has height at least two.

LEMMA 6.1. $\mathrm{char}(X_\infty)$ *is relatively prime to each of the ideals*

$$\mathrm{Ann}_\Lambda(W^{G_{K_\infty}}), \quad \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W)), \quad \mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W^*))^\bullet.$$

PROOF. The proofs for all three ideals are similar. If $W^{G_{K_\infty}}$ is finite or if $\mathrm{rank}_{\mathbf{Z}_p}(\Gamma) > 1$ then $\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})$ has height at least 2 and the first assertion holds trivially. We have assumed that V is irreducible over G_{K_∞}, so if $W^{G_{K_\infty}}$ is infinite then G_{K_∞} acts trivially on T. Thus (using hypothesis $\mathrm{Hyp}(K_\infty/K)$) the first assertion follows from Lemma 3.7.

The other two assertions follow similarly, using Lemma 3.7 and Corollary C.2.2. We sketch briefly the proof for the third ideal.

Corollary C.2.2 applied to T^*, with $F = K_\infty$, $\Omega = \Omega_\infty$, gives three cases. In case (i), $H^1(\Omega_\infty/K_\infty, W^*)$ is finite, so $\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W^*))$ has height at least two, and hence is relatively prime to everything. In case (ii) (resp. (iii)), G_K acts on T^* via a character ρ (resp. $\varepsilon_{\mathrm{cyc}}\rho$), and $H^1(\Omega_\infty/K_\infty, W^*)$ has a subgroup C of finite index on which G_K acts via ρ. Then G_K acts on T via $\varepsilon_{\mathrm{cyc}}\rho^{-1}$ (resp. ρ^{-1}), so $\mathrm{Ann}_\Lambda(C)^\bullet \supset \mathrm{Ann}_\Lambda(T(-1))$ (resp. $\mathrm{Ann}_\Lambda(C)^\bullet \supset \mathrm{Ann}_\Lambda(T)$). Since

$$\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W^*)) \supset \mathrm{Ann}_\Lambda(C)\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W^*)/C)$$

and the latter ideal has height at least two, the lemma in this case follows from Lemma 3.7. □

LEMMA 6.2. *Suppose B is a torsion Λ-module, $x, y \in B$, $g_x, g_y \in \Lambda$ and $\mathrm{Ann}_\Lambda(x) \subset g_x\Lambda$ and $\mathrm{Ann}_\Lambda(y) \subset g_y\Lambda$. Then there is an $n \in \mathbf{Z}$ such that*

$$\mathrm{Ann}_\Lambda(x + ny) \subset [g_x, g_y]\Lambda$$

where $[g_x, g_y]$ denotes the least common multiple of g_x and g_y.

PROOF. Suppose $\mathfrak{P}$ is a (height-one) prime divisor of $[g_x, g_y]$, and define

$$S_\mathfrak{P} = \{n \in \mathbf{Z} : \mathrm{Ann}_\Lambda(x + ny) \not\subset \mathfrak{P}^{\mathrm{ord}_\mathfrak{P}[g_x, g_y]}\}.$$

Recall that $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$. We will show that $S_\mathfrak{P}$ has at most one element if $\mathfrak{P} \neq \mathfrak{p}\Lambda$, and $S_\mathfrak{P}$ is contained in a congruence class modulo p if $\mathfrak{P} = \mathfrak{p}\Lambda$. Then it will follow that $\mathbf{Z} - \cup_\mathfrak{P} S_\mathfrak{P}$ is nonempty, and every n in this set satisfies the conclusion of the lemma.

Suppose $n, m \in S_{\mathfrak{P}}$, and let $\mathcal{A} = \mathrm{Ann}_\Lambda(x+ny) \cap \mathrm{Ann}_\Lambda(x+my)$. Then $\mathcal{A} \not\subset \mathfrak{P}^k$, where $k = \mathrm{ord}_{\mathfrak{P}}[g_x, g_y]$. But $(n-m)\mathcal{A}$ annihilates both y and x, so $(n-m)\mathcal{A} \subset \mathfrak{P}^k$ and we conclude that $n - m \in \mathfrak{P}$. If $\mathfrak{P} \neq \mathfrak{p}\Lambda$ it follows that $n = m$, and if $\mathfrak{P} = \mathfrak{p}\Lambda$ then $n \equiv m \pmod{p}$. This completes the proof. $\square$

LEMMA 6.3. *Suppose B is a finitely-generated torsion Λ-module, pseudo-isomorphic to $\oplus_{i=1}^k \Lambda/h_i\Lambda$, where $h_{i+1} \mid h_i$ for $1 \leq i < k$. Suppose we are given a subring Λ_0 of Λ such that Λ is finitely generated as a Λ_0-module, a Λ_0-submodule $B_0 \subset B$, and an element $t \in B$ such that t and B_0 generate B over Λ. Then there are elements $x_1 \in t + B_0$ and $x_2, \ldots, x_k \in B_0$ such that*

(i) *$\Lambda x_1 \cong \Lambda/\mathfrak{h}_1$ where $\mathfrak{h}_1 \subset h_1\Lambda$ and $h_1\Lambda/\mathfrak{h}_1$ is pseudo-null,*
(ii) *for every j, $2 \leq j \leq k$, there is a split exact sequence*

$$0 \longrightarrow \sum_{i=1}^{j-1} \Lambda x_i \longrightarrow \sum_{i=1}^{j} \Lambda x_i \longrightarrow \Lambda/h_j\Lambda \longrightarrow 0.$$

If $t = 0$ then we can replace (i) *by*

(i′) *$\Lambda x_1 \cong \Lambda/h_1\Lambda$, i.e.,* (ii) *holds for $j = 1$ as well.*

PROOF. We will prove the lemma by induction on k.

If $\mathcal{A}$ is an ideal of Λ then $\mathrm{char}(\Lambda/\mathcal{A})$ is the unique principal ideal containing $\mathcal{A}$ with pseudo-null quotient. For every $x \in B_0$ write

$$\mathcal{A}_x = \mathrm{char}(\Lambda/\mathrm{Ann}_\Lambda(x)).$$

By Lemma 6.2 (applied successively with $x = t$ and y running through a sequence of elements of B_0) we can choose $x_1 \in t + B_0$ such that $\mathcal{A}_{x_1} \subset \mathcal{A}_x$ for every $x \in t + B_0$. Since t and B_0 generate B over Λ, we must have $\mathcal{A}_{x_1} = h_1\Lambda$, so (i) is satisfied. This proves the lemma when $k = 1$ and $t \neq 0$.

If $t = 0$ then choose $g \in \Lambda_0$, prime to h_1, which annihilates the pseudo-null Λ-module $h_1\Lambda/\mathrm{Ann}_\Lambda(x_1)$, and replace x_1 by gx_1. This element has annihilator exactly $h_1\Lambda$, so this completes the proof when $k = 1$.

If $k > 1$, choose x_1 as above. Let $B' = B/\Lambda x_1$, let B_0' be the image of B_0 in B', and let $t' = 0$. Then B' is pseudo-isomorphic to $\oplus_{i=2}^k \Lambda/h_i\Lambda$, so by the induction hypothesis (in the "$t = 0$" case) we can choose $\bar{x}_2, \ldots, \bar{x}_k \in B_0'$ leading to split exact sequences

$$0 \longrightarrow \sum_{i=2}^{j-1} \Lambda\bar{x}_i \longrightarrow \sum_{i=2}^{j} \Lambda\bar{x}_i \longrightarrow \Lambda/h_j\Lambda \longrightarrow 0$$

if $2 \leq j \leq k$.

Now choose x_i to be any lift of $\bar{x}_i$ to B_0. We claim the lemma is satisfied with this choice of $x_1, \ldots, x_k$. It will suffice to check that the exact sequences

$$0 \longrightarrow \Lambda x_1 \longrightarrow \sum_{i=1}^{j} \Lambda x_i \longrightarrow \sum_{i=2}^{j} \Lambda\bar{x}_i \longrightarrow 0 \tag{9}$$

split for $2 \leq j \leq k$.

Let $\mathfrak{h} = \mathrm{Ann}_\Lambda(B)$. Then $\mathfrak{h} \subset h_1\Lambda$ and $h_1^{-1}\mathfrak{h}$ is pseudo-null. By our induction hypothesis we can choose elements $\bar{y}_2, \ldots, \bar{y}_k \in \sum_{i=2}^k \Lambda\bar{x}_i$ such that $\Lambda\bar{y}_i \cong \Lambda/h_i\Lambda$ for each i and $\sum_{i=2}^k \Lambda\bar{y}_i = \sum_{i=2}^k \Lambda\bar{x}_i$. Let y_i be a lift of $\bar{y}_i$ to $\sum_{i=1}^k \Lambda x_i$.

For each i we have $h_i y_i \in \Lambda x_1$, say $h_i y_i = c_i x_1$. Then $h_i^{-1}\mathfrak{h}$ annihilates $c_i x_1$, i.e., $c_i\mathfrak{h} \subset h_i\mathfrak{h}_1$, and we conclude that h_i divides c_i. Now the map $\bar{y}_i \mapsto y_i - (c_i/h_i)x_1$ gives a splitting of (9). □

Proof of Proposition 1.4. Recall that we have a pseudo-isomorphism

$$\oplus_{i=1}^r \Lambda/f_i\Lambda \longrightarrow X_\infty.$$

Define a Λ-submodule

$$X_0 = \Lambda\mathrm{Ev}^*(\tau) + \Lambda\mathrm{Ev}^*(G_{\Omega_\infty})$$

of X_∞. Then $X_\infty \supset X_0 \supset X_0 \cap a_\tau X_\infty$, and Lemmas 3.6(iii) and 6.1 show that $(a_\tau X_\infty)/(X_0 \cap a_\tau X_\infty)$ is pseudo-null. Thus we can find a new injective pseudo-isomorphism

$$\oplus_{i=1}^r \Lambda/g_i\Lambda \longrightarrow X_0$$

where $g_i \in \Lambda$, $g_i \mid f_i$, $f_i \mid a_\tau g_i$, and $g_{i+1} \mid g_i$ for every i.

Apply Lemma 6.3 with $B = X_0$, $h_i = g_i$, $B_0 = \mathrm{Ev}^*(G_{\Omega_\infty})$, and $t = \mathrm{Ev}^*(\tau)$ to produce a sequence $x_1, \ldots, x_n \in X_0$. (Note that B_0 satisfies the hypotheses of Lemma 6.3 with $\Lambda_0 = \mathrm{Tw}_{\chi^*}(\mathbf{Z}_p[[\Gamma_0]])$, where Γ_0 and χ^* are as in Proposition 5.1, and Tw_{χ^*} is as in the proof of Proposition 5.2.) Define $z_1 = x_1 \in \mathrm{Ev}^*(\tau G_{\Omega_\infty})$, $\mathfrak{g}_1 = \mathfrak{h}_1$, and for $2 \le i \le r$ let $z_i = x_1 + x_i \in \mathrm{Ev}^*(\tau G_{\Omega_\infty})$ and $\mathfrak{g}_i = g_i\Lambda$. Then the conclusions of Proposition 1.4 follow immediately from Lemma 6.3. □

7. Proof of Proposition 1.6

In this section we will prove Proposition 1.6, and thereby complete the proof of Theorems II.3.3 and II.3.4 begun in §1. Keep the notation of §1. In particular recall that

$$Z_\infty = \sum_{i=1}^r \Lambda z_i \cong \oplus_{i=1}^r \Lambda/\mathfrak{g}_i \subset X_\infty$$

where the z_i and $\mathfrak{g}_i$ are given by Proposition 1.4.

If $\boldsymbol{\sigma}$ is a Selmer sequence of length k, as defined in Definition 1.5, define

$$Z_{\boldsymbol{\sigma}} = \sum_{i=1}^k \Lambda\mathrm{Ev}^*(\sigma_i) \subset Z_\infty.$$

Lemma 7.1. *If $\boldsymbol{\sigma}$ is a Selmer sequence of length k then $Z_{\boldsymbol{\sigma}} \cong \oplus_{i=1}^k \Lambda/\mathfrak{g}_i\Lambda$ and $Z_{\boldsymbol{\sigma}}$ is a direct summand of Z_∞. If $k < r$ and $\boldsymbol{\sigma}'$ is a Selmer sequence of length $k+1$ extending $\boldsymbol{\sigma}$, then $Z_{\boldsymbol{\sigma}'}/Z_{\boldsymbol{\sigma}} \cong \Lambda/\mathfrak{g}_{k+1}$.*

Proof. Define $Y_k = \sum_{i=1}^k \Lambda z_i$. By Proposition 1.4(iii), $Y_k \cong \oplus_{i=1}^k \Lambda/\mathfrak{g}_i$ and there is a complementary submodule $Y_k' \subset Z_\infty$ such that $Y_k \oplus Y_k' = Z_\infty$. The image of $Z_{\boldsymbol{\sigma}} + Y_k'$ in $Z_\infty/\mathcal{M}Z_\infty$ contains the image of $Y_k + Y_k' = Z_\infty$, so by Nakayama's Lemma $Z_{\boldsymbol{\sigma}} + Y_k' = Z_\infty$. We will show that $Z_{\boldsymbol{\sigma}} \cap Y_k' = 0$, and thus $Z_\infty = Z_{\boldsymbol{\sigma}} \oplus Y_k'$ and

$$Z_{\boldsymbol{\sigma}} \cong Z_\infty/Y_k' \cong Y_k \cong \oplus_{i=1}^k \Lambda/\mathfrak{g}_i\Lambda.$$

If $k < r$ and $\boldsymbol{\sigma}'$ extends $\boldsymbol{\sigma}$, we can repeat the argument above with k replaced by $k+1$. We can choose Y'_{k+1} to be contained in Y'_k, and then $Y'_k/Y'_{k+1} \cong \Lambda/\mathfrak{g}_{k+1}$ and

$$Z_{\boldsymbol{\sigma}'} \oplus Y'_{k+1} = Z_\infty = Z_{\boldsymbol{\sigma}} \oplus Y'_k,$$

so

$$Z_{\boldsymbol{\sigma}'} = Z_{\boldsymbol{\sigma}} \oplus Y'_k/Y'_{k+1} = Z_{\boldsymbol{\sigma}} \oplus \Lambda/\mathfrak{g}_{k+1}.$$

It remains to show that $Z_{\boldsymbol{\sigma}} \cap Y'_k = 0$. For $1 \le i \le k$ write

$$\mathrm{Ev}^*(\sigma_i) = z_i + v_i + w_i$$

where $v_i \in \mathcal{M}Y_k$ and $w_i \in \mathcal{M}Y'_k$. Suppose

$$\sum_{i=1}^{k} a_i \mathrm{Ev}^*(\sigma_i) \in Y'_k$$

with $a_i \in \Lambda$; we need to show that $\sum_{i=1}^k a_i \mathrm{Ev}^*(\sigma_i) = 0$. Projecting into Y_k it follows that

$$\sum_{i=1}^{k} a_i(z_i + v_i) = 0. \tag{10}$$

Using Proposition 1.4, fix generators $y_1, \dots, y_k \in Y_k$ so that for every i, $1 \le i \le k$,

$$Y_i = \sum_{j=1}^{i} \Lambda z_j = \oplus_{j=1}^{i} \Lambda y_j$$

and $\Lambda y_i \cong \Lambda/\mathfrak{g}_i$. We can rewrite (10) in matrix form, using these generators, as

$$(a_1, \dots, a_k)B \in (\mathfrak{g}_1\Lambda, \dots, \mathfrak{g}_k\Lambda)$$

where B is a $k \times k$ matrix with entries in Λ. Modulo $\mathcal{M}$, B is lower-triangular with invertible diagonal entries (since $z_i \in Y_i$, the projection of z_i generates $Y_i/Y_{i-1} = \Lambda y_i$, and the v_i vanish modulo $\mathcal{M}$). Therefore B is invertible, and, since $\mathfrak{g}_i \subset \mathfrak{g}_k$ for every $i \le k$, we conclude that $a_i \in \mathfrak{g}_k$ for every i. But $\mathfrak{g}_k$ annihilates Y'_k since $\mathfrak{g}_k \subset \mathfrak{g}_i$ for $i \ge k$, so we deduce that

$$\sum_{i=1}^{k} a_i \mathrm{Ev}^*(\sigma_i) = \sum_{i=1}^{k} a_i w_i = 0.$$

This completes the proof of the lemma. □

PROPOSITION 7.2. *For every Selmer sequence $\boldsymbol{\sigma}$, every $K \subset_{\mathrm{f}} F \subset K_\infty$, and every power M of p,* $\mathrm{Ann}_\Lambda(X_\infty/Z_\infty)$ *annihilates the kernel of the map*

$$Z_{\boldsymbol{\sigma}} \otimes \Lambda_{F,M} \longrightarrow X_\infty \otimes \Lambda_{F,M}.$$

PROOF. By Lemma 7.1, $Z_{\boldsymbol{\sigma}}$ is a direct summand of Z_∞, so $Z_{\boldsymbol{\sigma}} \otimes \Lambda_{F,M}$ injects into $Z_\infty \otimes \Lambda_{F,M}$. Clearly $\mathrm{Ann}_\Lambda(X_\infty/Z_\infty)$ annihilates the kernel of the map $Z_\infty \otimes \Lambda_{F,M} \to X_\infty \otimes \Lambda_{F,M}$, so this proves the proposition. □

For the rest of this section fix a field F, $K \subset_{\mathrm{f}} F \subset K_\infty$. By (1), $\Lambda_F/f_1\Lambda_F$ is finite. Fix a power of N_F of p such that $N_F \ge |\Lambda_F/f_1\Lambda_F|$ and N_F is at least as large as the integer M_F of Proposition 3.4(iv).

Let $\mathcal{B}_0 = (\mathcal{A}^*_{\mathrm{glob}})^\bullet(\mathcal{A}^*_{\mathcal{N}})^\bullet \mathrm{Ann}_\Lambda(X_\infty/Z_\infty)$.

COROLLARY 7.3. *If $\boldsymbol{\sigma}$ is a Selmer sequence and M is a power of p, $M \geq N_F$, then $\mathcal{B}_0$ annihilates the kernel of the natural map*

$$Z_{\boldsymbol{\sigma}} \otimes \Lambda_{F,M} \longrightarrow \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*), \mathcal{O}/M\mathcal{O}).$$

PROOF. The map in question is the composition

$$Z_{\boldsymbol{\sigma}} \otimes \Lambda_{F,M} \longrightarrow X_\infty \otimes \Lambda_{F,M} \longrightarrow \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*), \mathcal{O}/M\mathcal{O}).$$

By (1), $\mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}$ is finite for every F, so we can apply Proposition 3.4(iv), and the corollary follows from that proposition and Proposition 7.2. □

If $\mathfrak{r} \in \mathcal{R}$, recall that $\Sigma_{p\mathfrak{r}}$ denote the set of primes of K dividing $p\mathfrak{r}$.

LEMMA 7.4. *Suppose M is a power of p, $\boldsymbol{\pi}$ is a Kolyvagin sequence, and $\boldsymbol{\sigma}$ is a Selmer sequence corresponding to $\boldsymbol{\pi}$. Then the map of Corollary 7.3 factors through a surjective map*

$$Z_{\boldsymbol{\sigma}} \otimes \Lambda_{F,M} \longrightarrow \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*)/\mathcal{S}_{\Sigma_{p\mathfrak{r}(\boldsymbol{\pi})}}(F, W_M^*), \mathcal{O}/M\mathcal{O}).$$

PROOF. Write $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_k)$ and $\boldsymbol{\pi} = (\mathcal{Q}_1, \ldots, \mathcal{Q}_k)$. The image of $Z_{\boldsymbol{\sigma}}$ in $\mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*), \mathcal{O}/M\mathcal{O})$ is equal to

$$\mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*)/B, \mathcal{O}/M\mathcal{O}),$$

where

$$B = \bigcap_{\substack{1 \leq i \leq k \\ \gamma \in \mathrm{Gal}(F/K)}} \ker(\mathrm{Ev}^*_{\mathcal{S}_{\Sigma_p}(F,W_M^*)}(\sigma_i)^\gamma) = \bigcap_{\substack{1 \leq i \leq k \\ \gamma \in \mathrm{Gal}(F/K)}} \ker(\mathrm{Ev}^*_{\mathcal{S}_{\Sigma_p}(F,W_M^*)}(\mathrm{Fr}_{\mathcal{Q}_i^\gamma})).$$

Since T is unramified at each of the $\mathcal{Q}_i^\gamma$, this is equal to $\mathcal{S}_{\Sigma_{p\mathfrak{r}(\boldsymbol{\pi})}}(F, W_M^*)$. □

PROPOSITION 7.5. *Suppose $1 \leq k \leq r$, $M \geq N_F$ is a power of p, and $\boldsymbol{\pi} \in \Pi(k, F, M)$. Let $\Sigma = \Sigma_{p\mathfrak{r}(\boldsymbol{\pi})}$, $\mathfrak{q} = \mathfrak{q}_k$. Then*

$$a_\tau \mathcal{B}_0 \widetilde{\mathrm{Ev}}_{\mathfrak{q}}(\mathcal{S}^\Sigma(F, W_M)) \subset \mathfrak{g}_k \Lambda_{F,M}.$$

PROOF. Fix M, k, and $\boldsymbol{\pi}$ as in the statement of the proposition. Let $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_k)$ be a Selmer sequence corresponding to $\boldsymbol{\pi}$ and let $\boldsymbol{\sigma}' = (\sigma_1, \ldots, \sigma_{k-1})$, $\Sigma' = \Sigma - \{\mathfrak{q}\}$.

Consider the commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] \\
 & Z_{\boldsymbol{\sigma}'} \otimes \Lambda_{F,M} \arrow[r] \arrow[d] & \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*)/\mathcal{S}_{\Sigma'}(F, W_M^*), \mathcal{O}/M\mathcal{O}) \arrow[d] \\
 & Z_{\boldsymbol{\sigma}} \otimes \Lambda_{F,M} \arrow[r] \arrow[d] & \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W_M^*), \mathcal{O}/M\mathcal{O}) \arrow[d] \\
 & (Z_{\boldsymbol{\sigma}}/Z_{\boldsymbol{\sigma}'}) \otimes \Lambda_{F,M} \arrow[r, "j"] \arrow[d] & \mathrm{Hom}(\mathcal{S}_{\Sigma'}(F, W_M^*), \mathcal{O}/M\mathcal{O}) \arrow[d] \\
 & 0 & 0.
\end{tikzcd}$$

The left-hand column is exact by Lemma 7.1, and the top horizontal map is the surjection of Lemma 7.4. Applying the snake lemma, Corollary 7.3 shows that $\ker(j)$ is annihilated by $\mathcal{B}_0$. The image of j is generated by $\mathrm{Ev}^*_{\mathcal{S}_{\Sigma'}(F,W_M^*)}(\sigma_k) = \mathrm{Ev}^*_{\mathcal{S}_{\Sigma'}(F,W_M^*)}(\mathrm{Fr}_\mathfrak{q})$, and $Z_{\boldsymbol{\sigma}}/Z_{\boldsymbol{\sigma}'} \cong \Lambda/\mathfrak{g}_k\Lambda$. Hence

$$\mathcal{B}_0\mathrm{Ann}_{\Lambda_{F,M}}(\mathrm{Ev}^*_{\mathcal{S}_{\Sigma'}(F,W_M^*)}(\mathrm{Fr}_\mathfrak{q})) \subset \mathfrak{g}_k\Lambda_{F,M}.$$

By Proposition 2.7, $a_\tau\widetilde{\mathrm{Ev}}_\mathfrak{q}(\mathcal{S}^\Sigma(F,W_M))$ annihilates $\mathrm{Ev}^*_{\mathcal{S}_{\Sigma'}(F,W_M^*)}(\mathrm{Fr}_\mathfrak{q})$. This proves the proposition. $\square$

Recall that we have fixed a field F. If M is a power of p and $\mathfrak{r} \in \mathcal{R}_{F,M}$, we will write simply $\kappa_{\mathfrak{r},M}$ for $\kappa_{F,\mathfrak{r},M}$, and $\langle\kappa_{\mathfrak{r},M}\rangle$ for the $\Lambda_{F,M}$-submodule $\Lambda_{F,M}\kappa_{\mathfrak{r},M}$ of $H^1(F,W_M)$.

COROLLARY 7.6. *With notation as in Proposition* 7.5*, suppose in addition that* $\pi \in \Pi(k,F,MN_F)$*. Let* $\mathfrak{r} = \mathfrak{r}(\pi)$*. If* $\eta \in a_\tau^2\mathcal{B}_0$ *then*

$$\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\langle\kappa_{\mathfrak{r},M}\rangle} \in f_k\mathrm{Hom}_\Lambda(\langle\kappa_{\mathfrak{r},M}\rangle, \Lambda_{F,M}).$$

PROOF. Let $M' = MN_F$. By Propositions 7.5 and 1.4(ii),

$$\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_{M'})} : \mathcal{S}^\Sigma(F,W_{M'}) \to a_\tau\mathfrak{g}_k\Lambda_{F,M'} \subset f_k\Lambda_{F,M'}.$$

We want to divide this map by f_k, at the expense of passing from M' to M.

Since $f_k \mid N_F$ in Λ_F, there is a well-defined "division by f_k" map

$$f_k\Lambda_{F,M'} \longrightarrow \Lambda_{F,M}$$

which sends $f_k g$ to $g \pmod M$ for every g. Let $\psi' : \mathcal{S}^\Sigma(F,W_{M'}) \to \Lambda_{F,M}$ be the composition of $\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_{M'})}$ with this division map.

Let $\iota_{N_F,M'}$ and $\iota_{M',M}$ be the natural maps in the exact cohomology sequence

$$H^1(F,W_{N_F}) \xrightarrow{\iota_{N_F,M'}} H^1(F,W_{M'}) \xrightarrow{\iota_{M',M}} H^1(F,W_M).$$

If we identify Λ_{F,N_F} with $M\Lambda_{F,M'}$, we have

$$\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_{N_F})} = \widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_{M'})} \circ \iota_{N_F,M'}.$$

Applying Propositions 7.5 and 1.4(ii) again we see that the image of $\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_{N_F})}$ is contained in $f_k\Lambda_{F,N_F}$, and it follows that $\psi' \circ \iota_{N_F,M'} = 0$. Therefore ψ' factors through $\iota_{M',M}$, i.e.,

$$\psi' = \psi \circ \iota_{M',M} \quad \text{where} \quad \psi \in \mathrm{Hom}_\Lambda(\iota_{M',M}(\mathcal{S}^\Sigma(F,W_{M'})), \Lambda_{F,M}).$$

Using Theorem IV.5.1, we also have a diagram

$$\begin{tikzcd}
\kappa_{\mathfrak{r},M'} \arrow[d, mapsto] & \in & \mathcal{S}^\Sigma(F,W_{M'}) \arrow[r, "\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_{M'})}"] \arrow[d, "\iota_{M',M}"'] \arrow[dr, "f_k\psi'"] & \Lambda_{F,M'} \arrow[d, two heads] \\
\kappa_{\mathfrak{r},M} & \in & \mathcal{S}^\Sigma(F,W_M) \arrow[r, "\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_M)}"'] & \Lambda_{F,M}
\end{tikzcd}$$

It follows that

$$f_k\psi(\kappa_{\mathfrak{r},M}) = f_k\psi'(\kappa_{\mathfrak{r},M'}) = \eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\mathcal{S}^\Sigma(F,W_M)}(\kappa_{\mathfrak{r},M}),$$

and so $\eta\widetilde{\mathrm{Ev}}_{\mathfrak{q},\langle\kappa_{\mathfrak{r},M}\rangle} = f_k\psi$. □

The following is a precise version of Proposition 1.6. Define

$$\mathcal{B} = a_\tau^4\mathcal{A}_0^\bullet\mathcal{B}_0\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))$$

where $\mathcal{A}_0$ is the ideal of Proposition 5.2 applied with $X' = \{x \in X_\infty : a_\tau x \in \mathcal{M}Z_\infty\}$ (so by Proposition 1.4(iv), X_∞/X' is pseudo-null) and $\mathcal{B}_0$ is as defined before Corollary 7.3.

PROPOSITION 7.7. *If $M \geq N_F$ is a power of p and $0 \leq k < r$, then*

$$\mathcal{B}\Psi(k, F, N_F M)\Lambda_{F,M} \subset f_{k+1}\Psi(k+1, F, M).$$

PROOF. Let $M' = N_F M$. Fix a Kolyvagin sequence $\boldsymbol{\pi} \in \Pi(k, F, M')$, let $\mathfrak{r} = \mathfrak{r}(\boldsymbol{\pi})$, and fix $\psi : \langle\kappa_{\mathfrak{r},M'}\rangle \to \Lambda_{F,M'}$. We need to show that

$$\mathcal{B}\psi(\kappa_{\mathfrak{r},M'})\Lambda_{F,M} \subset f_{k+1}\Psi(k+1, F, M).$$

The idea of the proof is as follows. Ideally, we would like to find $\gamma \in \tau G_{\Omega_\infty}$ such that

(a) $\mathrm{Ev}^*(\gamma) \in z_{k+1} + \mathcal{M}Z_\infty$,
(b) $\widetilde{\mathrm{Ev}}(\gamma) = \psi$ on $\langle\kappa_{\mathfrak{r},M'}\rangle$,

and choose a prime $\mathfrak{q}$ whose Frobenius on a suitable extension of F is γ. If we can do this then (a) says we can use $\mathfrak{q}$ to extend $\boldsymbol{\pi}$ to a Kolyvagin sequence of length $k+1$, (b) combined with Theorem 2.6 shows that $\psi(\kappa_{\mathfrak{r},M'}) = \widetilde{\mathrm{Ev}}_{\mathfrak{q}}(\kappa_{\mathfrak{r}\mathfrak{q},M'})$, and Corollary 7.6 shows that the map $\widetilde{\mathrm{Ev}}_{\mathfrak{q},\langle\kappa_{\mathfrak{r}\mathfrak{q},M}\rangle}$ is (almost) divisible by f_{k+1}.

Unfortunately, conditions (a) and (b) on γ may not be independent, and it may not be possible to satisfy them simultaneously. Instead, we will use Proposition 5.2 to find a finite set of elements $\{\gamma_i\}$ such that $\mathrm{Ev}^*(\gamma_i) \in \mathcal{M}Z_\infty$ and such that, instead of (b), a "small multiple" of ψ is a linear combination of the $\widetilde{\mathrm{Ev}}(\gamma_i)$.

We now return to the proof. Let $\psi_0 \in \mathrm{Hom}(\langle\kappa_{\mathfrak{r},M'}\rangle, \mathcal{O}/M'\mathcal{O})$ be the homomorphism corresponding to ψ under the isomorphism of Lemma 2.4. If

$$\eta \in \mathcal{A}_0 a_\tau^2\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})^\bullet\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))^\bullet,$$

then by Proposition 5.2 (applied with X' as defined just before the statement of this proposition) there are $\gamma_1, \ldots, \gamma_j \in G_{\Omega_\infty}$ and $c_1, \ldots, c_j \in \mathcal{O}$ such that $\mathrm{Ev}^*(\gamma_i) \in (\mathcal{M}Z_\infty)$ for every i and

$$\sum_{i=1}^{j} c_i\mathrm{Ev}_{\langle\kappa_{\mathfrak{r},M'}\rangle}(\gamma_i) = \eta\psi_0. \tag{11}$$

Fix i, $1 \leq i \leq j$ and let $\boldsymbol{\sigma}$ be a Selmer sequence corresponding to $\boldsymbol{\pi}$. Choose $\delta \in \tau G_{\Omega_\infty}$ such that $\mathrm{Ev}^*(\delta) = z_{k+1}$ (Proposition 1.4(i)), and define two Selmer sequences $\boldsymbol{\sigma}'$ and $\boldsymbol{\sigma}''$ of length $k+1$ extending $\boldsymbol{\sigma}$ by $\sigma'_{k+1} = \delta$ and $\sigma''_{k+1} = \delta\gamma_i$. (These are Selmer sequences because $\mathrm{Ev}^*(\delta) = z_{k+1}$ and $\mathrm{Ev}^*(\gamma_i) \in \mathcal{M}Z_\infty$.) Fix primes $\mathfrak{q}', \mathfrak{q}''$ of K lying below primes $\mathcal{Q}', \mathcal{Q}''$ of F such that

$$\mathrm{Fr}_{\mathcal{Q}'} = \sigma'_{k+1}, \mathrm{Fr}_{\mathcal{Q}''} = \sigma''_{k+1} \quad \text{on } L$$

where L is a finite Galois extension of F containing $F(\boldsymbol{\mu}_{M'}, W_{M'}, (\mathcal{O}_K^\times)^{1/M'})$ and such that the restriction to L of every element of the finite groups (see Lemma I.5.7) $\mathcal{S}_{\Sigma_p}(F, W_{M'}^*)$ and $\mathcal{S}^{\Sigma_{p\mathfrak{r}}}(F, W_{M'})$ is zero.

We define two Kolyvagin sequences $\boldsymbol{\pi}', \boldsymbol{\pi}'' \in \Pi(k+1, F, M')$ extending $\boldsymbol{\pi}$ by setting $\mathcal{Q}'_{k+1} = \mathcal{Q}'$ and $\mathcal{Q}''_{k+1} = \mathcal{Q}''$. By Corollary 7.6, if $\eta' \in a_\tau^2 \mathcal{B}_0$ we can choose

$$\psi' \in \mathrm{Hom}_\Lambda(\langle \kappa_{\mathfrak{r}\mathfrak{q}',M} \rangle, \Lambda_{F,M}), \quad \psi'' \in \mathrm{Hom}_\Lambda(\langle \kappa_{\mathfrak{r}\mathfrak{q}'',M} \rangle, \Lambda_{F,M})$$

so that

$$f_{k+1}\psi'(\kappa_{\mathfrak{r}\mathfrak{q}',M}) = \eta' \widetilde{\mathrm{Ev}}_{\mathfrak{q}'}(\kappa_{\mathfrak{r}\mathfrak{q}',M})$$

and

$$f_{k+1}\psi''(\kappa_{\mathfrak{r}\mathfrak{q}'',M}) = \eta' \widetilde{\mathrm{Ev}}_{\mathfrak{q}''}(\kappa_{\mathfrak{r}\mathfrak{q}'',M}).$$

Therefore, using Theorem 2.6 for the third equality,

$$\begin{aligned}
\eta'\widetilde{\mathrm{Ev}}(\gamma_i)(\kappa_{\mathfrak{r},M'}) &= \eta'\widetilde{\mathrm{Ev}}(\sigma''_{k+1})(\kappa_{\mathfrak{r},M'}) - \eta'\widetilde{\mathrm{Ev}}(\sigma'_{k+1})(\kappa_{\mathfrak{r},M'}) \\
&= \eta'\widetilde{\mathrm{Ev}}(\mathrm{Fr}_{\mathfrak{q}''})(\kappa_{\mathfrak{r},M'}) - \eta'\widetilde{\mathrm{Ev}}(\mathrm{Fr}_{\mathfrak{q}'})(\kappa_{\mathfrak{r},M'}) \\
&= \eta'\widetilde{\mathrm{Ev}}_{\mathfrak{q}''}(\kappa_{\mathfrak{r}\mathfrak{q}'',M'}) - \eta'\widetilde{\mathrm{Ev}}_{\mathfrak{q}'}(\kappa_{\mathfrak{r}\mathfrak{q}',M'}) \\
&\equiv f_{k+1}(\psi''(\kappa_{\mathfrak{r}\mathfrak{q}'',M}) - \psi'(\kappa_{\mathfrak{r}\mathfrak{q}',M})) \pmod{M} \\
&\in f_{k+1}\Psi(k+1, F, M).
\end{aligned}$$

By (11) and Lemma 2.4, $\sum_i c_i \widetilde{\mathrm{Ev}}(\gamma_i) = \widetilde{\eta\psi_0} = \eta^\bullet \psi$, so we conclude that

$$\eta^\bullet \eta' \psi(\kappa_{\mathfrak{r},M'})\Lambda_{F,M} \subset f_{k+1}\Psi(k+1, F, M).$$

As η and η' vary, the products $\eta^\bullet\eta'$ generate $\mathcal{B}$, and the Proposition is proved. □

Proof of Proposition 1.6. Observe that $\mathcal{A}_0$, $\mathcal{A}^*_{\mathrm{glob}}$, and $\mathcal{A}^*_{\mathcal{N}}$ have height at least 2 (Lemma 3.2, Proposition 5.2); $\mathrm{Ann}_\Lambda(W^{G_{K_\infty}})$ and $\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))$ are prime to $\mathrm{char}(X_\infty)$ by Lemma 6.1; $\mathrm{Ann}_\Lambda(X_\infty/Z_\infty)$ contains the product of a_τ and an ideal of height 2 (Proposition 1.4(iv)). An ideal of height at least two necessarily contains an element relatively prime to $\mathrm{char}(X_\infty)$ (since $\mathrm{char}(X_\infty) \neq 0$ by Theorem II.3.2), so the ideal $\mathcal{B}$ defined before the statement of Proposition 7.7 contains the product of a_τ^5 and an element h of Λ prime to $\mathrm{char}(X_\infty)$. Thus Proposition 1.6 follows from Proposition 7.7. □

CHAPTER VIII

Euler systems and p-adic L-functions

So far we have discussed at length how an Euler system for a p-adic representation T of G_K controls the Selmer groups $\mathcal{S}(K, W^*)$ and $\mathcal{S}(K_\infty, W^*)$. This raises several natural questions which we have not yet touched on.

- Except for the examples in Chapter III, we have not discussed at all how to produce Euler systems. Should Euler systems exist in any generality?
- If there is a nontrivial Euler system $\mathbf{c}$ for T, then there are infinitely many such (for example, we can act on $\mathbf{c}$ by elements of $\mathcal{O}[[G_K]]$). Is there a "best" Euler system?
- Conjecturally, Selmer groups should be related to L-functions and their special values. Is there an Euler system related to an L-function attached to T?

In this chapter we will sketch a picture which gives a conjectural, partial, answer to these questions, by describing a fundamental connection between Euler systems and (p-adic) L-functions. This general picture will rest on several layers of conjectures, but nonetheless there are several known examples (such as the ones in Chapter III) where the connection is proved.

The connection is made via the work of Perrin-Riou [**PR2**], [**PR4**]. Briefly, for certain p-adic representations T of $G_{\mathbf{Q}}$, and subject to some vast but plausible conjectures, Perrin-Riou shows how to view the p-adic L-functions attached to twists of T by characters of conductor m as elements in $H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_m), T)$ (or more precisely, in the tensor product of $H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_m), T)$ with the field of fractions of Λ). As we will see below in §3, these cohomology classes satisfy the distribution relation defining an Euler system for T. In other words, Perrin-Riou's conjectural elements form an Euler system, and since they arise from p-adic L-functions, Theorems II.2.10 and II.3.8 relate the Selmer groups $\mathcal{S}(\mathbf{Q}, W^*)$ and $\mathcal{S}(\mathbf{Q}_\infty, W^*)$ to L-values.

1. The setting

For this chapter we will assume

- $K = \mathbf{Q}$, i.e., T is a p-adic representation of $G_{\mathbf{Q}}$,
- the scalar ring $\mathcal{O}$ is $\mathbf{Z}_p$.

The first assumption is not too serious a restriction, as in general one could consider the induced representation $\mathrm{Ind}_{K/\mathbf{Q}} T$. The second is completely unimportant, and is made only for notational convenience.

Following Perrin Riou [**PR4**], we will also make the more serious assumption that $V = T \otimes \mathbf{Q}_p$ is the p-adic realization of a "motivic structure" in the sense of

[**FPR**] Chapter III, that T corresponds to an integral structure on this motive, and that the representation V is crystalline at p.

We let $\mathbf{D}(V)$ denote Fontaine's filtered vector space attached to V, i.e.,

$$\mathbf{D}(V) = (B_{\text{cris}} \otimes_{\mathbf{Q}_p} V)^{G_{\mathbf{Q}_p}}.$$

(By definition, the fact that V is crystalline means that $\dim_{\mathbf{Q}_p} \mathbf{D}(V) = \dim_{\mathbf{Q}_p} V$.)

Suppose F is an abelian extension of $\mathbf{Q}$, unramified at p. Then F has $[F:\mathbf{Q}]$ distinct embeddings into B_{cris} and we also define

$$\mathbf{D}_F(V) = \mathbf{D}(\oplus_{F\hookrightarrow B_{\text{cris}}} V) \cong \mathbf{D}(\mathrm{Ind}_{F/\mathbf{Q}} V)$$

where $G_{\mathbf{Q}}$ acts on $\oplus_{F\hookrightarrow B_{\text{cris}}} V$ by acting both on V and by permuting the embeddings.

Suppose E is a finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O}_E$, and $\chi : \mathrm{Gal}(F/\mathbf{Q}) \to E^\times$ is a character. Write $T \otimes \chi$ for the tensor product of T with a copy of $\mathcal{O}_E$ (i.e., a free, rank-one $\mathcal{O}_E$-module with a fixed generator) on which $\mathrm{Gal}(F/\mathbf{Q})$ acts via χ, and similarly for $V \otimes \chi$, and let

$$\epsilon_\chi = \sum_{\gamma \in \mathrm{Gal}(F/\mathbf{Q})} \chi(\gamma)\gamma^{-1} \in \mathcal{O}_E[\mathrm{Gal}(F/\mathbf{Q})].$$

LEMMA 1.1. (i) *There is a natural identification* $\mathbf{D}_F(V) \cong F \otimes_{\mathbf{Q}_p} \mathbf{D}(V)$.

(ii) *Each choice of embedding* $F \hookrightarrow B_{\text{cris}}$ *induces an isomorphism*

$$\mathbf{D}(V \otimes \chi) \cong \epsilon_{\chi^{-1}}(E \otimes_{\mathbf{Q}_p} \mathbf{D}_F(V))$$

where we let $\mathrm{Gal}(F/\mathbf{Q})$ *act on* $\mathbf{D}_F(V)$ *via its action on* F *in* (i).

PROOF. We have

$$\mathbf{D}_F(V) = (\oplus_{j:F\hookrightarrow B_{\text{cris}}} V \otimes B_{\text{cris}})^{G_{\mathbf{Q}_p}},$$

so there is a natural embedding of $F \otimes_{\mathbf{Q}_p} \mathbf{D}(V)$ into $\mathbf{D}_F(V)$

$$\alpha \otimes d \mapsto \oplus_j (j(\alpha)d).$$

Since V is crystalline and $F/\mathbf{Q}$ is unramified at p, $\mathrm{Ind}_{F/\mathbf{Q}} V$ is also crystalline, i.e.,

$$\dim_{\mathbf{Q}_p} \mathbf{D}_F(V) = [F:\mathbf{Q}] \dim_{\mathbf{Q}_p} V = \dim_{\mathbf{Q}_p}(F \otimes_{\mathbf{Q}_p} \mathbf{D}(V)).$$

This proves (i). For (ii), let $(E \otimes V \otimes B_{\text{cris}})^{\chi^{-1}}$ be the subspace of $E \otimes_{\mathbf{Q}_p} V \otimes_{\mathbf{Q}_p} B_{\text{cris}}$ on which $G_{\mathbf{Q}_p}$ (acting on V and B_{cris}, not on E) acts via χ^{-1}. An embedding $j : F \hookrightarrow B_{\text{cris}}$ induces an embedding $E \otimes F \hookrightarrow E \otimes B_{\text{cris}}$, and hence (using (i)) an isomorphism

$$\epsilon_{\chi^{-1}}(E \otimes \mathbf{D}_F(V)) = \epsilon_{\chi^{-1}}(E \otimes F) \otimes \mathbf{D}(V) \xrightarrow{\sim} (E \otimes V \otimes B_{\text{cris}})^{\chi^{-1}}.$$

But $(E \otimes V \otimes B_{\text{cris}})^{\chi^{-1}}$ is isomorphic (since we fixed a generator of our one-dimensional χ space) to $(V \otimes \chi \otimes B_{\text{cris}})^{G_{\mathbf{Q}_p}} = \mathbf{D}(V \otimes \chi)$, so this proves (ii). $\square$

Let $\mathbf{Q}_\infty = \cup \mathbf{Q}_n$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$, $\Gamma = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$, and $\Lambda = \mathbf{Z}_p[[\Gamma]]$ the Iwasawa algebra. Let $\mathbf{H}$ be the extended Iwasawa algebra defined by Perrin-Riou in [**PR2**] §1: if we identify Λ with a power series ring

$\mathbf{Z}_p[[X]]$ in the usual way, and let $\mathbf{Q}_p[[X]]_r \subset \mathbf{Q}_p[[X]]$ denote the $\mathbf{Q}_p$-vector space of power series which converge on the open unit ball in $\overline{\mathbf{Q}_p}$ with growth

$$\sup_{|X|<\rho} |f(X)| = o\big(\sup_{|X|<\rho} |\log(1+X)|^r\big)$$

as $\rho \to 1^-$, then $\mathbf{H}$ is the Λ-algebra

$$\mathbf{H} = \Lambda \otimes_{\mathbf{Z}_p[[X]]} (\varinjlim_r \mathbf{Q}_p[[X]]_r).$$

We let $\mathbf{K}$ be the field of fractions of $\mathbf{H}$.

Suppose F is an abelian extension of $\mathbf{Q}$, unramified at p. In [**PR2**] (see also [**PR4**] §1.2) Perrin-Riou constructs[1] what she calls a "logarithme élargi", a $\mathbf{Z}_p[[\mathrm{Gal}(F\mathbf{Q}_\infty/\mathbf{Q})]]$-module homomorphism

$$\bigoplus_{v|p} \varprojlim_n H^1((F\mathbf{Q}_n)_v, T) \to \mathbf{K} \otimes \mathbf{D}_F(V).$$

This is a generalization of work of Coleman [**Co**], who defined this map in the case where $T = \mathbf{Z}_p(1)$. Composing with the local restriction maps we obtain a $\mathbf{Z}_p[[\mathrm{Gal}(F\mathbf{Q}_\infty/\mathbf{Q})]]$-module homomorphism

$$\mathcal{L}_F : H^1_\infty(F,T) = \varprojlim_n H^1(F\mathbf{Q}_n, T) \to \mathbf{K} \otimes \mathbf{D}_F(V)$$

which will be crucial in what follows. If $F' \subset F$ then there is a commutative diagram

$$\begin{tikzcd} H^1_\infty(F,T) \arrow[r, "\mathcal{L}_F"] & \mathbf{K} \otimes \mathbf{D}_F(V) \\ H^1_\infty(F',T) \arrow[u, "\mathrm{res}"] \arrow[r, "\mathcal{L}_{F'}"] & \mathbf{K} \otimes \mathbf{D}_{F'}(V). \arrow[u] \end{tikzcd} \tag{1}$$

2. Perrin-Riou's p-adic L-function and related conjectures

Let $d = d(V) = \dim_{\mathbf{Q}_p} V$,

$$d_+ = d_+(V) = \dim_{\mathbf{Q}_p}(V^+) = \dim_{\mathbf{Q}_p}(V^{c=1})$$

where c is a complex conjugation in $G_\mathbf{Q}$, and

$$d_- = d_-(V) = \dim_{\mathbf{Q}_p}(V^-) = \dim_{\mathbf{Q}_p}(V^{c=-1}) = d - d_+.$$

Let $\omega : G_\mathbf{Q} \to (\mathbf{Z}_p^\times)_{\mathrm{tors}}$ be the Teichmüller character giving the action of $G_\mathbf{Q}$ on $\boldsymbol{\mu}_p$ (if p is odd) or $\boldsymbol{\mu}_4$ (if $p = 2$), and

$$\langle\varepsilon\rangle = \omega^{-1}\varepsilon_{\mathrm{cyc}} : G_\mathbf{Q} \twoheadrightarrow \Gamma \xrightarrow{\sim} \begin{cases} 1 + p\mathbf{Z}_p & \text{if } p \text{ is odd} \\ 1 + 4\mathbf{Z}_2 & \text{if } p = 2. \end{cases}$$

Fix embeddings $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ and $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p}$.

Suppose that E is a finite extension of $\mathbf{Q}_p$ and $\chi : G_\mathbf{Q} \to E^\times$ is an *even* character of finite order, unramified at p.

[1] Perrin-Riou's construction only deals with odd primes p. We will implicitly assume as part of the conjecture below that her construction can be extended to $p = 2$ to produce a map with similar properties.

CONJECTURE 2.1 (Perrin-Riou [**PR4**] §4.2). *Under the assumptions on T at the beginning of §1, if $r \in \mathbf{Z}^+$ is divisible by the conductor of χ then there is a p-adic L-function*

$$\mathbf{L}_r^{(p)}(T \otimes \chi) \in \mathbf{K} \otimes \wedge_E^{d_+} \mathbf{D}(V^* \otimes \chi^{-1}).$$

See [**PR4**] §4.2 for the properties defining this p-adic L-function (when $p > 2$). For our purposes we only say loosely that $\mathbf{L}_r^{(p)}(T \otimes \chi)$ is defined so that for characters ρ of finite order of Γ and sufficiently large positive integers k,

$$\begin{aligned}\langle \varepsilon \rangle^k \rho(\mathbf{L}_r^{(p)}(T \otimes \chi)) \\ &= (p\text{-Euler factor}) \times \frac{L_r(V \otimes \chi\omega^k\rho^{-1}, -k)}{(\text{archimedean period})} \times (p\text{-adic period}).\end{aligned}$$

Here $L_r(V \otimes \chi\omega^k\rho^{-1}, s)$ is the (conjectural) complex L-function of $V \otimes \chi\omega^k\rho^{-1}$ with Euler factors at primes dividing r removed, which has an Euler product expansion

$$\prod_{\ell \nmid r} L_\ell(V \otimes \chi\omega^k\rho^{-1}, s)^{-1}. \tag{2}$$

For primes $\ell \neq p$ where V is unramified,

$$L_\ell(V \otimes \chi\omega^k\rho^{-1}, s) = \det(1 - \mathrm{Fr}_\ell^{-1} x | V \otimes \chi\omega^k\rho^{-1})|_{x=\ell^{-s}},$$

so

$$L_\ell(V \otimes \chi\omega^k\rho^{-1}, -k) = \langle \varepsilon \rangle^k \rho\big(\det(1 - \mathrm{Fr}_\ell^{-1} x | V)|_{x=\chi^{-1}(\ell)\mathrm{Fr}_\ell}\big).$$

Hence for such ℓ, writing $P(\mathrm{Fr}_\ell^{-1}|T; x) = \det(1 - \mathrm{Fr}_\ell^{-1} x|T)$ as in Chapter II §1,

$$\mathbf{L}_{r\ell}^{(p)}(T \otimes \chi) = P(\mathrm{Fr}_\ell^{-1}|T; \chi^{-1}(\ell)\mathrm{Fr}_\ell)\mathbf{L}_r^{(p)}(T \otimes \chi). \tag{3}$$

The following statement is in the spirit of the conjectures of Perrin-Riou in [**PR4**] §4.4, but stronger. In fact it is so strong that this formulation is certain not to be true in general (see Remark 2.5 below). However, one can hope that it is "almost" true.

For $r \in \mathbf{Z}^+$ write $\Delta_r = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_r)^+/\mathbf{Q})$ and

$$\Lambda_r = \Lambda \otimes \mathbf{Z}_p[\Delta_r] = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty(\boldsymbol{\mu}_r)^+/\mathbf{Q})]].$$

For $f \in \mathbf{K}$ let f^ι denote the image of f under the involution induced by $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \mathrm{Gal}(\mathbf{Q}_\infty(\boldsymbol{\mu}_r)^+/\mathbf{Q})$.

WISHFUL THINKING 2.2. *Suppose $r \in \mathbf{Z}^+$ is prime to p. Then there is an element $\boldsymbol{\xi}_r \in \wedge^{d_-} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$ such that for every finite extension E of $\mathbf{Q}_p$ and every character $\chi : \Delta_r \to E^\times$,*

$$\epsilon_\chi^{\otimes d_-}(\mathcal{L}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_r)) = \mathbf{L}_r^{(p)}(T^* \otimes \chi)^\iota.$$

REMARK 2.3. In this statement, the exterior power is in the category of Λ_r-modules, and

$$\mathcal{L}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+} : \wedge_\Lambda^{d_-} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T) \to \mathbf{K} \otimes \wedge^{d_-}_{\mathbf{Q}_p[\Delta_r]} \mathbf{D}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(V)$$

is the map induced by $\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}$. Recalling that $\epsilon_\chi = \sum \chi(\gamma)\gamma^{-1}$, we also have a map

$$\epsilon_\chi : \mathbf{D}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(V) \to \mathbf{D}(V \otimes \chi^{-1})$$

from Lemma 1.1(ii) (our chosen embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p}$ gives an embedding $\mathbf{Q}(\boldsymbol{\mu}_r) \hookrightarrow B_{\mathrm{cris}}$) which induces

$$\epsilon_\chi^{\otimes d_-} : \mathbf{K} \otimes \wedge^{d_-}_{\mathbf{Q}_p[\Delta_r]} \mathbf{D}_F(V) \to \mathbf{K} \otimes \wedge^{d_-}_E \mathbf{D}(V \otimes \chi^{-1}).$$

Note that this makes sense even if $d_- = 0$, in which case ϵ_χ^0 is the projection from $\mathbf{K} \otimes \mathbf{Q}_p[\Delta_r]$ to $\mathbf{K} \otimes E$ induced by χ. Thus since $d_+(V^* \otimes \chi) = d_-(V)$, the equality above is an identity between two elements of $\mathbf{K} \otimes \wedge^{d_-}_E \mathbf{D}(V \otimes \chi^{-1})$.

REMARK 2.4. The statement above is a strengthening and "extrapolation" (by introducing the level r) of the conjectures of Perrin-Riou in §4.4 of [**PR4**]. We have also rephrased the conjecture in terms of $\mathbf{L}_r^{(p)}(T^* \otimes \chi)$ instead of $\mathbf{L}_r^{(p)}(T \otimes \chi^{-1})$ by using the functional equation [**PR4**] §4.3.2, because it simplifies the formulas below.

REMARK 2.5. One reason that the optimistic statement 2.2 should not be true in general is that it asserts that the p-adic L-functions should all be "integral" in a strong sense. But the L-values can have denominators, coming from $W^{G_{\mathbf{Q}_\infty(\boldsymbol{\mu}_r)^+}}$ where $W = T \otimes (\mathbf{Q}_p/\mathbf{Z}_p)$. Inspired by the theorem of Deligne and Ribet [**DR**] and Stark's conjecture [**T5**] (where this denominator has been extensively studied), and Perrin-Riou's [**PR4**] Conjecture 4.4.2 (and Lemme 1.3.3), one is led to the following slightly more modest assertion which (not knowing any counterexamples) we will optimistically call a conjecture.

CONJECTURE 2.6. *Suppose $r \in \mathbf{Z}^+$ is prime to p, $d_- = 1$, and $\alpha \in \mathbf{Z}_p[[G_{\mathbf{Q}}]]$ annihilates $W^{G_{\mathbf{Q}_\infty(\boldsymbol{\mu}_r)^+}}$.*

Then there is an element $\boldsymbol{\xi}_r = \boldsymbol{\xi}_r^{(\alpha)} \in H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$ such that for every finite extension E of $\mathbf{Q}_p$ and every character $\chi : \Delta_r \to E^\times$,

$$\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_r) = \chi(\alpha) \mathbf{L}_r^{(p)}(T^* \otimes \chi)^\iota,$$

where $\chi(\alpha)$ denotes the image of α under the composition

$$\mathbf{Z}_p[[G_{\mathbf{Q}}]] \twoheadrightarrow \Lambda_r \cong \Lambda \otimes \mathbf{Z}_p[\Delta_r] \xrightarrow{1 \otimes \chi} \Lambda \otimes E \longrightarrow \mathbf{K} \otimes E.$$

Note that if T is unramified at every prime dividing r, then

$$T^{G_{\mathbf{Q}_\infty(\boldsymbol{\mu}_r)}} = T^{G_{\mathbf{Q}_\infty}} \quad \text{and} \quad W^{G_{\mathbf{Q}_\infty(\boldsymbol{\mu}_r)}} = W^{G_{\mathbf{Q}_\infty}} \tag{4}$$

(this is essentially Lemma IV.2.5(i): $\mathrm{Gal}(\mathbf{Q}_\infty(\boldsymbol{\mu}_r)/\mathbf{Q}_\infty)$ is generated by inertia groups which act trivially on T and W).

3. Connection with Euler systems when $d_- = 1$

Suppose that T is as above, $d_- = 1$, Conjectures 2.1 and 2.6 hold, and that the weak Leopoldt conjecture (see [**PR4**] §1.3) holds for T^*. For technical reasons we also assume that $T^{G_{\mathbf{Q}_\infty}} = 0$. Let N be the product of all rational primes where T is ramified.

Fix an element $\alpha \in \mathbf{Z}_p[[G_{\mathbf{Q}}]]$ which annihilates $W^{G_{\mathbf{Q}_\infty}}$. By (4), α annihilates $W^{G_{\mathbf{Q}_\infty(\boldsymbol{\mu}_r)^+}}$ for every $r \in \mathbf{Z}^+$ prime to Np. For such r, let

$$\boldsymbol{\xi}_r = \{\xi_{n,r}\} \in H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), \quad \text{with } \xi_{n,r} \in H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+, T),$$

be an element satisfying the conclusion of Conjecture 2.6.

PROPOSITION 3.1. *With hypotheses and notation as above, suppose r is prime to Np and ℓ is a prime not dividing Nrp. Then for every n,*

$$\mathrm{Cor}_{\mathbf{Q}_n(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}_n(\boldsymbol{\mu}_r)^+}\xi_{n,r\ell} = P(\mathrm{Fr}_\ell^{-1}|T^*;\mathrm{Fr}_\ell^{-1})\xi_{n,r}.$$

where $P(\mathrm{Fr}_\ell^{-1}|T^*;x) = \det(1-\mathrm{Fr}_\ell^{-1}x|T^*) \in \mathbf{Z}_p[x]$.

PROOF. Suppose E contains $\boldsymbol{\mu}_{\varphi(r)}$ (so that all characters of Δ_r into $\overline{\mathbf{Q}_p}^\times$ take values in E) and $\chi : \Delta_r \to E^\times$ is an even character. Then by definition

$$\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}\boldsymbol{\xi}_{r\ell}) = \epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+}(\boldsymbol{\xi}_{r\ell}) = \chi(\alpha)\mathbf{L}_{r\ell}^{(p)}(T^*\otimes\chi)^\iota.$$

On the other hand,

$$\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_r) = \chi(\alpha)\mathbf{L}_r^{(p)}(T^*\otimes\chi)^\iota.$$

Equation (3) shows that, after applying the involution ι,

$$\mathbf{L}_{r\ell}^{(p)}(T^*\otimes\chi)^\iota = P(\mathrm{Fr}_\ell^{-1}|T^*;\chi^{-1}(\ell)\mathrm{Fr}_\ell^{-1})\mathbf{L}_r^{(p)}(T^*\otimes\chi)^\iota.$$

Combining these equalities shows that

$$\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}\boldsymbol{\xi}_{r\ell}) = \epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(P(\mathrm{Fr}_\ell^{-1}|T^*;\mathrm{Fr}_\ell^{-1})\boldsymbol{\xi}_r)$$

for every χ, and therefore since $\sum_\chi \epsilon_\chi = [\mathbf{Q}(\boldsymbol{\mu}_r)^+ : \mathbf{Q}] \in \mathcal{O}_E[\Delta_r]$,

$$\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}\boldsymbol{\xi}_{r\ell}) = \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(P(\mathrm{Fr}_\ell^{-1}|T^*;\mathrm{Fr}_\ell^{-1})\boldsymbol{\xi}_r).$$

It remains only to show that, under our hypotheses, $\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}$ is injective. Recall that $\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}$ is the composition

$$H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+,T) \longrightarrow \bigoplus_{v|p} \varprojlim_n H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+_v,T) \longrightarrow \mathbf{K}\otimes\mathbf{D}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(V). \tag{5}$$

The weak Leopoldt conjecture, which we have assumed, implies that ([**PR4**] (1.4.2) and Corollary B.3.5) the restriction map

$$H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+,T) \longrightarrow \bigoplus_{q|Np} \varprojlim_n \oplus_{v|q} H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+_v,T)$$

is injective. Proposition A.2.3 of [**PR4**] shows that $\varprojlim \oplus_{v|q} H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+_v,T)$ is a torsion Λ-module if $q \neq p$. Therefore the kernel of the first map of (5) is a torsion Λ-module, and the definition of the second map ([**PR4**] §1.2.5) shows that its kernel is torsion as well. But by [**PR4**] Lemme 1.3.3, the Λ-torsion submodule of $H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+,T)$ is $T^{G_{\mathbf{Q}_\infty(\mu_r)^+}}$, which is $T^{G_{\mathbf{Q}_\infty}}$ by (4), and by our hypothesis this is zero. Thus $\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}$ is injective and the proposition follows. □

COROLLARY 3.2. *With notation as above, the collection*

$$\{\xi_{n,r} \in H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+,T) : n \geq 0,\ r \text{ prime to } Np\}$$

defines an Euler system for $(T, \mathbf{Q}_\infty\mathbf{Q}^{\mathrm{ab},Np,+}, Np)$ in the sense of Definition II.1.1 *and Remark* II.1.3, *where $\mathbf{Q}^{\mathrm{ab},Np,+}$ is the maximal abelian extension of $\mathbf{Q}$ unramified outside $Np\infty$.*

PROOF. This is immediate from the definition and Proposition 3.1. □

REMARK 3.3. There is another way to think about the existence of Euler systems when $d_- = 1$, in terms complex L-functions. Namely, the Euler product (2) for $L(V^*, s)$ converges (conjecturally), and hence is nonzero, if s is a sufficiently large positive integer. This allows us to read off the value of $\mathrm{ord}_{s=-k}L(V,s)$ for large positive integers k in terms of the Γ-factors in the functional equation relating $L(V,s)$ and $L(V^*,s)$. Working this out shows that, subject to standard conjectures,

$$\mathrm{ord}_{s=0}L(V \otimes \langle\varepsilon\rangle^{-k}\rho, s) = d_-$$

for all sufficiently large positive integers k and all characters ρ of finite order of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$.

Fix one such k. The Beilinson and Bloch-Kato conjectures then predict that the leading term in the Taylor expansion of $L(V \otimes \langle\varepsilon\rangle^{-k}\rho, s)$ at 0 can be expressed in terms of, among other things, a $d_- \times d_-$ regulator. When $d_- = 1$, this predicts the existence of certain special elements, and one can hope that these elements produce an Euler system for $T \otimes \langle\varepsilon\rangle^{-k}$.

By Theorem VI.3.5, an Euler system for $T \otimes \langle\varepsilon\rangle^{-k}$ can then be twisted to produce an Euler system for T.

REMARK 3.4. In the next section we consider the example $T = \mathbf{Z}_p(1)$, which has $d = d^- = 1$. Another interesting example is when T is the symmetric square of an elliptic curve (as in Chapter III §6), so $d^- = 1$ and $d^+ = 2$.

4. Example: cyclotomic units

In this section we discuss the example $T = \mathbf{Z}_p(1)$. Most of what we do was worked out by Perrin-Riou in [**PR3**], and in fact much of it is due to Iwasawa.

We suppose for this section that $p > 2$. We will show that the Euler system of cyclotomic units discussed in Chapter III §2 arises in the way described in the previous section. Note that $d_-(\mathbf{Q}_p(1)) = d(\mathbf{Q}_p(1)) = 1$, $d_+(\mathbf{Q}_p(1)) = 0$.

For every $r \in \mathbf{Z}^+$ prime to p and $n \geq 0$, let

$$\tilde{\mathbf{c}}_{p^n r} = \mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{rp^{n+1}})/\mathbf{Q}_n(\boldsymbol{\mu}_r)^+}(\zeta_{rp^{n+1}} - 1) \in (\mathbf{Q}_n(\boldsymbol{\mu}_r)^+)^\times \subset H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+, \mathbf{Z}_p(1)),$$

the Euler system of Chapter III §2, and

$$\tilde{\mathbf{c}}_{r,\infty} = \{\tilde{\mathbf{c}}_{p^n r}\}_n \in H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, \mathbf{Z}_p(1)).$$

We will use the $\tilde{\mathbf{c}}_{r,\infty}$ to show that Conjecture 2.6 is satisfied in this case.

Let

$$u_r(X) = \zeta_r(1+X)^{r^{-1}} - 1 \quad \in (\mathbf{Z}[\boldsymbol{\mu}_r] \otimes \mathbf{Z}_p)[[X]]$$

and

$$h_r(X) = \prod_{\beta \in \boldsymbol{\mu}_{p-1} \subset \mathbf{Z}_p^\times} u_r((1+X)^\beta - 1)\bar{u}_r((1+X)^\beta - 1)$$

where $\bar{u}_r(X) = \zeta_r^{-1}(1+X)^{r^{-1}} - 1$. Then h_r is the "Coleman power series" attached to $\tilde{\mathbf{c}}_{r,\infty}$, i.e., for every $n \geq 0$

$$h_r^{\mathrm{Fr}_p^{-n-1}}(\zeta_{p^{n+1}} - 1) = \tilde{\mathbf{c}}_{p^n r}.$$

The p-adic L-functions $\mathbf{L}_r^{(p)}(\mathbf{Z}_p \otimes \chi)$ that arise below are the Kubota-Leopoldt p-adic L-functions, so their existence does not rely on any conjectures. The following proposition is essentially due to Iwasawa and Coleman; but we have translated it into the language of Perrin-Riou, following [**PR3**].

PROPOSITION 4.1. *If $r \geq 1$, E is a finite extension of $\mathbf{Q}_p$, and $\chi : \Delta_r \to E^\times$ is a character, then*

$$\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\tilde{\mathbf{c}}_{r,\infty}) = 2\mathbf{L}_r^{(p)}(\mathbf{Z}_p \otimes \chi)^\iota.$$

PROOF. Suppose first that $r > 1$. By [**PR3**] §1.8, §3.1 (or [**PR2**] §4.1.3) and [**Iw2**],

$$\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\tilde{\mathbf{c}}_{r,\infty}) \in \Lambda \otimes \mathbf{D}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathbf{Q}_p(1)) = \mathbf{Q}(\boldsymbol{\mu}_r)^+ \otimes \Lambda \otimes \mathbf{D}(\mathbf{Q}_p(1)), \tag{6}$$
$$\mathbf{L}_r^{(p)}(\mathbf{Z}_p \otimes \chi) \in \Lambda \otimes \mathbf{D}(\mathbf{Q}_p(1) \otimes \chi^{-1}) = \epsilon_\chi(\Lambda \otimes \mathbf{D}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathbf{Q}_p(1))), \tag{7}$$

the equalities from Lemma 1.1. Let e_{-1} denote the canonical generator of the one-dimensional vector space $\mathbf{D}(\mathbf{Q}_p(1))$, and define

$$\mathcal{H}_r(X) = \log h_r(X) - \frac{1}{p}\log h_r^{\mathrm{Fr}_p}((1+X)^p - 1).$$

From the definition in [**PR4**] §1.2.5 (see also [**PR3**] §1.3 and §3.1.4), we see that

$$\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\tilde{\mathbf{c}}_{r,\infty}) = \mathcal{F}_r e_{-1}$$

where $\mathcal{F}_r \in \mathbf{Q}(\boldsymbol{\mu}_r)^+ \otimes \Lambda$ is such that for every $k \geq 1$,

$$\langle\varepsilon\rangle^k(\mathcal{F}_r) = (D^k\mathcal{H}_r)(\zeta_p - 1)$$

where D is the derivation $(1+X)\frac{d}{dX}$. Thus if $\chi : \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_r)^+/\mathbf{Q}) \to E^\times$ then

$$\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\tilde{\mathbf{c}}_{r,\infty}) = \mathcal{F}_{r,\chi} e_{-1}$$

where $\mathcal{F}_{r,\chi} \in \mathbf{Q}(\boldsymbol{\mu}_r)^+ \otimes \Lambda \otimes E$ is such that for every $k \geq 1$,

$$\langle\varepsilon\rangle^k(\mathcal{F}_{r,\chi}) = \sum_{\gamma \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_r)^+/\mathbf{Q})} \chi^{-1}(\gamma)(D^k\mathcal{H}_r^\gamma)(\zeta_p - 1).$$

Therefore by Lemma D.2.2,

$$\langle\varepsilon\rangle^k(\mathcal{F}_{r,\chi}) = 2\Gamma(k)(-2\pi i)^{-k}L(\chi^{-1}\omega^k, k) \times \begin{cases} -\chi(p)p^k & \text{if } (p-1) \nmid k \\ 1 - p^{k-1}\chi(p) & \text{if } (p-1) \mid k \end{cases}$$

so by the formulas in [**PR4**] §4.2 and §4.3.3 we see that for $k \geq 1$,

$$\begin{aligned}\langle\varepsilon\rangle^k(\epsilon_\chi \mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\tilde{\mathbf{c}}_{r,\infty})) &= \langle\varepsilon\rangle^k(\mathcal{F}_{r,\chi} e_{-1}) \\ &= 2\langle\varepsilon\rangle^{-k}(\mathbf{L}_r^{(p)}(\mathbf{Z}_p \otimes \chi)) = 2\langle\varepsilon\rangle^k(\mathbf{L}_r^{(p)}(\mathbf{Z}_p \otimes \chi)^\iota)\end{aligned}$$

(the Gauss sums which appear in the formulas of [**PR4**] and [**PR3**] are not present here because we never identified $\mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_r)/\mathbf{Q})]$ with $\mathbf{Q}(\boldsymbol{\mu}_r)$ as in [**PR3**] §1.8). By (6) and (7), these equalities suffice to prove the proposition when $r > 1$. A similar computation shows that for every $\sigma \in G_{\mathbf{Q}}$,

$$\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}((\sigma - 1)\tilde{\mathbf{c}}_{1,\infty}) = 2(\sigma - 1)\mathbf{L}_1^{(p)}(\mathbf{Z}_p)^\iota. \qquad \square$$

COROLLARY 4.2. *Conjecture 2.6 holds for $\mathbf{Z}_p(1)$ and every r prime to p.*

PROOF. We have assumed that $p > 2$. Therefore $\boldsymbol{\mu}_{p^\infty}^{G_{\mathbf{Q}_\infty}} = \{1\}$, and for every $\alpha \in \mathbf{Z}_p[[G_{\mathbf{Q}}]]$, Proposition 4.1 shows that

$$\boldsymbol{\xi}_r = \frac{1}{2}\alpha\tilde{\mathbf{c}}_{r,\infty} \in H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$$

satisfies Conjecture 2.6. □

5. Connection with Euler systems when $d_- > 1$

Suppose now that T is such that d_- is greater than 1, and suppose that some version of the assertion 2.2 is true: i.e., suppose there is an integer N divisible by all primes where T is ramified, and an element $\alpha \in \mathbf{Z}_p[[G_{\mathbf{Q}}]]$ such that for every integer r prime to Np, there is an element

$$\boldsymbol{\xi}_r = \in \wedge^{d_-}_{\Lambda_r} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$$

satisfying

$$\epsilon_\chi^{\otimes d_-}\mathcal{L}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_r) = \chi(\alpha)\mathbf{L}_r^{(p)}(T^*\otimes\chi)^\iota,$$

for every character χ of Δ_r. We also suppose again that the weak Leopoldt conjecture holds for T^*. In this section we will adapt an idea from [**Ru8**] §6 to construct Euler systems (elements in $H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$) from the elements $\boldsymbol{\xi}_r \in \wedge^{d_-}_{\Lambda_r} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$.

LEMMA 5.1. *With hypotheses and notation as above, suppose r is prime to Np and ℓ is a prime not dividing Nrp. Then*

$$\mathrm{Cor}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_{r\ell}) - P(\mathrm{Fr}_\ell^{-1}|T^*;\mathrm{Fr}_\ell^{-1})(\boldsymbol{\xi}_r)$$

belongs to the Λ-torsion submodule of $\wedge^{d_-}_{\Lambda_r} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$, where $P(\mathrm{Fr}_\ell^{-1}|T^*;x) = \det(1-\mathrm{Fr}_\ell^{-1}x|T^*) \in \mathbf{Z}_p[x]$ and

$$\mathrm{Cor}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+} : \wedge^{d_-} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+, T) \to \wedge^{d_-} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$$

is the map induced by corestriction.

PROOF. Exactly as in the proof of Proposition 3.1, we deduce that

$$\mathcal{L}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}\big(\mathrm{Cor}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_{r\ell})\big) = \mathcal{L}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}\big(P(\mathrm{Fr}_\ell^{-1}|T^*;\mathrm{Fr}_\ell^{-1})(\boldsymbol{\xi}_r)\big).$$

Also as in the proof of Proposition 3.1, the kernel of $\mathcal{L}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}$ is a torsion Λ-module, and so the kernel of $\mathcal{L}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_r)^+}$ is torsion as well. □

Suppose $\varphi \in \mathrm{Hom}_{\Lambda_r}(H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), \Lambda_r)$. Then φ induces a Λ_r-module homomorphism from $\wedge^k_{\Lambda_r} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$ to $\wedge^{k-1}_{\Lambda_r} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$ for all $k \geq 1$ by the usual formula

$$c_1\wedge\cdots\wedge c_k \mapsto \sum_{i=1}^{k}(-1)^{i+1}\varphi(c_i)c_1\wedge\cdots\wedge c_{i-1}\wedge c_{i+1}\cdots\wedge c_k.$$

Iterating this construction $d_- - 1$ times gives a map

$$\begin{aligned}&\wedge^{d_- -1}_{\Lambda_r}\mathrm{Hom}_{\Lambda_r}(H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), \Lambda_r)\\ &\qquad\qquad \to \mathrm{Hom}(\wedge^{d_-}_{\Lambda_r} H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)).\end{aligned}$$

If $r \mid r'$ then there is a natural map

$$\mathbf{N}_{r'/r} : \mathrm{Hom}_{\Lambda_{r'}}(H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_{r'})^+, T), \Lambda_{r'}) \to \mathrm{Hom}_{\Lambda_r}(H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), \Lambda_r)$$

induced by restriction $H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T) \to H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_{r'})^+, T)$ and the identification $\Lambda_r \cong \Lambda_{r'}^{\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{r'})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+)}$.

Proposition 5.2. *With notation as above, suppose that* $T^{G_{\mathbf{Q}_\infty}} = 0$ *and*

$$\mathfrak{S} = \{\mathfrak{S}_r\} \in \varprojlim_r \wedge_{\Lambda_r}^{d_- -1} \mathrm{Hom}_{\Lambda_r}(H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), \Lambda_r).$$

Then $\mathfrak{S}_r(\boldsymbol{\xi}_r) \in H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$ *for every* r *prime to* N, *and if* ℓ *is a prime not dividing* Nrp *then*

$$\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathfrak{S}_{r\ell}(\boldsymbol{\xi}_{r\ell})) = P(\mathrm{Fr}_\ell^{-1}|T^*; \mathrm{Fr}_\ell^{-1})(\mathfrak{S}_r(\boldsymbol{\xi}_r)).$$

In other words, if we write $\mathfrak{S}_r(\boldsymbol{\xi}_r) = \{\xi_{n,r}\}_n$ *then the collection*

$$\{\xi_{n,r} \in H^1(\mathbf{Q}_n(\boldsymbol{\mu}_r)^+, T)\}$$

is an Euler system for T *(Definition* II.1.1 *and Remark* II.1.3*).*

Proof. The proof is identical to that of Proposition 6.2 and Corollary 6.3 of [**Ru8**]. It is immediate from the definition that $\mathfrak{S}_r(\boldsymbol{\xi}_r) \in H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$ for every r, and straightforward to check that

$$\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{r'})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathfrak{S}_{r'}(\boldsymbol{\xi}_{r'})) = \mathfrak{S}_r\big(\mathrm{Cor}^{\otimes d_-}_{\mathbf{Q}(\boldsymbol{\mu}_{r'})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\boldsymbol{\xi}_r)\big).$$

Combined with Lemma 5.1 this shows that

$$\mathrm{Cor}_{\mathbf{Q}(\boldsymbol{\mu}_{r\ell})^+/\mathbf{Q}(\boldsymbol{\mu}_r)^+}(\mathfrak{S}_{r\ell}(\boldsymbol{\xi}_{r\ell})) - P(\mathrm{Fr}_\ell^{-1}|T^*; \mathrm{Fr}_\ell^{-1})\mathfrak{S}_r(\boldsymbol{\xi}_r).$$

belongs to the Λ-torsion submodule of $H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T)$. But by [**PR4**] Lemme 1.3.3 and (4) this torsion submodule is $T^{G_{\mathbf{Q}_\infty}}$, which we have assumed to be zero. □

Remark 5.3. Of course, Proposition 5.2 is only useful if we know something about the size of $\varprojlim_r \wedge_{\Lambda_r}^{d_- -1} \mathrm{Hom}_{\Lambda_r}(H^1_\infty(\mathbf{Q}(\boldsymbol{\mu}_r)^+, T), \Lambda_r)$, and in particular that it is nonzero. See [**Ru8**] §6 for an example.

CHAPTER IX

Variants

In this chapter we discuss several alternatives and extensions to the definition of Euler systems we gave in Chapter II.

1. Rigidity

It is tempting to remove from the definition of an Euler system the requirement that the field $\mathcal{K}$ (over whose subfields the Euler system classes are defined) contains a $\mathbf{Z}_p$ extension of K. After all, the proofs of the Theorems of Chapter II §2 only use the derivative classes $\kappa_{K,\mathfrak{r},M}$ and not the $\kappa_{F,\mathfrak{r},M}$ for larger extensions F of K in K_∞. However, our proofs of the properties of the derivative classes $\kappa_{K,\mathfrak{r},M}$ very much used the fact that the Euler system class $\mathbf{c}_{K(\mathfrak{r})}$ is a "universal norms" in the extension $K_\infty(\mathfrak{r})/K(\mathfrak{r})$.

In fact, some such assumption is needed, as the following example shows. Suppose K has class number one, $\mathcal{N}$ is an ideal of K divisible by p and all primes where T is ramified, and T has the property that $P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;1) = 0$ for every $\mathfrak{q}$ not dividing $\mathcal{N}$. (For example, if T is the symmetric square of the Tate module of an elliptic curve as in Chapter III §6 then T has this property.) Suppose further that $\mathcal{K}$ is the maximal abelian extension of K unramified outside $\mathcal{N}$ (so $\mathcal{K}$ does not contain a $\mathbf{Z}_p$-extension of K) and $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$. Then in Definition II.1.1, the only equations tying $\mathbf{c}_K$ to the rest of the Euler system are of the form

$$\mathrm{Cor}_{F/K}\mathbf{c}_F = \prod_{\mathfrak{q}\in\Sigma(F/K)} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;\mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{c}_K = \prod_{\mathfrak{q}\in\Sigma(F/K)} P(\mathrm{Fr}_\mathfrak{q}^{-1}|T^*;1)\mathbf{c}_K.$$

If $F \neq K$ then the set $\Sigma(F/K)$ of primes ramifying in F/K is nonempty, so the right-hand side will always be zero. In other words $\mathbf{c}_K$ does not appear in any nontrivial Euler system relations, so *we can replace* $\mathbf{c}_K$ *by any element at all in* $H^1(K,T)$ *and we still have an Euler system!* For example, the collection defined by $\mathbf{c}_F = 0$ for $F \neq K$, with $\mathbf{c}_K$ arbitrary, is an Euler system. Since there are examples satisfying the conditions above with non-trivial Selmer groups, in this situation one cannot have a theorem like Theorem II.2.2 (or Theorem IV.5.4), in which the conclusion depends in an essential way on $\mathbf{c}_K$.

However, there are other possible ways to ensure the "rigidity" of an Euler system. In Definition II.1.1, we can replace condition (ii) by

(ii)′ at least one of the conditions (a), (b), (c) below is satisfied:

- (a) $\mathcal{K}$ contains a $\mathbf{Z}_p^d$-extension of K in which no finite prime splits completely,

(b) for every $\mathfrak{r}$, $\mathbf{c}_{K(\mathfrak{r})} \in \mathcal{S}^{\Sigma_p}(K(\mathfrak{r}), T)$; and there is a $\gamma \in G_K$ such that $\gamma = 1$ on $K(1)(\boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})$ and $\gamma - 1$ is injective on T,

(c) for every $\mathfrak{r} \in \mathcal{R}$, $\mathbf{c}_{K(\mathfrak{r})} \in \mathcal{S}^{\Sigma_p}(K(\mathfrak{r}), T)$; for every prime $\mathfrak{q}$ not dividing $\mathcal{N}$, and every power n of p, $\mathrm{Fr}_\mathfrak{q}^n - 1$ is injective on T; and the collection $\{\mathbf{c}_{K(\mathfrak{r})}\}$ satisfies the congruence of Corollary IV.8.1.

Condition (ii)$'$(a) is condition (ii) of the original definition.

Under this more general definition, Theorems II.2.2, II.2.3, and II.2.10 all hold, with conclusions exactly as stated, under the additional mild assumption that $T^{G_{K(1)}} = 0$. We indicate very briefly how to adapt the proofs in Chapters IV and V to cover this expanded definition.

The idea is that there is a power m of p, independent of M, such that one can still construct the derivative classes $\kappa_{K,\mathfrak{r},M}$, and prove the local properties of Chapter IV §5, under the assumption $\mathfrak{r} \in \mathcal{R}_{K,Mm}$ rather than $\mathfrak{r} \in \mathcal{R}_{K,M}$. This additional assumption does not interfere with the proofs of the theorems of Chapter II.

Construction of the derivative classes. Since we assumed $T^{G_{K(1)}} = 0$, Lemma IV.2.5(i) shows that $T^{G_{K(\mathfrak{r})}} = 0$ for every $\mathfrak{r}$. Thus if we replace $\mathbb{W}_M$ by $\mathbb{T} = \mathrm{Maps}(G_K, T)$ in Proposition IV.4.5 we get a short exact sequence

$$0 \longrightarrow \mathbb{T}^{G_{F(\mathfrak{r})}} \longrightarrow (\mathbb{T}/T)^{G_{F(\mathfrak{r})}} \xrightarrow{\delta_{F(\mathfrak{r})}} H^1(F(\mathfrak{r}), T) \longrightarrow 0.$$

Now as in Proposition IV.4.8, but using this exact sequence above instead of Proposition IV.4.7, we can find a map $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r})} \to (\mathbb{T}/T)^{G_{F(\mathfrak{r})}}$ lifting $\mathbf{c}$. Projecting this map to $(\mathbb{W}_M/W_M)^{G_{F(\mathfrak{r})}}$ we can proceed exactly as in Definition IV.4.10 to define $\kappa_{F,\mathfrak{r},M}$.

Analogue of Theorem IV.5.1. All we need is Corollary IV.6.5 in place of Theorem IV.5.1. Corollary IV.6.5 follows directly from Proposition IV.6.1, which is included as part of (ii)$'$(b) and (ii)$'$(c). (In the text, under assumption (ii)$'$(a), we used the $\mathbf{Z}_p^d$-extension K_∞/K and Corollary B.3.4 to prove Proposition IV.6.1.)

Analogue of Theorem IV.5.4. Theorem IV.5.4 follows directly from Lemma IV.7.3, so we must prove a form of that lemma. Suppose first that (ii)$'$(b) holds with an element $\gamma \in G_K$. Fix $\mathfrak{r}\mathfrak{q} \in \mathcal{R}$, a power M of p, and a power M' of p divisible by $MP(\gamma|T;1)$. Let $n = |\boldsymbol{\mu}_{p^\infty} \cap K|$. By definition of γ, $P(\gamma|T;1) \neq 0$. Choose a prime $\mathfrak{l}$ of K such that

(a) $\mathrm{Fr}_\mathfrak{l} = \gamma$ on $K(1)(\boldsymbol{\mu}_{nM'}, (\mathcal{O}_K^\times)^{1/(nM')}, W_{M'})$,

(b) $\mathrm{Fr}_\mathfrak{l} = 1$ on $K(\mathfrak{r}\mathfrak{q})$,

(c) $\mathrm{Fr}_\mathfrak{l} \neq 1$ on $K(\lambda^{1/(np)})$ where $\lambda\mathcal{O}_K = \mathfrak{q}^h$ with h equal to the order of $\mathfrak{q}$ in the ideal class group of K.

(Exercise: show that these conditions can be satisfied simultaneously.) One can imitate the proof of Lemma IV.7.3 by using the extensions $K(\mathfrak{l})/K$ in place of the finite extensions of K in K_∞. Condition (a) and the definition of γ ensure that $nM' \mid [K(\mathfrak{l}) : K]$. Condition (c) ensures that the decomposition group of $\mathfrak{q}$ has index dividing n in $\mathrm{Gal}(K(\mathfrak{l})/K)$, and therefore has order at least M'. The key point is that although $\mathbf{c}_{K(\mathfrak{r})}$ and $\mathbf{c}_{K(\mathfrak{r}\mathfrak{q})}$ are not "universal norms" from $K(\mathfrak{r}\mathfrak{l})$ and $K(\mathfrak{r}\mathfrak{q}\mathfrak{l})$ (as they would be in $K_\infty(\mathfrak{r})$ and $K_\infty(\mathfrak{r}\mathfrak{q})$), the Euler system distribution relation shows that $P(\mathrm{Fr}_{\mathfrak{l}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{l}}^{-1})\mathbf{c}_{K(\mathfrak{r})}$ is a norm from $K(\mathfrak{r}\mathfrak{l})$ and similarly with $\mathfrak{r}$ replaced by $\mathfrak{r}\mathfrak{q}$. Conditions (a) and (b) imply that in $\mathcal{O}[\mathrm{Gal}(K(\mathfrak{r}\mathfrak{q})/K)]$,

$$P(\mathrm{Fr}_{\mathfrak{l}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{l}}^{-1}) = P(\mathrm{Fr}_{\mathfrak{l}}^{-1}|T^*;1) \equiv P(\gamma^{-1}|T^*;1) = P(\gamma|T;1) \pmod{M}.$$

Now imitating the proof of Lemma IV.7.3 one can show that, with notation as in the statement of that lemma, if $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{K,M'}$ then

$$P(\gamma|T;1)(N_{\mathfrak{q}}\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r}\mathfrak{q})}) - P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})\gamma\hat{\mathbf{d}}(x_{F(\mathfrak{r})})) = 0 \in W_{M'}$$

This suffices to prove that $\kappa_{F,\mathfrak{r},M}$ and $\kappa_{F,\mathfrak{r}\mathfrak{q},M}$ satisfy the equality of Theorem IV.5.4.

Now suppose (ii)$'$(c) holds. In Chapter IV §8 we used Lemma IV.7.3 to prove the congruence of Corollary IV.8.1. Under the assumptions (ii)$'$(c) we can just reverse the argument to prove Lemma 7.3, and then Theorem IV.5.4.

EXAMPLE 1.1 (cyclotomic units revisited). With this expanded definition, we can redefine the cyclotomic unit Euler system of Chapter III §2.1. Namely, for every $m > 1$ prime to p define

$$\tilde{\mathbf{c}}_m = (\zeta_m - 1)(\zeta_m^{-1} - 1) \in (\mathbf{Q}(\boldsymbol{\mu}_m)^+)^\times \subset H^1(\mathbf{Q}(\boldsymbol{\mu}_m)^+, \mathbf{Z}_p(1))$$

and set $\tilde{\mathbf{c}}_1 = 1$. This collection is not an Euler system, since, for every prime $\ell \neq p$, $\tilde{\mathbf{c}}_{\mathbf{Q}(\boldsymbol{\mu}_\ell)} \notin \mathcal{S}^{\Sigma_p}(\mathbf{Q}(\boldsymbol{\mu}_\ell), \mathbf{Z}_p(1))$. However, suppose $\chi : G_{\mathbf{Q}} \to \mathcal{O}^\times$ is a nontrivial character of finite order, and its conductor f is prime to p. Then we can twist $\tilde{\mathbf{c}}$ by χ^{-1} as in Definition II.4.1, and the collection $\mathbf{c} = \tilde{\mathbf{c}}^{\chi^{-1}}$ *is* an Euler system for $(\mathbf{Z}_p(1) \otimes \chi^{-1}, \mathbf{Q}^{\mathrm{ab},p}, fp)$, where $\mathbf{Q}^{\mathrm{ab},p}$ is the maximal abelian extension of $\mathbf{Q}$ unramified outside p. Namely, although condition (ii)$'$(a) does not hold, (ii)$'$(b) (with $\gamma \in G_{\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})}, \gamma \notin \ker\chi$) and (ii)$'$(c) (see Example IV.8.2) both do hold. With this Euler system we can remove one of the hypotheses from Theorem III.2.3 and Corollary III.2.4. Namely, with notation as in Chapter III §2 (so L is the field cut out by χ), we have the following theorem.

THEOREM 1.2. *Suppose $p > 2$ and χ is a nontrivial even character of conductor prime to p. Then*

$$|A_L^\chi| = [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

SKETCH OF PROOF. If $\chi(p) \neq 1$ this is Corollary III.2.4. So we may assume that the conductor of χ is prime to p and use the Euler system constructed above. For this Euler system, $\mathbf{c}_1$ generates $\mathcal{C}_{L,\chi}$, so exactly as in the proof of Theorem III.2.3 we deduce from Theorem II.2.2 that

$$|\mathcal{S}_{\Sigma_p}(\mathbf{Q}, (\mathbf{Q}_p/\mathbf{Z}_p) \otimes \chi)| \quad \text{divides} \quad [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

However, while $\mathcal{S}(\mathbf{Q}, (\mathbf{Q}_p/\mathbf{Z}_p) \otimes \chi) = \mathrm{Hom}_{\mathcal{O}}(A_L^\chi, \mathbf{D})$ (Proposition I.6.1),

$$\mathcal{S}_{\Sigma_p}(\mathbf{Q}, (\mathbf{Q}_p/\mathbf{Z}_p) \otimes \chi) = \mathrm{Hom}(A_L^\chi/P, \mathbf{D})$$

where P is the subgroup of A_L^χ generated by the classes of primes of L above p.

To complete the proof, we observe that the derivative classes $\kappa_{K,r,M}$ attached to our Euler system all lie in $\mathcal{S}^{\Sigma_r}(\mathbf{Q}, \boldsymbol{\mu}_M \otimes \chi^{-1})$, not just in $\mathcal{S}^{\Sigma_{rp}}(\mathbf{Q}, \boldsymbol{\mu}_M \otimes \chi^{-1})$ as Theorem IV.5.1 shows in the general case. (This follows from the fact that $\mathbf{c}_{\mathbf{Q}(\boldsymbol{\mu}_r)} \in \mathcal{S}(\mathbf{Q}(\boldsymbol{\mu}_r), \mathbf{Z}_p(1) \otimes \chi^{-1})$ for every r. See for example [**Ru3**] Proposition

2.4.) Therefore we can repeat the proof of Theorem II.2.2, but using $\Sigma_0 = \emptyset$ and $\Sigma = \Sigma_r$ in Theorem I.7.3 instead of $\Sigma_0 = \{p\}$ and $\Sigma = \Sigma_{rp}$, to conclude that

$$|A_L^\chi| = |\mathcal{S}(\mathbf{Q}, (\mathbf{Q}_p/\mathbf{Z}_p) \otimes \chi)| \quad \text{divides} \quad [\mathcal{E}_L^\chi : \mathcal{C}_{L,\chi}].$$

Now the equality of the theorem follows from the analytic class number formula exactly as in Corollary III.2.4. $\square$

2. Finite primes splitting completely in K_∞/K

Definition II.1.1 of an Euler system requires a $\mathbf{Z}_p^d$-extension K_∞/K, with $K_\infty \subset \mathcal{K}$, such that no finite prime splits completely in K_∞/K.

In fact, the assumption that no prime splits completely is unnecessarily strong. We can remove this hypothesis if we assume instead that

(*) for every prime $\mathfrak{q}$ of K which splits completely in K_∞/K, and for every finite extension F of K in $\mathcal{K}$, we have $(\mathbf{c}_F)_\mathfrak{q} \in H^1_{\mathrm{ur}}(F_\mathfrak{q}, T)$.

If $\mathfrak{q}$ is a prime of K, our proofs used the fact that $\mathfrak{q}$ does not split completely in K_∞/K

(i) for every $\mathfrak{q}$, to show that $(\mathbf{c}_F)_\mathfrak{q} \in H^1_{\mathrm{ur}}(F_\mathfrak{q}, T)$ for every F (see Proposition IV.6.1 and Corollary B.3.4);

(ii) for primes $\mathfrak{q} \in \mathcal{R}$, at various places.

This condition (*) takes care of (i), and for (ii) we only need observe that the set of primes splitting completely in K_∞/K has density zero, so we can remove from $\mathcal{R}$ all ideals divisible by those primes without interfering with our Tchebotarev arguments.

3. Euler systems of finite depth

Definition 3.1. Fix a nonzero $M \in \mathcal{O}$. An *Euler system for W_M* (or an Euler system of depth M) is a collection of cohomology classes satisfying all the properties of Definition II.1.1 except that instead of $\mathbf{c}_F \in H^1(F, T)$ we require $\mathbf{c}_F \in H^1(F, W_M)$. Thus an Euler system in the sense of Definition II.1.1 can be viewed as an Euler system of infinite depth, which gives rise to an Euler system for W_M for every M.

Remark 3.2. For this definition we could replace W_M by a free $\mathcal{O}/M\mathcal{O}$-module of finite rank with an action of G_K; it is not necessary that it can be written as T/MT for some T.

The construction of the derivative classes $\kappa_{F,\mathfrak{r},M}$ in Chapter IV §4 only used the images of the classes $\mathbf{c}_{F(\mathfrak{s})}$ (for $\mathfrak{s}$ dividing $\mathfrak{r}$) in $H^1(F(\mathfrak{r}), W_M)$. Thus if $\mathbf{c}$ is an Euler system for W_M then we can define the classes $\kappa_{F,\mathfrak{r},M}$ in exactly the same way.

The proof of Theorem IV.5.4 also only used the images of the Euler system classes in $H^1(\,\cdot\,, W_M)$, so that theorem still holds for the derivative classes of an Euler system for W_M. However, the proof of Theorem IV.5.1 used the images of the Euler system classes in $H^1(\,\cdot\,, W_{M'})$ for every M', so that proof breaks down in this setting. However, as discussed in §1 above (and see Remark IV.6.4), we can still prove a weaker version of Theorem IV.5.1, and this will suffice for some applications.

For example, the proofs in Chapters IV and V will prove the following Theorem. Keep the setting and notation of Chapter II (so in particular, for simplicity, $W_M = T/MT$).

THEOREM 3.3. *Suppose $M \in \mathcal{O}$ is nonzero and $\mathbf{c}$ is an Euler system for W_M. Suppose that Hypotheses* $\mathrm{Hyp}(K,T)$ *hold, that the error terms $\mathfrak{n}_W$ and $\mathfrak{n}^*_W$ of Theorem* II.2.2 *are both zero, and that $W_M^{G_K} = 0$. Let*

$$m = \sup_{\substack{\text{primes } \mathfrak{q} \text{ of } K \\ \mathfrak{q} \nmid p}} [W^{\mathcal{I}_\mathfrak{q}} : (W^{\mathcal{I}_\mathfrak{q}})_{\mathrm{div}}].$$

and let n be the order of $m\mathbf{c}_K$ in $H^1(K, W_M)$. Then $n\mathcal{S}_{\Sigma_p}(K, W_M^*) = 0$. In particular if $m\mathbf{c}_K \neq 0$ then $\mathcal{S}_{\Sigma_p}(K, W^*)$ is finite.

REMARK 3.4. The integer m of Theorem 3.3 is finite, since $[W^{\mathcal{I}} : (W^{\mathcal{I}})_{\mathrm{div}}]$ is finite for all $\mathfrak{q}$, and equal to one if T is unramified at $\mathfrak{q}$. See the proof of Corollary IV.6.5.

One could reformulate Theorem 3.3 for a general G_K-module $\bar{W}$ which is free of finite rank over $\mathcal{O}/M\mathcal{O}$, i.e., one which does not come from a "T", but one would have to redefine the Selmer group since our definition depends on T, not just on W_M.

4. Anticyclotomic Euler systems

The "Euler system of Heegner points", one of Kolyvagin's original Euler systems, is not an Euler system under our Definition II.1.1. If one tries to make the definition fit with $K = \mathbf{Q}$, the problem is that the cohomology classes (Heegner points) are not defined over abelian extensions of $\mathbf{Q}$, but rather over abelian extensions of an imaginary quadratic field which are not abelian ("anticyclotomic") over $\mathbf{Q}$. On the other hand, if one tries to make the definition fit by taking K to be an appropriate imaginary quadratic field, then the problem is that the Heegner points are not defined over large enough abelian extensions of K, but only over those which are anticyclotomic over $\mathbf{Q}$.

We will not discuss Heegner points in any detail (see instead [**Ko2**], [**Ru2**], or [**Gro2**]), but in this section we propose an expanded definition of Euler systems that will include "anticyclotomic" Euler systems like Heegner points as examples.

Fix a number field K and a p-adic representation T of G_K as in Chapter II §1. Suppose d is a positive integer dividing $p-1$, and $\chi : G_K \to \mathbf{Z}_p^\times$ is a character of order d. Let $K' = \bar{K}^{\ker(\chi)}$ be the cyclic extension of degree d of K cut out by χ.

For every prime $\mathfrak{q}$ of K not dividing p let $K'(\mathfrak{q})_\chi$ denote the maximal p-extension of K' inside the ray class field of K' modulo $\mathfrak{q}$, *such that* $\mathrm{Gal}(K'/K)$ *acts on* $\mathrm{Gal}(K'(\mathfrak{q})_\chi/K')$ *via the character* χ. Similarly, let $K'(1)_\chi$ denote the χ-part of maximal unramified p-extension of K'.

Now suppose $\mathcal{K}'$ is an (infinite) abelian p-extension of K' and $\mathcal{N}$ is an ideal of K divisible by p, the conductor of χ, and by all primes where T is ramified, such that $\mathcal{K}'$ contains $K'(\mathfrak{q})_\chi$ for every prime $\mathfrak{q}$ of K not dividing $\mathcal{N}$.

DEFINITION 4.1. A collection of cohomology classes

$$\mathbf{c} = \{\mathbf{c}_F \in H^1(F,T) : K' \subset_{\mathrm{f}} F \subset \mathcal{K}'\}$$

is a χ-*anticyclotomic Euler system* for $(T,\mathcal{K}',\mathcal{N})$ (or simply for T) if

(i) whenever $K' \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}'$,

$$\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \Big(\prod_{\mathfrak{q}\in\Sigma(F'/F)} P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;\mathrm{Fr}_{\mathfrak{q}}^{-1})\Big)\mathbf{c}_F$$

where $\Sigma(F'/F)$ is the set of primes of K not dividing $\mathcal{N}$ which ramify in F' but not in F, $\mathrm{Fr}_{\mathfrak{q}}$ is a Frobenius of $\mathfrak{q}$ in G_K, and

$$P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;x) = \det(1-\mathrm{Fr}_{\mathfrak{q}}^{-1}x|T^*) \in \mathcal{O}[x],$$

(ii) at least one of the following analogues of the hypotheses (ii)$'$ of §1 holds:

(a) $\mathcal{K}'$ contains a $\mathbf{Z}_p^d$-extension K'_∞ of K' in which no finite prime splits completely, and such that $\mathrm{Gal}(K'/K)$ acts on $\mathrm{Gal}(K'_\infty/K')$ via χ, or

(b) for every $\mathfrak{r}$, $\mathbf{c}_{K'(\mathfrak{r})_\chi} \in \mathcal{S}^{\Sigma_p}(K'(\mathfrak{r})_\chi,T)$, and there is a $\gamma \in G_K$ such that $\varepsilon_{\mathrm{cyc}}(\gamma) = \chi(\gamma)$, γ^d is the identity on $K'(1)_\chi(\boldsymbol{\mu}_{p^\infty},(\mathcal{O}_{K'}^\times)^{1/p^\infty})$, and $\gamma-1$ is injective on T, or

(c) for every $\mathfrak{r} \in \mathcal{R}$, $\mathbf{c}_{K(\mathfrak{r})} \in \mathcal{S}^{\Sigma_p}(K(\mathfrak{r}),T)$; for every $\mathfrak{q}$ not dividing $\mathcal{N}$, and every power n of p, $\mathrm{Fr}_{\mathfrak{q}}^n - 1$ is injective on T; and the classes $\{\mathbf{c}_F\}$ satisfy the appropriate analogue of the congruence of Corollary IV.8.1.

REMARK 4.2. If $d=1$, then χ is trivial, $K'=K$, and so a χ-anticyclotomic Euler system for T is the same as an Euler system for T in the sense of Definition II.1.1 (or §1).

If $K=\mathbf{Q}$, $d=2$ and χ is an odd quadratic character, then K' is an imaginary quadratic field and $\mathcal{K}'$ is an anticyclotomic p-extension of K'. If T is the Tate module of a modular elliptic curve, and we make the additional assumption that $\chi(q)=1$ for every q dividing the conductor of χ, then the Heegner points in anticyclotomic extensions of K' give a χ-anticyclotomic Euler system for T. (One must modify the Heegner points slightly, as in §6 below, to get the correct distribution relation.) Note that in this situation we can take $\mathcal{K}'$ to contain the anticyclotomic $\mathbf{Z}_p$-extension K'_∞ of K', but all rational primes which are inert in K' split completely in K'_∞/K' so condition (ii)(a) of the definition fails. However, both (ii)(b) and (ii)(c) hold.

Given a χ-anticyclotomic Euler system and a power M of p, one can proceed exactly as in Chapter IV §4 to define derivative classes

$$\kappa_{K',\mathfrak{r},M} \in H^1(K',W_M)$$

for every $\mathfrak{r} \in \mathcal{R}_{K',M}$, where $\mathcal{R}_{K',M}$ is the set of squarefree ideals of K divisible only by primes $\mathfrak{q}$ such that $\mathfrak{q} \nmid \mathcal{N}$, $M \mid [K'(\mathfrak{q})_\chi : K'(1)_\chi]$, and $M \mid P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*;1)$. These classes satisfy analogues of Theorems IV.5.1 and IV.5.4, and can be used along with global duality (Theorem I.7.3) to bound the appropriate Selmer group.

For example, one can prove the following theorem. Let

$$\Omega' = K'(1)_\chi(\boldsymbol{\mu}_{p^\infty},(\mathcal{O}_{K'}^\times)^{1/p^\infty},W),$$

and for every i let

$$\mathrm{ind}_{\mathcal{O}}(\mathbf{c},\chi^i) = \sup\{n : \mathbf{c}_{K'}^{\chi^i} \in \mathfrak{p}^n H^1(K',T) + H^1(K',T)_{\mathrm{tors}}\} \le \infty,$$

where $\mathbf{c}_{K'}^{\chi^i}$ denotes the projection of $\mathbf{c}_{K'}$ into the subgroup $H^1(K',T)^{\chi^i}$ of $H^1(K',T)$ on which $\mathrm{Gal}(K'/K)$ acts via χ^i.

THEOREM 4.3. *Suppose* $\mathbf{c}$ *is a* χ*-anticyclotomic Euler system for* T*. Suppose further that* $H^1(\Omega'/K',W) = H^1(\Omega'/K',W^*) = 0$*,* $T \otimes \Bbbk$ *is an irreducible* $\Bbbk[G_{K'}]$*-module, and there is a* $\tau \in G_K$ *such that*

- $\varepsilon_{\mathrm{cyc}}(\tau) = \chi(\tau)$,
- τ^d *is the identity on* $K'(1)_\chi(\boldsymbol{\mu}_{p^\infty},(\mathcal{O}_{K'}^\times)^{1/p^\infty})$*, and*
- $T/(\tau-1)T$ *is free of rank one over* $\mathcal{O}$*.*

Then for every i*,*

$$\mathfrak{p}^{\mathrm{ind}_{\mathcal{O}}(\mathbf{c},\chi^i)}\mathcal{S}_{\Sigma_p}(K',W^*)^{\chi^{1-i}} = 0.$$

REMARK 4.4. The main difference between the case of trivial χ (i.e., Theorem II.2.2) and nontrivial χ is reflected in the way the powers of χ appear in the statement of Theorem 4.3. This is caused by the analogue of Theorem IV.5.4, which states that for $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{K',M}$, $\mathrm{loc}_{\mathfrak{q}}^s(\kappa_{K',\mathfrak{r}\mathfrak{q},M}) = \phi_{\mathfrak{q}}^{fs}(\kappa_{K',\mathfrak{r},M})$ where

$$\phi_{\mathfrak{q}}^{fs} : H^1_f(K'_{\mathfrak{q}},W_M) \longrightarrow H^1_s(K'_{\mathfrak{q}},W_M).$$

As usual we write $H^1_f(K'_{\mathfrak{q}},W_M) = \oplus_{v|\mathfrak{q}} H^1_f(K'_v,W_M)$ and similarly for $H^1_s(K'_{\mathfrak{q}},W_M)$, so that both are $\mathrm{Gal}(K'/K)$-modules. But $\phi_{\mathfrak{q}}^{fs}$ is not $\mathrm{Gal}(K'/K)$-equivariant; for $\mathfrak{q} \in \mathcal{R}_{K',M}$, one can show that

$$\phi_{\mathfrak{q}}^{fs}(H^1_f(K'_{\mathfrak{q}},W_M)^{\chi^i}) \subset H^1_s(K'_{\mathfrak{q}},W_M)^{\chi^{i-1}}.$$

Thus, taking $\mathfrak{r} = 1$ and letting $\mathfrak{q}$ vary, we obtain many classes in $H^1(K',W_M)^{\chi^{i-1}}$, ramified at only one prime of K not dividing p, whose ramification is expressed in terms of $\mathbf{c}_{K'}^{\chi^i}$, and these classes can be used to annihilate classes in $\mathcal{S}_{\Sigma_p}(K',W^*)^{\chi^{1-i}}$. This is how Theorem 4.3 is proved.

To prove an analogue of Theorem II.2.2 and bound the order of the various components of $\mathcal{S}_{\Sigma_p}(K',W^*)$, we would need to proceed by induction as in Chapter V. Unfortunately this is not at all straightforward, because at each step of the induction we move to a different component. We will not attempt to formulate, much less prove, such a statement here.

In the case of the Euler system of Heegner points, the induction succeeds using the fact that $T^* \cong T$. When $d > 2$ there is no obvious property to take the place of this self-duality. Also, when $d = 2$, χ takes values ± 1, so if L is any abelian extension of K' it makes sense to ask if $\mathrm{Gal}(K'/K)$ acts on $\mathrm{Gal}(L/K')$ via χ. When $d > 2$, this only makes sense when L/K' is a p-extension. This is sufficient to discuss and work with Euler systems, but it raises the question of whether one should expect χ-anticyclotomic Euler systems with $d > 2$ to exist.

5. Adding additional local conditions

Inspired by work on Stark's conjectures (see for example [**Gro1**] or [**Ru6**]) it may be useful to impose local conditions on Euler system cohomology classes.

Suppose Σ and Σ' are disjoint finite sets of places of K. If A is T, W, W_M, T^*, W or W_M^*, define

$$\mathcal{S}_{\Sigma'}^{\Sigma}(K,A) = \ker\left(\mathcal{S}^{\Sigma}(K,A) \to \oplus_{v\in\Sigma'} H^1(K_v,A)\right)$$

and similarly with K replaced by a finite extension. For example, $\mathcal{S}_{\Sigma'}^{\Sigma}(K,T)$ consists of all classes $c \in H^1(K,T)$ satisfying the local conditions

- $c_v \in H^1_f(K_v,W)$ if $v \notin \Sigma \cup \Sigma'$,
- $c_v = 0$ if $v \in \Sigma'$,
- no restriction for $v \in \Sigma$.

Definition 5.1. Suppose $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$, and Σ is a finite set of primes of K not dividing p. We say $\mathbf{c}$ is *trivial at* Σ if $\mathbf{c}_F \in \mathcal{S}_{\Sigma}^{\Sigma_p}(F,T)$ for every F.

If an Euler system is trivial at Σ, we can use it to bound the Selmer group $\mathcal{S}_{\Sigma_p}^{\Sigma}(K,W^*)$. The proof will be the same as the original case where Σ is empty, once we have the following strengthening of Theorem IV.5.1.

Theorem 5.2. *Let Σ be a finite set of primes of K not dividing p. If $\mathbf{c}$ is an Euler system for T, trivial at Σ, then the derivative classes $\kappa_{F,\mathfrak{r},M}$ constructed in Chapter* IV §4 *satisfy*

$$\kappa_{F,\mathfrak{r},M} \in \mathcal{S}_{\Sigma}^{\Sigma_{p\mathfrak{r}}}(F,W_M).$$

Proof. By Theorem IV.5.1, we only need to show that $(\kappa_{F,\mathfrak{r},M})_{\mathfrak{q}} = 0$ if $\mathfrak{q} \in \Sigma$. The proof is similar to that of Theorem IV.5.1 in Chapter IV §6. We use the notation of that proof.

Fix a lift $\mathbf{d} : \mathbf{X}_{F(\mathfrak{r})} \to \mathbb{W}_M/W_M$ of $\mathbf{c}$ as in Proposition IV.4.8 and write $\mathbf{d}_{\mathfrak{q}}$ for the image of $\mathbf{d}$ in $\mathrm{Hom}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M/\mathrm{Ind}_{\mathcal{D}}^{G_K}(W_M))$ in the diagram of Lemma IV.6.7. Then $\mathbf{d}_{\mathfrak{q}}$ is a lift of $\mathbf{c}$ in the sense of Proposition IV.6.8, but so is the zero map, since $(\mathbf{c}_{F(\mathfrak{r})})_{\mathfrak{q}} = 0$. Therefore the uniqueness portion of Proposition IV.6.8 shows that

$$\mathbf{d}_{\mathfrak{q}} \in \mathrm{image}(\mathrm{Hom}(\mathbf{X}_{F(\mathfrak{r})}, \mathbb{W}_M^{G_{F(\mathfrak{r})}}))$$

and from this it follows without difficulty, as in the proof of Theorem IV.5.1, that $(\kappa_{F,\mathfrak{r},M})_{\mathfrak{q}} = 0$. $\square$

The following analogue of Theorem II.2.2 (using the same notation) is an example of the kind of bound that comes from using an Euler system which is trivial at Σ.

Theorem 5.3. *Suppose that $p > 2$ and that T satisfies* $\mathrm{Hyp}(K,T)$. *Let Σ be a finite set of primes of K not dividing p. If $\mathbf{c}$ is an Euler system for T, trivial at Σ, then*

$$\ell_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}^{\Sigma}(K,W^*)) \le \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + \mathfrak{n}_W + \mathfrak{n}_W^*$$

where

$$\mathfrak{n}_W = \ell_{\mathcal{O}}(H^1(\Omega/K, W) \cap \mathcal{S}_{\Sigma}^{\Sigma_p}(K, W))$$
$$\mathfrak{n}_W^* = \ell_{\mathcal{O}}(H^1(\Omega/K, W^*) \cap \mathcal{S}_{\Sigma_p}(K, W^*))$$

PROOF. The proof is identical to that of Theorem II.2.2, using Theorem 5.2 instead of Theorem IV.5.1. □

REMARKS 5.4. There are similar analogues of the other theorems of Chapter II, bounding $\mathcal{S}_{\Sigma_p}^{\Sigma}(K, W^*)$ and $\mathcal{S}_{\Sigma_p}^{\Sigma}(K_\infty, W^*)$.

By taking Σ to be large, we can ensure that the error term $\mathfrak{n}_W$ in Theorem 5.3 is small.

In the spirit of Chapter VIII, if we think of Euler systems as corresponding to p-adic L-functions, then an Euler system which is trivial at Σ corresponds to a p-adic L-function with modified Euler factors at primes in Σ. As in [**Gro1**] §1 (where our Σ is denoted T), these Euler factors can be used to remove denominators from the original p-adic L-function (see Remark VIII.2.5 and Conjecture VIII.2.6).

6. Varying the Euler factors

It may happen that one has a collection of cohomology classes satisfying distribution relations different from the ones in Definition 1.1. Under certain conditions one can modify the given classes to obtain an Euler system.

Return again to the setting of Chapter II §1: fix a number field K and a p-adic representation T of G_K. Suppose $\mathcal{K}$ is an abelian extension of K and $\mathcal{N}$ is an ideal of K divisible by p and all primes where T is ramified. If $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$, let $\Sigma(F'/F)$ denote the set of primes of K not dividing $\mathcal{N}$ which ramify in F'/K but not in F/K.

LEMMA 6.1. *Suppose* $\{f_{\mathfrak{q}} \in \mathcal{O}[x] : \mathfrak{q} \nmid \mathcal{N}\}$ *and* $\{g_{\mathfrak{q}} \in \mathcal{O}[x] : \mathfrak{q} \nmid \mathcal{N}\}$ *are two collections of polynomials such that* $f_{\mathfrak{q}}(x) \equiv g_{\mathfrak{q}}(x) \pmod{\mathbf{N}(\mathfrak{q}) - 1}$ *for every* $\mathfrak{q}$*, and* $\{\tilde{\mathbf{c}}_F \in H^1(F, T) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$ *is a collection of cohomology classes such that if* $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$*, then*

$$\mathrm{Cor}_{F'/F}(\tilde{\mathbf{c}}_{F'}) = \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F)} f_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})\Big)\tilde{\mathbf{c}}_F.$$

Then there is a collection of classes $\{\mathbf{c}_F \in H^1(F, T) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$ *such that*

(i) *for all* F *and* F' *as above,*

$$\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F)} g_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})\Big)\mathbf{c}_F,$$

(ii) *for every finite abelian extension* F *of* K *unramified outside* $\mathcal{N}$*,*

$$\mathbf{c}_F = \tilde{\mathbf{c}}_F,$$

(iii) *if* F *is a finite abelian extension of* K*,* χ *is a character of* $\mathrm{Gal}(F/K)$ *of conductor* $\mathfrak{f}$*, and every prime which ramifies in* F/K *divides* $\mathcal{N}\mathfrak{f}$*, then*

$$\sum_{\gamma \in \mathrm{Gal}(F/K)} \chi(\gamma)\gamma\mathbf{c}_F = \sum_{\gamma \in \mathrm{Gal}(F/K)} \chi(\gamma)\gamma\tilde{\mathbf{c}}_F.$$

Proof. If $K \subset_{\mathrm{f}} F \subset \mathcal{K}$ let $\Sigma(F) = \Sigma(F/K)$, and if S is a finite set of primes of K let F_S be the largest extension of K in F which is unramified outside S and $\mathcal{N}$. If $\mathfrak{q} \nmid \mathcal{N}$ let $d_\mathfrak{q} = g_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) - f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1})$. For every F define

$$\mathbf{c}_F = \sum_{S \subset \Sigma(F)} \frac{\prod_{\mathfrak{q} \in \Sigma(F)-S} d_\mathfrak{q}}{[F : F_S]} \Big(\prod_{\mathfrak{q} \in S - \Sigma(F_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big) \tilde{\mathbf{c}}_{F_S}.$$

(Let $\mathcal{I}_\mathfrak{q}(F/K)$ denote the inertia group of $\mathfrak{q}$ in $\mathrm{Gal}(F/K)$. Then $\mathrm{Gal}(F/F_S)$ is generated by $\{\mathcal{I}_\mathfrak{q} : \mathfrak{q} \in \Sigma(F) - S\}$, and $|\mathcal{I}_\mathfrak{q}|$ divides $(\mathbf{N}(\mathfrak{q}) - 1)$ in $\mathcal{O}$, so $[F : F_S]$ divides $\prod_{\mathfrak{q} \in \Sigma(F)-S} (\mathbf{N}(\mathfrak{q}) - 1)$. Since $d_\mathfrak{q} \in (\mathbf{N}(\mathfrak{q}) - 1)\mathcal{O}[\mathrm{Gal}(F/K)]$, the fractions above belong to $\mathcal{O}[\mathrm{Gal}(F/K)]$.)

With this definition, (ii) is clear. Assertion (iii) (of which (ii) is a special case) also holds, because if S is a proper subset of $\Sigma(F)$ then our assumption on the conductor of χ implies that $\sum_{\gamma \in \mathrm{Gal}(F/K)} \chi(\gamma)\gamma \tilde{\mathbf{c}}_{F_S} = 0$.

For (i), observe that for every S, $F'_S \cap F = F_S$. Thus, using the diagram

$$\begin{tikzcd}[column sep=small]
 & F' \arrow[d, dash] & \\
 & F'_S F \arrow[dl, dash] \arrow[dr, dash] & \\
F'_S \arrow[dr, dash] & & F \arrow[dl, dash] \\
 & F_S &
\end{tikzcd}$$

we see that

$$\begin{aligned}
\mathrm{Cor}_{F'/F}(\tilde{\mathbf{c}}_{F'_S}) &= \mathrm{Cor}_{F'_S F/F} \mathrm{Cor}_{F'/F'_S F}(\tilde{\mathbf{c}}_{F'_S}) = [F' : F'_S F] \mathrm{Cor}_{F'_S F/F}(\tilde{\mathbf{c}}_{F'_S}) \\
&= \frac{[F' : F]}{[F'_S : F_S]} \mathrm{Cor}_{F'_S/F_S}(\tilde{\mathbf{c}}_{F'_S}) = \frac{[F' : F]}{[F'_S : F_S]} \Big(\prod_{\mathfrak{q} \in \Sigma(F'_S/F_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big) \tilde{\mathbf{c}}_{F_S},
\end{aligned}$$

and so $\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \sum_{S \subset \Sigma(F')} a_S \tilde{\mathbf{c}}_{F_S}$ where

$$\begin{aligned}
a_S &= \frac{\prod_{\mathfrak{q} \in \Sigma(F')-S} d_\mathfrak{q}}{[F' : F'_S]} \Big(\prod_{\mathfrak{q} \in S - \Sigma(F'_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big) \frac{[F' : F]}{[F'_S : F_S]} \Big(\prod_{\mathfrak{q} \in \Sigma(F'_S/F_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big) \\
&= \frac{\prod_{\mathfrak{q} \in \Sigma(F')-S} d_\mathfrak{q}}{[F : F_S]} \Big(\prod_{\mathfrak{q} \in S - \Sigma(F_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big).
\end{aligned}$$

Since $F_S = F_{S \cap \Sigma(F)}$, we can group together those sets S which have the same intersection with $\Sigma(F)$, and we get a new expression $\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \sum_{S \subset \Sigma(F)} b_S \tilde{\mathbf{c}}_{F_S}$ where

$$\begin{aligned}
b_S &= \sum_{S' \subset \Sigma(F'/F)} \frac{\prod_{\mathfrak{q} \in \Sigma(F')-S-S'} d_\mathfrak{q}}{[F : F_S]} \Big(\prod_{\mathfrak{q} \in S \cup S' - \Sigma(F_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big) \\
&= \frac{\prod_{\mathfrak{q} \in \Sigma(F)-S} d_\mathfrak{q}}{[F : F_S]} \Big(\prod_{\mathfrak{q} \in S - \Sigma(F_S)} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big) \\
&\qquad \times \sum_{S' \subset \Sigma(F'/F)} \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F)-S'} d_\mathfrak{q} \Big) \Big(\prod_{\mathfrak{q} \in S'} f_\mathfrak{q}(\mathrm{Fr}_\mathfrak{q}^{-1}) \Big).
\end{aligned}$$

Since

$$\sum_{S' \subset \Sigma(F'/F)} \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F) - S'} d_{\mathfrak{q}} \Big) \Big(\prod_{\mathfrak{q} \in S'} f_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) \Big) = \prod_{\mathfrak{q} \in \Sigma(F'/F)} (d_{\mathfrak{q}} + f_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1})) = \prod_{\mathfrak{q} \in \Sigma(F'/F)} g_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}),$$

we conclude that $\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \prod_{\mathfrak{q} \in \Sigma(F'/F)} g_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) \mathbf{c}_F$ as desired. □

Example 6.2. Suppose $K = \mathbf{Q}$, $f_q(x) = 1 - x$ and $g_q(x) = 1 - q^{-1}x$. Then $f_q(x) \equiv g_q(x) \pmod{(q-1)\mathbf{Z}_p}$ for every $q \neq p$. By applying Lemma 6.1 with these data to the collection $\{\tilde{\mathbf{c}}'_F \in H^1(F, \mathbf{Z}_p)\}$ constructed in Chapter III §4.1, we obtain an Euler system for $\mathbf{Z}_p(1)$.

Lemma 6.3. *Suppose* $\{f_{\mathfrak{q}}(x) \in \mathcal{O}[x, x^{-1}] : \mathfrak{q} \nmid \mathcal{N}\}$ *is a collection of polynomials,* $\{u_{\mathfrak{q}} \in \mathcal{O}^\times : \mathfrak{q} \nmid \mathcal{N}\}$ *a collection of units,* $d \in \mathbf{Z}$*, and* $\{\tilde{\mathbf{c}}_F \in H^1(F, T) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$ *is a collection of cohomology classes such that if* $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$ *then*

$$\mathrm{Cor}_{F'/F}(\tilde{\mathbf{c}}_{F'}) = \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F)} f_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}) \Big) \tilde{\mathbf{c}}_F.$$

For each $\mathfrak{q}$ *define*

$$g_{\mathfrak{q}}(x) = u_{\mathfrak{q}} x^d f_{\mathfrak{q}}(x^{-1}) \in \mathcal{O}[x, x^{-1}].$$

Then there is a collection of classes

$$\{\mathbf{c}_F \in H^1(F, T) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$$

such that

(i) *for all* F *and* F' *as above,*

$$\mathrm{Cor}_{F'/F}(\mathbf{c}_{F'}) = \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F)} g_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}}^{-1}) \Big) \mathbf{c}_F,$$

(ii) *for every finite extension* F *of* K *unramified outside* $\mathcal{N}$*,*

$$\mathbf{c}_F = \tilde{\mathbf{c}}_F.$$

Proof. For every F define

$$\mathbf{c}_F = \Big(\prod_{\mathfrak{q} \in \Sigma(F/K)} u_{\mathfrak{q}} \mathrm{Fr}_{\mathfrak{q}}^{-d} \Big) \tilde{\mathbf{c}}_F$$

where we fix some Frobenius $\mathrm{Fr}_{\mathfrak{q}} \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ (previously we always had $\mathrm{Fr}_{\mathfrak{q}}$ acting through an extension unramified at $\mathfrak{q}$). Then it is easy to check that this collection has the desired properties. □

Let $P(\mathrm{Fr}_{\mathfrak{q}}^{-1} | T; x) = \det(1 - \mathrm{Fr}_{\mathfrak{q}}^{-1} x | T)$.

Corollary 6.4. *Suppose* $\{\tilde{\mathbf{c}}_F \in H^1(F, T) : K \subset_{\mathrm{f}} F \subset \mathcal{K}\}$ *is a collection of cohomology classes such that if* $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset \mathcal{K}$*, then*

$$\mathrm{Cor}_{F'/F}(\tilde{\mathbf{c}}_{F'}) = \Big(\prod_{\mathfrak{q} \in \Sigma(F'/F)} P(\mathrm{Fr}_{\mathfrak{q}}^{-1} | T; \mathrm{Fr}_{\mathfrak{q}}) \Big) \tilde{\mathbf{c}}_F.$$

Then there is an Euler system $\{\mathbf{c}_F\}$ for $(T, \mathcal{K}, \mathcal{N})$ such that for every finite extension F of K unramified outside $\mathcal{N}$,

$$\mathbf{c}_F = \tilde{\mathbf{c}}_F.$$

PROOF. This will follow directly from the previous two lemmas. For every $\mathfrak{q}$ we have

$$\begin{aligned} P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T; x^{-1}) &= \det(1 - \mathrm{Fr}_{\mathfrak{q}}^{-1}x^{-1}|T) = \det(1 - \mathbf{N}(\mathfrak{q})^{-1}\mathrm{Fr}_{\mathfrak{q}}x^{-1}|T^*) \\ &= (-\mathbf{N}(\mathfrak{q}))^{-d}\det(\mathrm{Fr}_{\mathfrak{q}}|T^*)x^{-d}\det(1 - \mathbf{N}(\mathfrak{q})\mathrm{Fr}_{\mathfrak{q}}^{-1}x|T^*) \end{aligned}$$

where $d = \mathrm{rank}_{\mathcal{O}}T$. Thus if we first apply Lemma 6.3 with

$$f_{\mathfrak{q}} = P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T; x), \qquad u_{\mathfrak{q}} = (-\mathbf{N}(\mathfrak{q}))^{d}\det(\mathrm{Fr}_{\mathfrak{q}}|T^*)^{-1},$$

and then apply Lemma 6.1 with

$$f_{\mathfrak{q}} = P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*; \mathbf{N}(\mathfrak{q})x), \qquad g_{\mathfrak{q}} = P(\mathrm{Fr}_{\mathfrak{q}}^{-1}|T^*; x),$$

we obtain the desired Euler system. $\square$

APPENDIX A

Linear algebra

Suppose for this appendix that $\mathcal{O}$ is a discrete valuation ring. Let $\ell_{\mathcal{O}}(B)$ denote the length of an $\mathcal{O}$-module B.

1. Herbrand quotients

Suppose $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{O}[x]$.

DEFINITION 1.1. If S is an $\mathcal{O}[x]$-module and $\boldsymbol{\alpha\beta} S = 0$, then

$$\boldsymbol{\alpha} S \subset S^{\boldsymbol{\beta}=0}, \qquad \boldsymbol{\beta} S \subset S^{\boldsymbol{\alpha}=0},$$

and we define the (additive) Herbrand quotient

$$h(S) = \ell_{\mathcal{O}}(S^{\boldsymbol{\beta}=0}/\boldsymbol{\alpha} S) - \ell_{\mathcal{O}}(S^{\boldsymbol{\alpha}=0}/\boldsymbol{\beta} S)$$

if both lengths are finite.

EXAMPLE 1.2. If $S = \mathcal{O}[x]/\boldsymbol{\alpha\beta}\mathcal{O}[x]$ then $S^{\boldsymbol{\beta}=0} = \boldsymbol{\alpha} S = \boldsymbol{\alpha}\mathcal{O}[x]/\boldsymbol{\alpha\beta}\mathcal{O}[x]$ and $S^{\boldsymbol{\alpha}=0} = \boldsymbol{\beta} S = \boldsymbol{\beta}\mathcal{O}[x]/\boldsymbol{\alpha\beta}\mathcal{O}[x]$, so $h(S) = 0$.

PROPOSITION 1.3. (i) *If S is an $\mathcal{O}[x]/\boldsymbol{\alpha\beta}\mathcal{O}[x]$-module and $\ell_{\mathcal{O}}(S)$ is finite, then $h(S) = 0$.*

(ii) *If $0 \to S' \to S \to S'' \to 0$ is an exact sequence of $\mathcal{O}[x]/\boldsymbol{\alpha\beta}\mathcal{O}[x]$-modules and two of the three Herbrand quotients exist, then the third exists and*

$$h(S) = h(S') + h(S'').$$

PROOF. This is a standard fact about Herbrand quotients, see for example [**Se3**] §VIII.4. If $\boldsymbol{\alpha} = (x^n - 1)/(x - 1)$, $\boldsymbol{\beta} = x - 1$ and G is a cyclic group of order n with a generator which acts on S as multiplication by x, then

$$\hat{H}^0(G, S) = S^{\boldsymbol{\beta}=0}/\boldsymbol{\alpha} S \quad \text{and} \quad \hat{H}^1(G, S) = S^{\boldsymbol{\alpha}=0}/\boldsymbol{\beta} S.$$

For completeness we sketch a proof in our more general setting.

Assertion (i) follows from the exact sequences

$$0 \longrightarrow S^{\boldsymbol{\alpha}=0} \longrightarrow S \xrightarrow{\boldsymbol{\alpha}} \boldsymbol{\alpha} S \longrightarrow 0,$$

$$0 \longrightarrow S^{\boldsymbol{\beta}=0}/\boldsymbol{\alpha} S \longrightarrow S/\boldsymbol{\alpha} S \xrightarrow{\boldsymbol{\beta}} S^{\boldsymbol{\alpha}=0} \longrightarrow S^{\boldsymbol{\alpha}=0}/\boldsymbol{\beta} S \longrightarrow 0.$$

For (ii), multiplication by $\boldsymbol{\beta}$ induces a snake lemma exact sequence

$$0 \longrightarrow {S'}^{\boldsymbol{\beta}=0} \longrightarrow S^{\boldsymbol{\beta}=0} \longrightarrow {S''}^{\boldsymbol{\beta}=0} \xrightarrow{\psi} S'/\boldsymbol{\beta} S' \longrightarrow S/\boldsymbol{\beta} S \longrightarrow S''/\boldsymbol{\beta} S'' \longrightarrow 0.$$

This gives rise to a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{coker}(\psi) & \longrightarrow & S/\boldsymbol{\beta}S & \longrightarrow & S''/\boldsymbol{\beta}S'' & \longrightarrow & 0 \\ & & \boldsymbol{\alpha}\Big\downarrow & & \boldsymbol{\alpha}\Big\downarrow & & \boldsymbol{\alpha}\Big\downarrow & & \\ 0 & \longrightarrow & S'^{\boldsymbol{\beta}=0} & \longrightarrow & S^{\boldsymbol{\beta}=0} & \longrightarrow & \ker(\psi) & \longrightarrow & 0. \end{array}$$

Applying the snake lemma again gives an exact sequence

$$\begin{aligned} 0 \longrightarrow A \longrightarrow S^{\boldsymbol{\alpha}=0}/\boldsymbol{\beta}S \longrightarrow S''^{\boldsymbol{\alpha}=0}/\boldsymbol{\beta}S'' \\ \longrightarrow S'^{\boldsymbol{\beta}=0}/\boldsymbol{\alpha}S' \longrightarrow S^{\boldsymbol{\beta}=0}/\boldsymbol{\alpha}S \longrightarrow B \longrightarrow 0 \end{aligned}$$

where

$$0 \longrightarrow B \longrightarrow S''^{\boldsymbol{\beta}=0}/\boldsymbol{\alpha}S'' \xrightarrow{\psi} S'^{\boldsymbol{\alpha}=0}/\boldsymbol{\beta}S' \longrightarrow A \longrightarrow 0.$$

Assertion (ii) follows from these two exact sequences. □

LEMMA 1.4. *Suppose* $\boldsymbol{\alpha\beta} = \prod_{i=1}^{k} \boldsymbol{\rho}_i$ *with* $\boldsymbol{\rho}_i \in \mathcal{O}[x]$, *and suppose further that* $\boldsymbol{\rho}_i$ *is relatively prime to* $\boldsymbol{\beta}$ *for every* $i > 1$. *Let* $S = \oplus_i \mathcal{O}[x]/\boldsymbol{\rho}_i\mathcal{O}[x]$. *Then* $h(S) = 0$.

PROOF. For each i let $S_i = \mathcal{O}[x]/\boldsymbol{\rho}_i\mathcal{O}[x]$. If $i > 1$ then, since $\boldsymbol{\rho}_i$ is relatively prime to $\boldsymbol{\beta}$ (and therefore must divide $\boldsymbol{\alpha}$), we see easily that $S_i^{\boldsymbol{\beta}=0} = \boldsymbol{\alpha}S_i = 0$ and $S_i^{\boldsymbol{\alpha}=0} = S_i$. Thus

$$h(S_i) = -\ell_{\mathcal{O}}(S_i/\boldsymbol{\beta}S_i) = -\ell_{\mathcal{O}}(\mathcal{O}[x]/(\boldsymbol{\beta}, \boldsymbol{\rho}_i))$$

which is finite. By Proposition 1.3 and Example 1.2 we conclude that the Herbrand quotient $h(S_1)$ exists as well, and that $h(S) = \sum_i h(S_i) = h(\mathcal{O}[x]/p(x)) = 0$. □

2. p-adic representations

Let T be a free $\mathcal{O}$-module of finite rank, and let σ be an $\mathcal{O}$-linear automorphism of T. Let $p(x) = \det(1 - \sigma^{-1}x|T) \in \mathcal{O}[x]$, and suppose further that $p(1) = 0$ (i.e., $\det(1 - \sigma|T) = 0$). Then there is a unique polynomial $q(x) \in \mathcal{O}[x]$ such that

$$p(x) = (1 - x)q(x).$$

The Cayley-Hamilton theorem shows that $p(\sigma) = 0$, so T is an $\mathcal{O}[x]/p(x)$-module, with x acting via σ. Thus we are in the setting of §1, with $\boldsymbol{\alpha} = q(x)$ and $\boldsymbol{\beta} = x - 1$.

Let Φ denote the field of fractions of $\mathcal{O}$ and $V = T \otimes \Phi$.

LEMMA 2.1. *Suppose* T *is a direct sum of cyclic* $\mathcal{O}[\sigma]$*-modules, and suppose further that* $\dim_\Phi(V/(\sigma - 1)V) = 1$. *Then the Herbrand quotient* $h(T) = 0$.

PROOF. Since $\mathcal{O}[\sigma]$ is a quotient of $\mathcal{O}[x]$, as an $\mathcal{O}[x]$-module we can identify

$$T = \oplus_i \mathcal{O}[x]/f_i(x)\mathcal{O}[x]$$

where $p(x) = \prod_i f_i(x)$. The assumption that $\dim_\Phi(V/(\sigma - 1)V) = 1$ implies that exactly one of the $f_i(x)$ (say, f_1) is divisible by $x - 1$. Thus we can apply Lemma 1.4 to conclude that $h(T) = 0$. □

LEMMA 2.2. *There is an* $\mathcal{O}[\sigma]$*-submodule* S *of* T *such that* S *is a direct sum of cyclic* $\mathcal{O}[\sigma]$*-modules and* $\ell_{\mathcal{O}}(T/S)$ *is finite.*

PROOF. Since the polynomial ring $\Phi[x]$ is a principal ideal domain, V is a direct sum of cyclic $\Phi[\sigma]$-modules, and the lemma follows easily. $\square$

PROPOSITION 2.3. *If* $\dim_\Phi(V/(\sigma-1)V)=1$ *then* $h(T)=0$.

PROOF. This is immediate from Proposition 1.3 and Lemmas 2.1 and 2.2. $\square$

LEMMA 2.4. *Suppose* $\dim_\Phi(V/(\sigma-1)V)=1$. *Then*

(i) $V^{q(\sigma)=0}=(\sigma-1)V$ *and* $V^{\sigma=1}=q(\sigma)V$,

(ii) *the map* $V/(\sigma-1)V \xrightarrow{q(\sigma)} V^{\sigma=1}$ *is an isomorphism.*

PROOF. Viewing V as a $\Phi[x]$-module with x acting via σ, there is an isomorphism

$$V\cong\bigoplus_i \Phi[x]/f_i^{e_i}\Phi[x]$$

where the $f_i\in\Phi[x]$ are irreducible, $f_i(0)=1$, and

$$\prod_i f_i(x)^{e_i}=p(x)=(1-x)q(x).$$

Since $\dim_\Phi(V/(\sigma-1)V)=1$, precisely one of the f_i is $1-x$. Both assertions follow easily from this. $\square$

PROPOSITION 2.5. *Suppose* $\dim_\Phi(V/(\sigma-1)V)=1$, *and let* $W=V/T$. *Then the lengths of the following* $\mathcal{O}$*-modules are finite and equal.*

(i)	$T^{\sigma=1}/q(\sigma)T$	(iv)	$W^{\sigma=1}/q(\sigma)W$
(ii)	$T^{q(\sigma)=0}/(\sigma-1)T$	(v)	$W^{q(\sigma)=0}/(\sigma-1)W$
(iii)	$(T/(\sigma-1)T)_{\mathrm{tors}}$	(vi)	$W^{\sigma=1}/W^{\sigma=1}_{\mathrm{div}}$

where $W^{\sigma=1}_{\mathrm{div}}$ *denotes the maximal divisible* $\mathcal{O}$*-submodule of* $W^{\sigma=1}$.

PROOF. Proposition 2.3 says that $h(T)=0$, so (i) and (ii) have the same (finite) length. Similarly Lemma 2.4(i) shows that $h(V)=0$, so by Proposition 1.3(ii) $h(W)=0$ as well. Thus (iv) and (v) have the same length.

By Lemma 2.4(i), $V^{q(\sigma)=0}/(\sigma-1)V=0$. Therefore $T^{q(\sigma)=0}/(\sigma-1)T$ is a torsion $\mathcal{O}$-module, and since $T/T^{q(\sigma)=0}$ is torsion-free we have

$$(T/(\sigma-1)T)_{\mathrm{tors}}=T^{q(\sigma)=0}/(\sigma-1)T$$

and so (ii) and (iii) are isomorphic. It follows similarly from Lemma 2.4(i) that $q(\sigma)W=W^{\sigma=1}_{\mathrm{div}}$ and (iv) is isomorphic to (vi).

It remains to compare (i) with (v). Consider the diagram

$$\begin{tikzcd}
 & T/(\sigma-1)T \arrow[r] \arrow[d, "q(\sigma)"'] & V/(\sigma-1)V \arrow[r] \arrow[d, "q(\sigma)"'] & W/(\sigma-1)W \arrow[r] \arrow[d, "q(\sigma)"'] & 0 \\
0 \arrow[r] & T^{\sigma=1} \arrow[r] & V^{\sigma=1} \arrow[r] & W^{\sigma=1}. &
\end{tikzcd}$$

By Lemma 2.4(ii), the center vertical map is an isomorphism, so the snake lemma gives (i) $\cong$ (v). $\square$

For the next two corollaries let $W=V/T$, and if $M\in\mathcal{O}$ let W_M denote the kernel of multiplication by M on W.

COROLLARY 2.6. *Suppose* $\dim_\Phi(V/(\sigma-1)V) = 1$, *and let* b *denote the common length of the modules in Proposition* 2.5. *Then the kernel and cokernel of the map*

$$W_M/(\sigma-1)W_M \xrightarrow{q(\sigma)} W_M^{\sigma=1}$$

have length at most $2b$.

PROOF. Consider the diagram

$$\begin{tikzcd} W/(\sigma-1)W \arrow[r, "q(\sigma)", "\phi"'] & W^{\sigma=1} \\ W_M/(\sigma-1)W_M \arrow[u] \arrow[r, "q(\sigma)", "\phi_M"'] & W_M^{\sigma=1} \arrow[u] \end{tikzcd} \tag{1}$$

The kernel and cokernel of ϕ are (v) and (iv) of Proposition 2.5, respectively, and therefore both have length b. Multiplying the exact sequence

$$0 \longrightarrow W_M \longrightarrow W \xrightarrow{M} W \longrightarrow 0$$

by $\sigma - 1$ yields a snake lemma exact sequence

$$W^{\sigma=1} \xrightarrow{M} W^{\sigma=1} \longrightarrow W_M/(\sigma-1)W_M \longrightarrow W/(\sigma-1)W.$$

Therefore the kernel of the left-hand vertical map of (1) is $W^{\sigma=1}/M(W^{\sigma=1})$, which is a quotient of the module (vi) of Proposition 2.5, and hence has length at most b. Thus we conclude that $\ell_{\mathcal{O}}(\ker(\phi_M)) \le 2b$. The exact sequence

$$0 \longrightarrow W_M^{\sigma=1} \longrightarrow W_M \xrightarrow{\sigma-1} W_M \longrightarrow W_M/(\sigma-1)W_M \longrightarrow 0$$

shows that $\ell_{\mathcal{O}}(W_M/(\sigma-1)W_M) = \ell_{\mathcal{O}}(W_M^{\sigma=1})$, so

$$\ell_{\mathcal{O}}(\operatorname{coker}(\phi_M)) = \ell_{\mathcal{O}}(\ker(\phi_M)) \le 2b$$

as well. □

COROLLARY 2.7. *Suppose* τ *is an* $\mathcal{O}$*-linear automorphism of* W_M *such that* $W_M/(\tau-1)W_M$ *is free of rank one over* $\mathcal{O}/M\mathcal{O}$, *and* $Q(x) \in (\mathcal{O}/M\mathcal{O})[x]$ *is such that* $(1-x)Q(x) = \det(1-\tau^{-1}x|W_M)$. *Then the map*

$$W_M/(\tau-1)W_M \xrightarrow{Q(\tau)} W_M^{\tau=1}$$

is an isomorphism.

PROOF. We will show that there is an automorphism σ of T such that

(i) σ induces τ on W_M,
(ii) $T/(\sigma-1)T$ is free of rank one over $\mathcal{O}$.

Once we have done this, we can apply the results of this section with this choice of σ. Condition (ii) shows that the module of Proposition 2.5(iii) is zero, so the integer b of Corollary 2.6 is zero. It follows from condition (i) that $q(\sigma)$ reduces to $Q(\tau)$ on W_M, so this corollary follows from Corollary 2.6.

It remains to find such a σ. Since $W_M/(\tau-1)W_M$ is free of rank one over $\mathcal{O}/M\mathcal{O}$, it follows that $W_M^{\tau=1}$ is free of rank one over $\mathcal{O}/M\mathcal{O}$ as well. Therefore we can choose a basis $\{w_1, \ldots, w_d\}$ of W_M such that $\tau w_1 = w_1$, where $d = \operatorname{rank}_{\mathcal{O}} T$.

For each i fix $t_i \in T$ which reduces to w_i. By Nakayama's Lemma $\{t_1, t_2, \dots, t_d\}$ is an $\mathcal{O}$-basis of T, and we define σ on this basis by lifting the action of τ on the w_i, and requiring that $\sigma(t_1) = t_1$. Then (i) is satisfied, $\operatorname{rank}_{\mathcal{O}} T/(\sigma - 1)T \geq 1$, and since $(T/(\sigma - 1)T) \otimes (\mathcal{O}/M\mathcal{O}) = W_M/(\tau - 1)W_M$ is a cyclic $\mathcal{O}$-module, we can apply Nakayama's Lemma again to deduce (ii). $\square$

APPENDIX B

Continuous cohomology and inverse limits

NOTATION. If G and T are topological groups then $\mathrm{Hom}(G,T)$ will always denote the group of *continuous* homomorphisms from G to T. We denote by $\mathrm{Maps}(G,T)$ the topological group of continuous functions (not necessarily homomorphisms) from G to T, with the compact-open topology.

1. Preliminaries

Since we will use it repeatedly, we record without proof the following well-known algebraic result.

PROPOSITION 1.1. (i) *Suppose $\{A_n\}$, $\{B_n\}$, and $\{C_n\}$ are inverse systems of topological groups and there are exact sequences*

$$0 \longrightarrow A_n \longrightarrow B_n \longrightarrow C_n \longrightarrow 0$$

for every n, compatible with the maps of the inverse systems. If the A_n are compact, then the induced sequence

$$0 \longrightarrow \varprojlim_n A_n \longrightarrow \varprojlim_n B_n \longrightarrow \varprojlim_n C_n \longrightarrow 0$$

is exact.

(ii) *If $\mathcal{O}$ is a discrete valuation ring with fraction field Φ and $\{A_n\}$ is an inverse system of finite $\mathcal{O}$-modules, then the canonical map*

$$\varinjlim_n \mathrm{Hom}(A_n, \Phi/\mathcal{O}) \longrightarrow \mathrm{Hom}(\varprojlim_n A_n, \Phi/\mathcal{O})$$

is an isomorphism.

2. Continuous cohomology

For this section suppose G is a profinite group and T is a topological G-module, i.e., an abelian topological group with a continuous action of G.

DEFINITION 2.1. Following Tate [**T4**], we define the continuous cohomology groups $H^i(G,T)$ as follows. Let $C^i(G,T) = \mathrm{Maps}(G^i,T)$. For every $i \geq 0$ there is a coboundary map $d_i : C^i(G,T) \to C^{i+1}(G,T)$ defined in the usual way (see for example [**Se3**] §VII.3), and we set

$$H^i(G,T) = \ker(d_i)/\mathrm{image}(d_{i-1}).$$

If $0 \to T' \to T \to T'' \to 0$ is an exact sequence and *if* there is a continuous section (again a set map, not necessarily a homomorphism) from $T'' \to T$, then

$$0 \longrightarrow C^i(G,T') \longrightarrow C^i(G,T) \longrightarrow C^i(G,T'') \longrightarrow 0$$

is exact for every i and there is a long exact sequence

$$\cdots \longrightarrow H^i(G,T') \longrightarrow H^i(G,T) \longrightarrow H^i(G,T'') \longrightarrow H^{i+1}(G,T') \longrightarrow \cdots.$$

REMARK 2.2. Note that if T'' is topologically discrete, as is assumed in the more "classical" formulations of profinite group cohomology, then there is always a continuous section $T'' \to T$. This is the case whenever T' is open in T. Also, when T is a finitely generated $\mathbf{Z}_p$-module, or a finite-dimensional $\mathbf{Q}_p$-vector space, with the usual topology, there is a continuous section. These are the only situations in which we will use these cohomology groups.

For the situations of interest to us, the following propositions will allow us to work with the cohomology groups $H^1(G,T)$ exactly as if T were discrete. The first two are due to Tate [**T4**]; see also Jannsen [**J**].

PROPOSITION 2.3 ([**T4**] Corollary 2.2, [**J**] §2). *Suppose $i > 0$ and $T = \varprojlim T_n$ where each T_n is a finite (discrete) G-module. If $H^{i-1}(G,T_n)$ is finite for every n then*

$$H^i(G,T) = \varprojlim_n H^i(G,T_n).$$

PROPOSITION 2.4 ([**T4**] Proposition 2.3). *If T is a finitely-generated $\mathbf{Z}_p$-module, then for every $i \geq 0$, $H^i(G,T)$ has no divisible elements and the natural map*

$$H^i(G,T) \otimes \mathbf{Q}_p \longrightarrow H^i(G,T \otimes \mathbf{Q}_p)$$

is an isomorphism.

PROPOSITION 2.5. *Suppose H is a closed, normal subgroup of G.*

(i) *There is an inflation-restriction exact sequence*

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

(ii) *Suppose further that p is a prime, and for every G-module (resp. H-module) S of finite, p-power order, $H^1(G,S)$ and $H^2(G,S)$ (resp. $H^1(H,S)$) is finite. If T is discrete, or T is a finitely generated $\mathbf{Z}_p$-module, or T is a finite dimensional $\mathbf{Q}_p$-vector space, then there is a Hochschild-Serre exact sequence extending the sequence of* (i)

$$0 \to H^1(G/H,T^H) \to H^1(G,T) \to H^1(H,T)^{G/H} \to H^2(G/H,T^H) \to H^2(G,T).$$

PROOF. If T is discrete both assertions are standard. The proof of (i) in general is identical to proof in this classical case.

Suppose T is finitely generated over $\mathbf{Z}_p$. Then for every $n \geq 0$, T/p^nT is discrete so there is a Hochschild-Serre exact sequence for T/p^nT. Our hypotheses ensure that all the terms in this sequence are finite, and so taking the inverse limit over n and applying Proposition 2.3 gives the exact sequence of (ii) for T.

If T is a finite dimensional $\mathbf{Q}_p$-vector space, choose a G-stable $\mathbf{Z}_p$-lattice $T_0 \subset T$. Then as above we have a Hochschild-Serre exact sequence for T_0, and tensoring with $\mathbf{Q}_p$ and using Proposition 2.4 gives the desired exact sequence for T. $\square$

REMARK 2.6. To apply Proposition 2.5(ii) we need to know when a group G has the property that $H^i(G,S)$ is finite for every i and every G-module S of finite p-power order. For example, this is true whenever the pro-p-part of G is (topologically) finitely generated.

We also have the following well-known result. In the important case $i = 1$ it follows easily from class field theory (see for example [**Se2**] Propositions II.14 and III.8). We say a $\mathbf{Z}_p$-module is co-finitely generated if its Pontryagin dual is finitely generated.

PROPOSITION 2.7. *Suppose either*

(i) *K is a global field, K_S is a (possibly infinite) Galois extension of K unramified outside a finite set of places of K, and $G = \mathrm{Gal}(K_S/K)$,*
(ii) *K is a local field and $G = G_K$, or*
(iii) *K is a local field of residue characteristic different from p and G is the inertia group in G_K.*

If T is a G-module which is finite (resp. finitely generated over $\mathbf{Z}_p$, resp. co-finitely generated over $\mathbf{Z}_p$) and $i \geq 0$, then $H^i(G,T)$ is finite (resp. finitely generated over $\mathbf{Z}_p$, resp. co-finitely generated over $\mathbf{Z}_p$).

LEMMA 2.8. *Suppose $G \cong \hat{\mathbf{Z}}$, the profinite completion of $\mathbf{Z}$, and γ is a topological generator of G. Suppose T is a $\mathbf{Z}_p[G_K]$ module which is either a finitely generated $\mathbf{Z}_p$-module, or a finite dimensional $\mathbf{Q}_p$-vector space, or a discrete torsion $\mathbf{Z}_p$-module. Then*

$$H^1(G,T) \cong T/(\gamma-1)T$$

with an isomorphism induced by evaluating cocycles at γ.

PROOF. It is easy to see that evaluating cocycles at γ induces a well-defined, injective map

$$H^1(G,T) \longrightarrow T/(\gamma-1)T. \tag{1}$$

It remains only to show that this map is surjective.

Using direct limits, inverse limits (Proposition 2.3), and/or tensoring with $\mathbf{Q}_p$ (Proposition 2.4), we can reduce this lemma to the case where T is finite. When T is finite, the Lemma is well-known, see for example [**Se3**] §XIII.1. $\square$

3. Inverse limits

For this section suppose that K is a field, p is a rational prime, and T is a $\mathbf{Z}_p[G_K]$-module which is finitely generated over $\mathbf{Z}_p$.

We will write $K \subset_{\mathrm{f}} F$ to indicate that F is a finite extension of K. If K_∞ is an infinite extension of K and $\{C_F : K \subset_{\mathrm{f}} F \subset K_\infty\}$ is an inverse system of abelian groups, we will write $\{c_F\}$ for a typical element of $\varprojlim C_F$ with $c_F \in C_F$.

LEMMA 3.1. *If $K \subset_{\mathrm{f}} F_1 \subset_{\mathrm{f}} F_2 \subset_{\mathrm{f}} \cdots$ and $\cup_{n=1}^{\infty} F_n = K_\infty$, then*

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T) = \varprojlim_n H^1(F_n, T/p^nT).$$

PROOF. By Proposition 2.3 we see

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T) = \varprojlim_n H^1(F_n,T) = \varprojlim_n \varprojlim_m H^1(F_n,T/p^mT)$$
$$= \varprojlim_n H^1(F_n,T/p^nT). \qquad \square$$

LEMMA 3.2. *Suppose K_∞ is an infinite p-extension of K. Then*

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} T^{G_F} = 0.$$

where the maps in the inverse system are given by the norm maps

$$\mathbf{N}_{F'/F} : T^{G_{F'}} \to T^{G_F}$$

if $K \subset_{\mathrm{f}} F \subset_{\mathrm{f}} F' \subset K_\infty$.

PROOF. Define a submodule T_0 of T by

$$T_0 = \cup_{K \subset_{\mathrm{f}} F \subset K_\infty} T^{G_F}.$$

Then T_0 is finitely generated over $\mathbf{Z}_p$ since T is, so we must have $T_0 = T^{G_{F_0}}$ for some finite extension F_0 of K in K_∞. Therefore

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} T^{G_F} = \varprojlim_{F_0 \subset_{\mathrm{f}} F \subset K_\infty} T^{G_F} = \varprojlim_{F_0 \subset_{\mathrm{f}} F \subset K_\infty} T_0$$

where the norm maps $\mathbf{N}_{F'/F}$ in the right-hand inverse system are multiplication by $[F' : F]$. Since T_0 is finitely generated over $\mathbf{Z}_p$, and for every F, $[F' : F]$ is divisible by arbitrarily large powers of p as F' varies, this inverse limit is zero. $\square$

If K is a finite extension of $\mathbf{Q}_\ell$ for some ℓ, let $H^1_{\mathrm{ur}}(K,T)$ denote the subgroup of $H^1(K,T)$ defined in Chapter I §3.1.

PROPOSITION 3.3. *Suppose K is a finite extension of $\mathbf{Q}_\ell$, $\ell \neq p$, and K_∞ is the unique $\mathbf{Z}_p$-extension of K. If $\{c_F\} \in \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T)$ then for every F*

$$c_F \in H^1_{\mathrm{ur}}(F,T).$$

PROOF. Let $\mathcal{I} \subset G_K$ denote the inertia group. Since $\ell \neq p$, K_∞/K is unramified, so $\mathcal{I}$ is also the inertia group in G_F for every $F \subset K_\infty$. Thus for $K \subset_{\mathrm{f}} F \subset K_\infty$ we have an exact sequence

$$0 \longrightarrow H^1_{\mathrm{ur}}(F,T) \longrightarrow H^1(F,T) \longrightarrow H^1(\mathcal{I},T)^{G_F}.$$

Since $\ell \neq p$, Proposition 2.7(iii) shows that $H^1(\mathcal{I},T)$ is finitely generated over $\mathbf{Z}_p$. Now taking inverse limits with respect to F and applying Lemma 3.2 to the G_K-module $H^1(\mathcal{I},T)$ shows

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1_{\mathrm{ur}}(F,T) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T)$$

which proves the proposition. $\square$

For the next two corollaries, suppose that K is a number field and K_∞ is an abelian extension of K satisfying

$$\mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^d, \qquad d \geq 1.$$

COROLLARY 3.4. *Suppose*

$$\{c_F\} \in \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T).$$

If $K \subset_{\mathrm{f}} F \subset K_\infty$, λ *is a prime of* F *not dividing* p, *and the decomposition group of* λ *in* $\mathrm{Gal}(K_\infty/K)$ *is infinite, then* $(c_F)_\lambda \in H^1_{\mathrm{ur}}(F_\lambda, T)$.

PROOF. Fix a prime $\bar{\lambda}$ of K_∞ above λ. Since the decomposition group of λ in $\mathrm{Gal}(K_\infty/K)$ is infinite, if $K \subset_{\mathrm{f}} F \subset K_\infty$ we can find $F \subset_{\mathrm{f}} F' \subset F_\infty \subset K_\infty$ such that $\mathrm{Gal}(F_\infty/F') \cong \mathbf{Z}_p$ and $\bar{\lambda}$ is undecomposed in F_∞/F'. Thus Proposition 3.3 applied to the classes $\{(c_L)_{\bar{\lambda}} : F' \subset_{\mathrm{f}} L \subset F_\infty\}$ shows that $(c_{F'})_{\bar{\lambda}} \in H^1_{\mathrm{ur}}(F'_{\bar{\lambda}}, T)$. Since this holds for all choices of $\bar{\lambda}$, and $\mathrm{Cor}_{F'/F}(c_{F'}) = c_F$, we deduce that $(c_F)_\lambda \in H^1_{\mathrm{ur}}(F_\lambda, T)$. □

The following corollary will be used together with Proposition 2.7 to study $\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T)$.

COROLLARY 3.5. *If* S *is a set of places of* K *containing all primes where* T *is ramified, all primes dividing* p, *all primes whose decomposition group in* $\mathrm{Gal}(K_\infty/K)$ *is finite, and all infinite places then*

$$\varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T) = \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(K_S/F,T)$$

where K_S *is the maximal extension of* K *unramified outside* S.

PROOF. Suppose that

$$\{c_F\} \in \varprojlim_{K \subset_{\mathrm{f}} F \subset K_\infty} H^1(F,T).$$

Let $\mathcal{I} \subset G_K$ be an inertia group of a prime $\mathfrak{q}$ of K not in S and fix $K \subset_{\mathrm{f}} F \subset K_\infty$. Since F/K is unramified at $\mathfrak{q}$, $\mathcal{I}$ is also an inertia group of a prime $\mathcal{Q}$ of F above $\mathfrak{q}$, so by Corollary 3.4 the restriction of c_F is zero in $H^1(\mathcal{I},T) = \mathrm{Hom}(\mathcal{I},T)$. It follows that every cocycle representing c_F factors through $\mathrm{Gal}(K_S/F)$, which proves the corollary. □

4. Induced modules

Again we suppose that G is a profinite group, and now H is a closed subgroup of G and T is a discrete H-module (not necessarily a G-module).

DEFINITION 4.1. Define the induced module $\mathrm{Ind}_H(T) = \mathrm{Ind}_H^G(T)$ by

$$\mathrm{Ind}_H(T) = \{f \in \mathrm{Maps}(G,T) : f(\eta\gamma) = \eta f(\gamma) \text{ for every } \gamma \in G \text{ and } \eta \in H.\}$$

We let G act on $\mathrm{Ind}_H(T)$ by

$$(gf)(\gamma) = f(\gamma g) \quad \text{for } g, \gamma \in G.$$

Since T is discrete, $\mathrm{Ind}_H(T)$ a discrete G-module.

If $H = \{1\}$, then $\mathrm{Ind}_H(T)$ is just $\mathrm{Maps}(G,T)$. If H' is a closed subgroup of H then there is a natural inclusion $\mathrm{Ind}_H(T) \subset \mathrm{Ind}_{H'}(T)$. If T is a G-module then evaluation at 1 induces an isomorphism $\mathrm{Ind}_G(T) \xrightarrow{\sim} T$, and so there is a natural (continuous) inclusion $T \hookrightarrow \mathrm{Ind}_H(T)$, in which $t \in T$ goes to the map $\gamma \mapsto \gamma t$.

PROPOSITION 4.2. *Suppose Γ is an open subgroup of G. For every $i \geq 0$ there is a canonical isomorphism*

$$H^i(\Gamma, \mathrm{Ind}_H(T)) \cong \bigoplus_{g \in H\backslash G/\Gamma} H^i(g\Gamma g^{-1} \cap H, T).$$

PROOF. First suppose $i = 0$. Fix a set $S \subset G$ of double coset representatives for $H\backslash G/\Gamma$. If $f \in \mathrm{Ind}_H(T)^\Gamma$ then for every $s \in S$,

$$f(hs\gamma) = h(f(s)) \quad \text{for every } h \in H,\ \gamma \in \Gamma. \tag{2}$$

In particular if $h \in s\Gamma s^{-1} \cap H$, then $hf(s) = f(s)$ and so $f(s) \in T^{(s\Gamma s^{-1} \cap H)}$. Conversely, if for every $s \in S$ we have an element $f(s) \in T^{s\Gamma s^{-1} \cap H}$, we can use (2) to define an element $f \in \mathrm{Ind}_H(T)^\Gamma$. This proves the proposition when $i = 0$.

Now consider $i \geq 1$. The functor $T \rightsquigarrow \mathrm{Ind}_H(T)$ is exact on the category of discrete H-modules, so the proposition for T with $i \geq 1$ follows from the case $i = 0$ and the Leray spectral sequence comparing the functors

$$A \rightsquigarrow \bigoplus_{g \in H\backslash G/\Gamma} A^{g\Gamma g^{-1} \cap H}, \quad A \rightsquigarrow \mathrm{Ind}_H(A), \quad B \rightsquigarrow B^\Gamma$$

(see for example [**Sh**] pp. 50–51). □

REMARK 4.3. When $\Gamma = G$, Proposition 4.2 is Shapiro's Lemma.

COROLLARY 4.4. *With T, G, and H as above, for every open subgroup Γ of G there is an exact sequence*

$$\begin{aligned} 0 \longrightarrow \mathrm{Ind}_H(T)^\Gamma \longrightarrow \mathrm{Ind}_{\{1\}}(T)^\Gamma & \\ \longrightarrow (\mathrm{Ind}_{\{1\}}(T)/\mathrm{Ind}_H(T))^\Gamma & \longrightarrow H^1(\Gamma, \mathrm{Ind}_H(T)) \longrightarrow 0 \end{aligned}$$

PROOF. Proposition 4.2 with $H = \{1\}$ shows that $H^1(\Gamma, \mathrm{Ind}_{\{1\}}(T)) = 0$, so the exact sequence of the corollary is the beginning of the long exact Γ-cohomology sequence of the canonical exact sequence

$$0 \longrightarrow \mathrm{Ind}_H(T) \longrightarrow \mathrm{Ind}_{\{1\}}(T) \longrightarrow \mathrm{Ind}_{\{1\}}(T)/\mathrm{Ind}_H(T) \longrightarrow 0.$$ □

PROPOSITION 4.5. *Suppose K is a field, F is a finite extension of K, and T is a discrete G_K-module. Let $\mathbb{T} = \mathrm{Ind}_{\{1\}}^{G_K}(T)$. Then there is a commutative diagram with exact rows*

$$\begin{tikzcd}
0 \arrow[r] & T^{G_K} \arrow[r] \arrow[d, hook] & \mathbb{T}^{G_K} \arrow[r] \arrow[d, hook] & (\mathbb{T}/T)^{G_K} \arrow[r] \arrow[d, hook] & H^1(K,T) \arrow[r] \arrow[d, "\mathrm{Res}_F"] & 0 \\
0 \arrow[r] & T^{G_F} \arrow[r] \arrow[d, "\mathbf{N}_{F/K}"] & \mathbb{T}^{G_F} \arrow[r] \arrow[d, "\mathbf{N}_{F/K}"] & (\mathbb{T}/T)^{G_F} \arrow[r] \arrow[d, "\mathbf{N}_{F/K}"] & H^1(F,T) \arrow[r] \arrow[d, "\mathrm{Cor}_{F/K}"] & 0 \\
0 \arrow[r] & T^{G_K} \arrow[r] & \mathbb{T}^{G_K} \arrow[r] & (\mathbb{T}/T)^{G_K} \arrow[r] & H^1(K,T) \arrow[r] & 0
\end{tikzcd}$$

PROOF. The horizontal sequences are the exact sequences of Corollary 4.4 applied with $H = G_K$ and $\Gamma = G_K$ or G_F. The commutativity of the lower right square is essentially the definition of the corestriction map, and the rest of the commutativity is clear. □

5. Semilocal Galois cohomology

Suppose for this section that K is a number field, $\mathfrak{q}$ is a prime of K, F is a finite extension of K, and S is the set of primes of F above $\mathfrak{q}$. For every prime $\mathcal{Q} \in S$ fix a prime $\mathfrak{Q}$ of $\bar{K}$ above $\mathcal{Q}$ and let $\mathcal{I}_{\mathcal{Q}} \subset \mathcal{D}_{\mathcal{Q}} \subset G_K$ denote the inertia group and decomposition group of $\mathfrak{Q}$. Fix a $\mathcal{Q}_0 \in S$ and write $\mathcal{D} = \mathcal{D}_{\mathcal{Q}_0}$, $\mathcal{I} = \mathcal{I}_{\mathcal{Q}_0}$. Let $g_{\mathcal{Q}} \in G_K$ be such that $\mathfrak{Q} = g_{\mathcal{Q}}^{-1}\mathfrak{Q}_0$, and then $\mathcal{D}_{\mathcal{Q}} = g_{\mathcal{Q}}^{-1}\mathcal{D}g_{\mathcal{Q}}$.

Let T be a discrete G_K-module, and let $T' \subset T$ be a subset which is a $\mathcal{D}$-submodule, i.e., $\mathcal{D}$ sends T' into itself. For every $\mathcal{Q} \in S$ we let $T'_{\mathcal{Q}} = g_{\mathcal{Q}}^{-1}T'$, and then $T'_{\mathcal{Q}}$ is a $\mathcal{D}_{\mathcal{Q}}$-module.

PROPOSITION 5.1. *With notation as above, if $i \geq 0$ there is a canonical isomorphism*

$$H^i(F, \mathrm{Ind}_{\mathcal{D}}^{G_K}(T')) \cong \bigoplus_{\mathcal{Q}\in S} H^i(F_{\mathcal{Q}}, T'_{\mathcal{Q}}).$$

PROOF. The map

$$\begin{array}{ccc} \mathcal{D}\backslash G_K/G_F & \longrightarrow & S \\ \mathcal{D}gG_F & \mapsto & g^{-1}\mathcal{Q}_0 \end{array}$$

is a bijection. Applying Proposition 4.2 with $G = G_K$, $H = \mathcal{D}$, and $\Gamma = G_F$ yields

$$\begin{aligned} H^i(F, \mathrm{Ind}_{\mathcal{D}}^{G_K}(T')) &\cong \bigoplus_{\mathcal{Q}\in S} H^i(g_{\mathcal{Q}} G_F g_{\mathcal{Q}}^{-1} \cap \mathcal{D}, T') \\ &\cong \bigoplus_{\mathcal{Q}\in S} H^i(G_F \cap \mathcal{D}_{\mathcal{Q}}, T'_{\mathcal{Q}}) \\ &= \bigoplus_{\mathcal{Q}\in S} H^i(F_{\mathcal{Q}}, T'_{\mathcal{Q}}) \end{aligned}$$

so this proves the proposition. □

COROLLARY 5.2. *With notation as above, there are canonical isomorphisms*

$$H^i(G_F, \mathrm{Ind}_{\mathcal{D}}^{\mathcal{G}}(T)) \cong \bigoplus_{\mathcal{Q}\in S} H^i(F_{\mathcal{Q}}, T),$$

$$H^i(G_F, \mathrm{Ind}_{\mathcal{D}}^{\mathcal{G}}(T^{\mathcal{I}})) \cong \bigoplus_{\mathcal{Q}\in S} H^i(F_{\mathcal{Q}}, T^{\mathcal{I}_{\mathcal{Q}}}).$$

PROOF. This is Proposition 5.1 applied with $T' = T$ and with $T' = T^{\mathcal{I}}$. □

COROLLARY 5.3. *Suppose F is a finite Galois extension of K, T is a finitely generated $\mathbf{Z}_p$-module with a continuous action of G_K, and let $V = T \otimes \mathbf{Q}_p$.*

(i) *If $[F : K]$ is prime to p, the restriction map induces an isomorphism*

$$H^1(K_{\mathfrak{q}}, T) \cong \left(\oplus_{\mathcal{Q}|\mathfrak{q}} H^1(F_{\mathcal{Q}}, T)\right)^{\mathrm{Gal}(F/K)}.$$

(ii) *The restriction map induces an isomorphism*

$$H^1(K_{\mathfrak{q}}, V) \cong \left(\oplus_{\mathcal{Q}|\mathfrak{q}} H^1(F_{\mathcal{Q}}, V)\right)^{\mathrm{Gal}(F/K)}.$$

Proof. Using the discrete module T/p^nT we have a diagram

$$\begin{array}{ccc} H^1(K, \mathrm{Ind}_{\mathcal{D}}^{G_K}(T/p^nT)) & \xrightarrow{\sim} & H^1(K_{\mathfrak{q}}, T/p^nT) \\ {\scriptstyle \mathrm{Res}_F}\big\downarrow & & \big\downarrow{\scriptstyle \oplus \mathrm{Res}_{\mathcal{Q}}} \\ H^1(F, \mathrm{Ind}_{\mathcal{D}}^{G_K}(T/p^nT))^{\mathrm{Gal}(F/K)} & \xrightarrow{\sim} & \left(\oplus_{\mathcal{Q}\in S} H^1(F_{\mathcal{Q}}, T/p^nT)\right)^{\mathrm{Gal}(F/K)} \end{array}$$

where the vertical maps are restriction maps and the horizontal maps are the isomorphisms of Corollary 5.2. The inflation-restriction sequence shows that the left-hand vertical map has kernel and cokernel annihilated by $[F : K]$, and hence the right-hand map does as well. Taking the inverse limit of the right-hand maps and applying Proposition 2.3 shows that the restriction map

$$H^1(K_{\mathfrak{q}}, T) \longrightarrow \left(\oplus_{\mathcal{Q}\in S} H^1(F_{\mathcal{Q}}, T)\right)^{\mathrm{Gal}(F/K)}$$

has kernel and cokernel annihilated by $[F : K]$. This proves (i), and combined with Proposition 2.4 it proves (ii). $\square$

APPENDIX C

Cohomology of p-adic analytic groups

1. Irreducible actions of compact groups

THEOREM 1.1. *Suppose V is a finite dimensional $\mathbf{Q}_p$-vector space, and G is a compact subgroup of* $\mathrm{GL}(V)$ *which acts irreducibly on V. Then $H^1(G,V)=0$.*

The proof will be divided into a series of lemmas. For this section we fix a finite dimensional $\mathbf{Q}_p$-vector space V and a compact subgroup G of $\mathrm{GL}(V)$ which acts irreducibly on V, as in Theorem 1.1. Let Z denote the center of G.

LEMMA 1.2. *If $g \in Z$, $g \neq 1$ then $g-1$ is invertible on V.*

PROOF. Let $V_1 = \ker(g-1)$. Since g is in the center of G, V_1 is stable under G. Since $g \neq 1$, $V_1 \neq V$, and hence by our irreducibility assumption $V_1 = 0$. □

LEMMA 1.3. *If $Z \neq \{1\}$ then $H^1(G,V)=0$.*

PROOF. Suppose that $g \in Z$, $g \neq 1$, and let B be the closed subgroup generated by g. We have an inflation-restriction exact sequence

$$0 \longrightarrow H^1(G/B, V^B) \longrightarrow H^1(G,V) \longrightarrow H^1(B,V).$$

By Lemma 1.2, $V^B = 0$ and

$$H^1(B,V) \subset V/(g-1)V = 0.$$ □

LEMMA 1.4. *Suppose U is an open normal subgroup of G. Then V is completely reducible as a representation of U.*

PROOF. Let V_0 denote the subspace of V generated by all irreducible U-subspaces of V. Since U is normal in G, V_0 is stable under G. Clearly $V_0 \neq 0$, so the irreducibility hypothesis for G implies that $V_0 = V$. It follows easily that V is a direct sum of a finite collection of irreducible U-subspaces. □

For a general reference for the material on p-adic Lie groups, Lie algebras, and their cohomology which we need, see [**Laz**] or [**Bo**].

PROPOSITION 1.5. $\mathrm{Lie}(G)$ *is reductive.*

PROOF. It follows from Lemma 1.4 that the representation of $\mathrm{Lie}(G)$ on V is semisimple, and it is clearly also faithful. By [**Bo**] §I.6.4 Proposition 5, it follows that $\mathrm{Lie}(G)$ is reductive. □

PROOF OF THEOREM 1.1. The compact subgroup G of $\mathrm{GL}(V)$ is a profinite p-analytic group in the sense of [**Laz**] §III.3.2. Therefore by Lazard's Théorème V.2.4.10, for every sufficiently small open normal subgroup U of G,

$$H^1(G,V) = H^1(U,V)^G = H^1(\mathrm{Lie}(G),V)^G.$$

If the center of $\mathrm{Lie}(G)$ is zero then (since $\mathrm{Lie}(G)$ is reductive by Lemma 1.5) $\mathrm{Lie}(G)$ is semisimple, and in that case (see [**Bo**] Exercise 1(b), §I.6) $H^1(\mathrm{Lie}(G),V) = 0$. If the center of $\mathrm{Lie}(G)$ is not zero then every sufficiently small open normal subgroup U of G has nontrivial center, and then Lemmas 1.3 and 1.4 together show that $H^1(U,V) = 0$. Thus in either case we can conclude that $H^1(G,V) = 0$. □

LEMMA 1.6. *Suppose $\mathcal{O}$ is the ring of integers of a finite extension Φ of $\mathbf{Q}_p$, V is a Φ-vector space and G acts Φ-linearly. If G contains an element g such that* $\dim_\Phi(V/(g-1)V) = 1$, *then Z acts on V via scalars in $\mathcal{O}^\times$.*

PROOF. The one-dimensional subspace $\ker(g-1)$ of V is preserved by Z. Let $\chi : Z \to \mathrm{Aut}(\ker(g-1)) \cong \Phi^\times$ be the character determined by this action. Since Z is compact, $\chi(Z) \subset \mathcal{O}^\times$. Let

$$V_\chi = \{v \in V : zv = \chi(z)v \text{ for every } z \in Z\}.$$

Then V_χ is nonzero and stable under G, so the irreducibility of V implies that $V_\chi = V$. □

PROPOSITION 1.7. *Suppose A is an abelian quotient of G. Then the projection of Z to A has finite cokernel.*

PROOF. Let $\pi : G \twoheadrightarrow A$ be the projection map. Since A is compact, it is a finitely generated $\mathbf{Z}_p$-module.

By Proposition 1.5, G is reductive. It follows easily that the induced map of Lie algebras maps the center of $\mathrm{Lie}(G)$ onto $\mathrm{Lie}(A)$, and hence $[A : \pi(Z_U)]$ is finite where Z_U is the center of a sufficiently small open normal subgroup U of G.

The finite group G/U acts on Z_U by conjugation, and we define (writing Z_U as an additive group)

$$\mathbf{N}(z) = \sum_{g \in G/U} z^g.$$

Clearly $\mathbf{N}(Z_U) \subset Z$, and also (since $\ker(\pi)$ contains all commutators) $\pi(\mathbf{N}(z)) = \pi([G : U]z)$ for every $z \in Z_U$. Therefore $\pi(Z)$ contains $[G : U]\pi(Z_U)$. This completes the proof. □

2. Application to Galois representations

For this section fix a (possibly infinite) Galois extension F/K of fields of characteristic different from p, and a subgroup B of $K^\times$. (In our applications, K will be a number field, F will be an abelian extension of K and B will be $\mathcal{O}_K^\times$.) Suppose $\mathcal{O}$ is the ring of integers of a finite extension Φ of $\mathbf{Q}_p$, and V is a finite-dimensional Φ-vector space with a continuous Φ-linear action of G_K, such that V is irreducible over G_F. Let $\Omega = F(\boldsymbol{\mu}_{p^\infty}, B^{1/p^\infty}, V)$, the smallest extension of F whose absolute Galois group acts trivially on $\boldsymbol{\mu}_{p^\infty}$, B^{1/p^∞}, and V. The result we will need is the following.

THEOREM 2.1. *One of the following three situations holds.*

(i) $H^1(\Omega/F, V) = 0$.

(ii) G_K *acts on* V *via a character* ρ *of* $\mathrm{Gal}(F/K)$*, and* $\mathrm{Gal}(F/K)$ *acts on* $H^1(\Omega/F, V)$ *via* ρ.

(iii) B *is infinite,* G_K *acts on* V *via* $\varepsilon_{\mathrm{cyc}}\rho$ *where* $\varepsilon_{\mathrm{cyc}}$ *is the cyclotomic character and* ρ *is a character of* $\mathrm{Gal}(F/K)$*, and* $\mathrm{Gal}(F/K)$ *acts on* $H^1(\Omega/F, V)$ *via* ρ.

PROOF. Let $\Omega_V = F(V)$, the smallest extension of F such that G_{Ω_V} acts trivially on V (so $\Omega_V = \bar{F}^H$ where $H = \ker(G_F \to \mathrm{Aut}(V))$, and Ω_V is necessarily Galois over F). Define $D = \mathrm{Gal}(\Omega_V/F)$, and $\Omega_{V,\boldsymbol{\mu}} = \Omega_V(\boldsymbol{\mu}_{p^\infty})$. We have a diagram

$$\begin{tikzcd}
& & & \Omega \\
& & \Omega_{V,\boldsymbol{\mu}} \arrow[ur, dash] \arrow[dr, dash] \arrow[ddll, dash] & \\
& & & \Omega_V \\
K(\boldsymbol{\mu}_{p^\infty}) & & F \arrow[ur, dash, "D"'] & \\
& K \arrow[ul, dash] \arrow[ur, dash] & &
\end{tikzcd}$$

The inflation restriction exact sequence gives

$$H^1(D, V) \longrightarrow H^1(\Omega/F, V) \longrightarrow H^1(\Omega/\Omega_V, V)^D.$$

The map $D \to \mathrm{Aut}(V)$ is injective by definition of Ω_V, so D is isomorphic to a compact subgroup of $\mathrm{GL}(V)$. We have assumed that D acts irreducibly on V, so Theorem 1.1 shows that $H^1(D, V) = 0$ and we get an injection

$$H^1(\Omega/F, V) \hookrightarrow H^1(\Omega/\Omega_V, V)^D = \mathrm{Hom}(\mathrm{Gal}(\Omega/\Omega_V), V)^D.$$

If $\mathrm{Hom}(\mathrm{Gal}(\Omega/\Omega_V), V)^D = 0$ then (i) holds. We consider two cases.

Case I: $\Omega_{V,\boldsymbol{\mu}} \neq \Omega_V$. In this case $\mathrm{Gal}(\Omega_{V,\boldsymbol{\mu}}/\Omega_V)$ acts on $\mathrm{Gal}(\Omega/\Omega_{V,\boldsymbol{\mu}})$ via the (nontrivial) cyclotomic character. Let Ω_{ab} denote the maximal abelian extension of Ω_V in Ω. Then $\mathrm{Gal}(\Omega_{V,\boldsymbol{\mu}}/\Omega_V)$ acts on $\mathrm{Gal}(\Omega_{\mathrm{ab}}/\Omega_{V,\boldsymbol{\mu}})$ trivially *and* via the cyclotomic character, and it follows that $\mathrm{Gal}(\Omega_{\mathrm{ab}}/\Omega_{V,\boldsymbol{\mu}})$ is killed by $|\boldsymbol{\mu}_{p^\infty} \cap \Omega_V|$, which is finite since $\Omega_{V,\boldsymbol{\mu}} \neq \Omega_V$. Hence $\mathrm{Hom}(\mathrm{Gal}(\Omega_{\mathrm{ab}}/\Omega_{V,\boldsymbol{\mu}}), V) = 0$ so

$$\begin{aligned}
\mathrm{Hom}(\mathrm{Gal}(\Omega/\Omega_V), V)^D &= \mathrm{Hom}(\mathrm{Gal}(\Omega_{\mathrm{ab}}/\Omega_V), V)^D \\
&= \mathrm{Hom}(\mathrm{Gal}(\Omega_{V,\boldsymbol{\mu}}/\Omega_V), V)^D = \mathrm{Hom}(\mathrm{Gal}(\Omega_{V,\boldsymbol{\mu}}/\Omega_V), V^D)
\end{aligned}$$

since D (and in fact all of $\mathrm{Gal}(\Omega_V/K)$) acts trivially on $\mathrm{Gal}(\Omega_{V,\boldsymbol{\mu}}/\Omega_V)$. Since D acts irreducibly on V, either $V^D = 0$ or V is one-dimensional with trivial action of G_F. Therefore (i) or (ii) is satisfied in this case.

Case II: $\Omega_{V,\boldsymbol{\mu}} = \Omega_V$. In this case $\boldsymbol{\mu}_{p^\infty} \subset \Omega_V$, $\mathrm{Gal}(\Omega/\Omega_V)$ is abelian, and $\mathrm{Gal}(\Omega_V/K)$ acts on $\mathrm{Gal}(\Omega/\Omega_V)$ via the cyclotomic character. Thus

$$\mathrm{Hom}(\mathrm{Gal}(\Omega/\Omega_V), V)^D = \mathrm{Hom}(\mathrm{Gal}(\Omega/\Omega_V), V^{\varepsilon_{\mathrm{cyc}}})$$

where $V^{\varepsilon_{\mathrm{cyc}}}$ denotes the subspace of V on which D (and hence G_F) acts via $\varepsilon_{\mathrm{cyc}}$. Again, since D acts irreducibly on V, either $V^{\varepsilon_{\mathrm{cyc}}} = 0$ or V is one-dimensional with G_F acting via $\varepsilon_{\mathrm{cyc}}$. Therefore (i) or (iii) is satisfied in this case. □

COROLLARY 2.2. *Suppose T is a finitely generated $\mathcal{O}$-submodule of V, stable under G_K, and let $W = V/T$. Then one of the following three situations holds.*

(i) *$H^1(\Omega/F, W)$ is finite.*

(ii) *G_K acts on T via a character ρ of* $\mathrm{Gal}(F/K)$, *and $H^1(\Omega/F, W)$ has a subgroup of finite index on which* $\mathrm{Gal}(F/K)$ *acts via ρ.*

(iii) *B is infinite, G_K acts on T via $\varepsilon_{\mathrm{cyc}}\rho$ where $\varepsilon_{\mathrm{cyc}}$ is the cyclotomic character and ρ is a character of* $\mathrm{Gal}(F/K)$, *and $H^1(\Omega/F, W)$ has a subgroup of finite index on which* $\mathrm{Gal}(F/K)$ *acts via ρ.*

PROOF. Since $\mathrm{Gal}(\Omega/F)$ is (topologically) finitely generated, it follows from Proposition B.2.4 that the map $H^1(\Omega/F, V) \to H^1(\Omega/F, W)$ has finite cokernel. Now the corollary is immediate from Theorem 2.1. □

APPENDIX D

p-adic calculations in cyclotomic fields

In this appendix we carry out some p-adic calculations in cyclotomic fields which are used in examples in Chapters III and VIII. Everything here is essentially well-known, due originally to Iwasawa and Coleman.

For every $n \geq 1$ fix a primitive n-th root of unity ζ_n such that $\zeta_{mn}^n = \zeta_m$ for every m and n. By slight abuse of notation, for every n we will write $\mathbf{Z}_p[\boldsymbol{\mu}_n] = \mathbf{Z}[\boldsymbol{\mu}_n] \otimes \mathbf{Z}_p$, the p-adic completion of $\mathbf{Z}[\boldsymbol{\mu}_n]$, and similarly $\mathbf{Q}_p(\boldsymbol{\mu}_n) = \mathbf{Q}(\boldsymbol{\mu}_n) \otimes \mathbf{Q}_p$.

Define

$$\log : \mathbf{Z}_p[\boldsymbol{\mu}_n][[X]]^\times = \mathbf{Z}_p[\boldsymbol{\mu}_n]^\times \times (1 + X\mathbf{Z}_p[\boldsymbol{\mu}_n][[X]]) \to \mathbf{Q}_p(\boldsymbol{\mu}_n)[[X]]$$

by combining the p-adic logarithm on $\mathbf{Z}_p[\boldsymbol{\mu}_n]^\times$ and the power series expansion of $\log(1 + Xf(X))$.

If $\alpha \in \mathbf{Z}_p$ define

$$[\alpha](X) = (1+X)^\alpha - 1 \in X\mathbf{Z}_p[[X]].$$

Let D be the derivation $(1+X)\frac{d}{dX}$ of $\overline{\mathbf{Q}_p}[[X]]$. Then for every $\alpha \in \mathbf{Z}_p$ and $g \in \overline{\mathbf{Q}_p}[[X]]$,

$$D[\alpha] = \alpha \cdot ([\alpha](X) + 1) \quad \text{and} \quad D(g \circ [\alpha]) = \alpha \cdot (Dg) \circ [\alpha].$$

If m is prime to p we let Fr_p be the Frobenius of p in $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})$, the automorphism which sends ζ_m to ζ_m^p. We let Fr_p act on $\mathbf{Q}_p(\boldsymbol{\mu}_m)[[X]]$ by acting on the power series coefficients.

1. Local units in cyclotomic fields

In this section we will construct, for every positive integer n, a homomorphism $\lambda_n : \mathbf{Z}_p[\boldsymbol{\mu}_n]^\times \to \mathbf{Z}_p$. These maps are used in Chapter III §4 to construct an Euler system for the trivial representation $\mathbf{Z}_p$.

Fix an integer m prime to p. Define

$$f_m(X) = m\zeta_m[m^{-1}](X) - \frac{m\zeta_m^p}{|(\mathbf{Z}_p^\times)_{\mathrm{tors}}|} \sum_{\beta \in (\mathbf{Z}_p^\times)_{\mathrm{tors}}} \frac{[m^{-1}\beta](X)}{\beta} \in \mathbf{Z}_p[\boldsymbol{\mu}_m][[X]]$$

and

$$\mathcal{G}_m(X) = \zeta_m \log(1+X) - m \sum_{i=1}^{\infty} p^i \zeta_m^{p^{-i}} + \sum_{i=0}^{\infty} \Big(\frac{f_m^{\mathrm{Fr}_p^i}([p^i](X))}{p^i} - (\zeta_m^{p^i} - \zeta_m^{p^{i+1}}) \log(1+X) \Big).$$

Lemma 1.1(i) below shows that this sum converges to an element of $\mathbf{Q}_p(\boldsymbol{\mu}_m)[[X]]$, and a direct computation shows that

$$D\mathcal{G}_m(X) = \zeta_m + \sum_{i=0}^{\infty}\Big(\zeta_m^{p^i}[m^{-1}p^i](X) - \frac{\zeta_m^{p^{i+1}}}{|(\mathbf{Z}_p^{\times})_{\mathrm{tors}}|}\sum_{\beta\in(\mathbf{Z}_p^{\times})_{\mathrm{tors}}}[m^{-1}\beta p^i](X)\Big) \tag{1}$$

LEMMA 1.1. (i) $\mathcal{G}_m(X) \in \mathbf{Q}_p(\boldsymbol{\mu}_m)[[X]]$, *i.e., the sum in the definition of* $\mathcal{G}_m(X)$ *converges.*

(ii) *There is a unique* $g_m(X) \in \mathbf{Z}_p[\boldsymbol{\mu}_m][[X]]$, $g_m(X) \equiv 1 \pmod{(p, X)}$, *such that* $\log(g_m(X)) = \mathcal{G}_m(X)$.

(iii) *If ℓ is a prime different from p then*

$$\mathrm{Tr}_{\mathbf{Q}_p(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}_p(\boldsymbol{\mu}_m)} D\mathcal{G}_{\ell m}(X) = \begin{cases} -\ell D\mathcal{G}_m^{\mathrm{Fr}_\ell^{-1}}([\ell^{-1}](X)) & \text{if } \ell \nmid m \\ 0 & \text{if } \ell \mid m. \end{cases}$$

(iv) $\sum_{\zeta\in\boldsymbol{\mu}_p}\mathcal{G}_m(\zeta(1+X)-1) = \mathcal{G}_m^{\mathrm{Fr}_p}([p](X))$.

(v) *If g_m is as in* (ii), *then* $\prod_{\zeta\in\boldsymbol{\mu}_p} g_m(\zeta(1+X)-1) = g_m^{\mathrm{Fr}_p}([p](X))$.

PROOF. The first two assertions follow from Theorem 24 of [**Co**] with $a = -m\sum_{i=1}^{\infty}p^i\zeta_m^{p^{-i}}$, $b=\zeta_m$, and $f(X) = f_m(X) - (\zeta_m - \zeta_m^p)X$. Assertion (iii) follows directly from (1) and the fact that

$$\mathrm{Tr}_{\mathbf{Q}(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}(\boldsymbol{\mu}_m)}\zeta_{m\ell} = \begin{cases} -\zeta_m^{\mathrm{Fr}_\ell^{-1}} & \text{if } \ell\nmid m \\ 0 & \text{if } \ell \mid m. \end{cases}$$

The fourth assertion is similarly a direct computation, and then (v) follows from (iv), since log is injective on $1 + (p,X)\mathbf{Z}_p[\boldsymbol{\mu}_m][[X]]$. □

DEFINITION 1.2. Suppose $m \geq 1$ is prime to p, and let $N(m) = \prod_{\text{primes } \ell \mid m}\ell$. Let $g_m(X) \in \mathbf{Z}_p[\boldsymbol{\mu}_m][[X]]^{\times}$ be as in Lemma 1.1(ii). For $n \geq 0$ define

$$\alpha_{mp^n} = \prod_{d\mid m, N(m)\mid d}\Big(g_d^{\mathrm{Fr}_p^{-n}}(\zeta_{p^n}-1)\Big) \in \mathbf{Z}_p[\boldsymbol{\mu}_{mp^n}]^{\times}.$$

By Lemma 1.1(v),

$$\mathbf{N}_{\mathbf{Q}(\boldsymbol{\mu}_{mp^{n+1}})/\mathbf{Q}(\boldsymbol{\mu}_{mp^n})}\alpha_{mp^{n+1}} = \begin{cases} \alpha_{mp^n} & \text{if } n\geq 1 \\ \alpha_m^{1-\mathrm{Fr}_p^{-1}} & \text{if } n=0. \end{cases}$$

Suppose $\mathfrak{P}$ is a prime of $\mathbf{Q}(\boldsymbol{\mu}_m)$ above p. We will also write $\mathfrak{P}$ for the unique prime of $\mathbf{Q}(\boldsymbol{\mu}_{mp^n})$ above $\mathfrak{P}$, for every n. We let $\boldsymbol{\alpha}_{m,\mathfrak{P}} \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{mp^\infty})_{\mathfrak{P}}^{\mathrm{ab}}/\mathbf{Q}(\boldsymbol{\mu}_{mp^\infty})_{\mathfrak{P}})$ be the image of $\{\alpha_{mp^n}\}_{n\geq 1}$ under the Artin map of local class field theory. Using the Kummer pairing we define

$$\lambda_{mp^n} : \mathbf{Z}_p[\boldsymbol{\mu}_{mp^n}]^{\times} \to \mathbf{Z}_p$$

by, writing $u \in \mathbf{Z}_p[\boldsymbol{\mu}_{mp^n}]^{\times}$ as $(u_{\mathfrak{P}}) \in \oplus_{\mathfrak{P}}\mathbf{Z}[\boldsymbol{\mu}_{mp^n}]_{\mathfrak{P}}^{\times}$,

$$\prod_{\mathfrak{P}\mid p}(u_{\mathfrak{P}}^{p^{-n}})^{\boldsymbol{\alpha}_{m,\mathfrak{P}}-1} = \zeta_{p^n}^{m\lambda_{mp^n}(u)}.$$

The explicit reciprocity law gives the following description of the map λ_{mp^n}. Recall that D is the derivation $(1+X)\frac{d}{dX}$.

PROPOSITION 1.3. *If m is prime to p and $n \geq 0$ then*

$$\lambda_{mp^n}(u) = p^{-n}\mathrm{Tr}_{\mathbf{Q}_p(\boldsymbol{\mu}_{mp^n})/\mathbf{Q}_p}(x_{mp^n}\log_p(u))$$

where $\log_p$ *is the usual p-adic logarithm and*

$$x_{mp^n} = \begin{cases} m^{-1} \displaystyle\sum_{d \mid m, N(m) \mid d} (D\mathcal{G}_d^{\mathrm{Fr}_p^{-n}})(\zeta_{p^n} - 1) & \text{if } n > 0 \\ m^{-1} \displaystyle\sum_{d \mid m, N(m) \mid d} (D\mathcal{G}_d)(0) - \dfrac{1}{p}(D\mathcal{G}_d^{\mathrm{Fr}_p^{-1}})(0) & \text{if } n = 0. \end{cases}$$

PROOF. The formula for $\lambda_{mp^n}(u)$ is the explicit reciprocity law of Wiles [**Wi**] (see also [**dS**] Theorem I.4.2) in the present situation. □

LEMMA 1.4. *For every $m \geq 1$ (not necessarily prime to p) and prime ℓ, there is a commutative diagram*

$$\begin{tikzcd}
\mathbf{Z}_p[\boldsymbol{\mu}_{m\ell}]^\times \arrow[dr, "\lambda_{m\ell}"] & \\
& \mathbf{Z}_p \\
\mathbf{Z}_p[\boldsymbol{\mu}_m]^\times \arrow[uu, hook, "1 \text{ or } -\mathrm{Fr}_\ell"] \arrow[ur, "\lambda_m"'] &
\end{tikzcd}$$

where the vertical map is $\begin{cases} \text{the inclusion } \mathbf{Z}_p[\boldsymbol{\mu}_m]^\times \subset \mathbf{Z}_p[\boldsymbol{\mu}_{m\ell}]^\times & \text{if } \ell \mid m \text{ or } \ell = p, \\ -\mathrm{Fr}_\ell \text{ followed by that inclusion} & \text{if } \ell \nmid mp. \end{cases}$

PROOF. Let the x_m be as defined in Proposition 1.3. Using Lemma 1.1(iii) and (iv) we see that

$$\mathrm{Tr}_{\mathbf{Q}_p(\boldsymbol{\mu}_{m\ell})/\mathbf{Q}_p(\boldsymbol{\mu}_m)} x_{m\ell} = \begin{cases} -\mathrm{Fr}_\ell^{-1} x_m & \text{if } \ell \nmid mp \\ x_m & \text{if } \ell \mid m \text{ or } \ell = p. \end{cases}$$

for every m and ℓ. Now the lemma follows from Proposition 1.3. □

Let ω denote the Teichmüller character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$ (if p is odd) or $\boldsymbol{\mu}_4$ (if $p = 2$).

LEMMA 1.5. *Suppose $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbf{Q}_p$, and $\chi : G_{\mathbf{Q}} \to \mathcal{O}^\times$ is a character of finite order. Let f be the conductor of χ, and suppose that $p^2 \nmid f$ and $\chi^{-1}\omega(p) \neq 1$ (where we view $\chi^{-1}\omega$ as a primitive Dirichlet character). Let $\Delta = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_f)/\mathbf{Q})$. Then $\sum_{\delta \in \Delta} \chi(\delta)\lambda_f^\delta$ generates the $\mathcal{O}$-module $\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times, \mathcal{O})^{\chi^{-1}}$ (the submodule of $\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times, \mathcal{O})$ on which Δ acts via χ^{-1}).*

PROOF. Let $\lambda_{f,\chi} = \sum_{\delta \in \Delta} \chi(\delta)\lambda_f^\delta$. Write $f = mp^\epsilon$ with m prime to p, $\epsilon = 0$ or 1. Let x_f be as in Proposition 1.3, and let y_f be the "conductor f" part of x_f, namely

$$y_f = \begin{cases} f^{-1}\big((D\mathcal{G}_f)(0) - \frac{1}{p}(D\mathcal{G}_f^{\mathrm{Fr}_p^{-1}})(0)\big) = f^{-1}(\zeta_f - \frac{1}{p}\zeta_f^{\mathrm{Fr}_p^{-1}}) & \text{if } \epsilon = 0 \\ m^{-1}(D\mathcal{G}_m^{\mathrm{Fr}_p^{-1}})(\zeta_p - 1) = m^{-1}(\zeta_f + \frac{p}{p-1}\zeta_m) & \text{if } \epsilon = 1. \end{cases}$$

By Proposition 1.3,

$$\begin{aligned}
\lambda_{f,\chi}(u) &= p^{-\epsilon}\sum_{\delta\in\Delta}\chi(\delta)\mathrm{Tr}_{\mathbf{Q}_p(\boldsymbol{\mu}_f)/\mathbf{Q}_p} x_f^{\delta}\log_p(u) \\
&= p^{-\epsilon}\sum_{\delta\in\Delta}\chi(\delta)\mathrm{Tr}_{\mathbf{Q}_p(\boldsymbol{\mu}_f)/\mathbf{Q}_p} y_f^{\delta}\log_p(u) \\
&= p^{-\epsilon}\sum_{\delta\in\Delta}\sum_{\gamma\in\Delta}\chi(\delta)y_f^{\delta\gamma}\log_p(u^{\gamma}) \\
&= p^{-\epsilon}\sum_{\delta\in\Delta}(\chi(\delta)y_f^{\delta})\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\log_p(u^{\gamma}) \\
&= \frac{1}{f}(1-p^{-1}\chi(p))\sum_{\delta\in\Delta}(\chi(\delta)\zeta_f^{\delta})\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\log_p(u^{\gamma})).
\end{aligned}$$

First suppose $p\nmid f$, so $\chi(p)\in\mathcal{O}^{\times}$. Let g_m be as in Lemma 1.1(ii) and let $u=g_m(0)^{1/m}\in\mathbf{Z}_p[\boldsymbol{\mu}_f]^{\times}$. Then $\log_p(u)=m^{-1}\mathcal{G}_m(0)=-\sum_{i=1}^{\infty}p^i\zeta_m^{p^{-i}}$, so

$$\begin{aligned}
\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\log_p(u^{\gamma})) &= -\sum_{i=1}^{\infty}p^i\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\zeta_m^{\mathrm{Fr}_p^{-i}\gamma}) \\
&= -\sum_{i=1}^{\infty}p^i\chi^{-i}(p)\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\zeta_m^{\gamma}).
\end{aligned}$$

Thus

$$\begin{aligned}
\lambda_{f,\chi}(u) &= \frac{1}{f}(\chi(p)-p)\sum_{i=0}^{\infty}p^i\chi^{-i-1}(p)\sum_{\delta\in\Delta}(\chi(\delta)\zeta_f^{\delta})\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\zeta_f^{\gamma}) \\
&= \chi(-1)(\chi(p)-p)\sum_{i=0}^{\infty}p^i\chi^{-i-1}(p)\in\mathcal{O}^{\times}
\end{aligned}$$

the last equality since the product of the two Gauss sums is $\chi(-1)f$.

Now suppose $p\mid f$, but $p^2\nmid f$, and take $u=\big(g_m^{\mathrm{Fr}_p^{-1}}(\zeta_p-1)\big)^{1/m}\in\mathbf{Z}_p[\boldsymbol{\mu}_f]^{\times}$. Then

$$\begin{aligned}
\log_p(u) &= m^{-1}\mathcal{G}_m^{\mathrm{Fr}_p^{-1}}(\zeta_p-1) \\
&= \Big(1-\frac{1}{p-1}\sum_{\substack{\sigma\in\Delta\\ \sigma|_{\mathbf{Q}(\boldsymbol{\mu}_m)}=\mathrm{Fr}_p}}\omega(\sigma^{-1})\sigma\Big)\Big(\zeta_m^{p^{-1}}(\zeta_p^{m^{-1}}-1)\Big)-\sum_{i=1}^{\infty}p^i\zeta_m^{p^{-(i+1)}}
\end{aligned}$$

so with this choice, since $\zeta_m^{p^{-1}}\zeta_p^{m^{-1}}=\zeta_f$,

$$\begin{aligned}
\sum_{\gamma\in\Delta}\chi^{-1}(\gamma)\log_p(u^{\gamma}) &= \Big(1-\frac{1}{p-1}\sum_{\substack{\sigma\in\Delta\\ \sigma|_{\mathbf{Q}(\boldsymbol{\mu}_m)}=\mathrm{Fr}_p}}\omega(\sigma^{-1})\chi(\sigma)\Big)\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\zeta_f^{\gamma}) \\
&= (1-\chi\omega^{-1}(p))\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\zeta_f^{\gamma})
\end{aligned}$$

and

$$\lambda_{f,\chi}(u)=\frac{1}{f}(1-\chi\omega^{-1}(p))\sum_{\delta\in\Delta}(\chi(\delta)\zeta_f^{\delta})\sum_{\gamma\in\Delta}(\chi^{-1}(\gamma)\zeta_f^{\gamma})=\chi(c)(1-\chi\omega(p)^{-1})\in\mathcal{O}^{\times}.$$

In either case the p-adic logarithm shows that $\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times, \mathcal{O})^{\chi^{-1}}$ is a rank-one $\mathcal{O}$-module, which is clearly torsion-free and hence free. The formulas above show that

$$\lambda_{f,\chi} \notin \mathfrak{p}\mathrm{Hom}(\mathbf{Z}_p[\boldsymbol{\mu}_f]^\times, \mathcal{O})^{\chi^{-1}}$$

where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$, and the lemma follows. $\square$

2. Cyclotomic units

For this section suppose that $m > 1$ and m is prime to p. Fix an embedding $\overline{\mathbf{Q}_p} \subset \mathbf{C}$ and let $\zeta_n = e^{2\pi i/n}$ for every $n \in \mathbf{Z}^+$. Define

$$u_m(X) = \zeta_m(1+X)^{m^{-1}} - 1 \in \mathbf{Z}_p[\boldsymbol{\mu}_m][[X]].$$

LEMMA 2.1. *Suppose $m > 1$, m is prime to p, $\gamma \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{mp})/\mathbf{Q})$, and $\zeta_{mp^n}^\gamma = \zeta_{mp^n}^b$ with $b \in \mathbf{Z}$. Then for every $k \geq 2$ and $n \geq 0$,*

$$\begin{aligned}(D^k \log u_m^{\mathrm{Fr}_p^{-n}\gamma})&(\zeta_{p^n}^\gamma - 1)\\ &= (-1)^{k-1}\Gamma(k)(2\pi i)^{-k} p^{nk}(\zeta(b, mp^n; k) + (-1)^k \zeta(-b, mp^n; k))\end{aligned}$$

where $\zeta(a, r; s)$ is the partial Riemann zeta function $\displaystyle\sum_{j \equiv a \pmod r} j^{-s}$.

PROOF. Since $m > 1$ and m is prime to p, we see that $u_m(0) \in \mathbf{Z}_p[\boldsymbol{\mu}_m]^\times$. Therefore $u_m^{\mathrm{Fr}_p^{-n}\gamma} \in \mathbf{Z}_p[\boldsymbol{\mu}_m][[X]]^\times$ and $\log u_m^{\mathrm{Fr}_p^{-n}\gamma}$ is defined. Thus

$$\begin{aligned}(D^k \log u_m^{\mathrm{Fr}_p^{-n}\gamma})(\zeta_{p^n}^\gamma - 1) &= D^{k-1} \left. \frac{(1+X)(u_m^{\mathrm{Fr}_p^{-n}\gamma})'(X)}{u_m^{\mathrm{Fr}_p^{-n}\gamma}(X)} \right|_{X=\zeta_{p^n}^b - 1} \\ &= D^{k-1} \left. \frac{m^{-1}\zeta_m^{bp^{-n}}(1+X)^{m^{-1}}}{\zeta_m^{bp^{-n}}(1+X)^{m^{-1}} - 1} \right|_{X=\zeta_{p^n}^b - 1} \\ &= m^{-k} D^{k-1} \left. \frac{\zeta_m^{bp^{-n}}(1+X)}{\zeta_m^{bp^{-n}}(1+X) - 1} \right|_{X=\zeta_{p^n}^{bm^{-1}} - 1}.\end{aligned}$$

Substituting $e^Z = 1 + X$, $\frac{d}{dZ} = (1+X)\frac{d}{dX}$, this becomes

$$\begin{aligned} m^{-k} D^{k-1} \left. \frac{\zeta_m^{bp^{-n}}(1+X)}{\zeta_m^{bp^{-n}}(1+X) - 1} \right|_{X=\zeta_{p^n}^{bm^{-1}} - 1} &= m^{-k} \frac{d^{k-1}}{dZ^{k-1}} \left. \frac{\zeta_m^{bp^{-n}} e^Z}{\zeta_m^{bp^{-n}} e^Z - 1} \right|_{e^Z = \zeta_{p^n}^{bm^{-1}}} \\ &= m^{-k} \frac{d^{k-1}}{dZ^{k-1}} \left. \frac{e^Z}{e^Z - 1} \right|_{Z = \frac{2\pi i b}{mp^n}}. \end{aligned}$$

By [**A1**] equation (10), p. 187 (or just observe that the difference is a bounded entire function which vanishes at 0)

$$\frac{e^Z}{e^Z - 1} = \frac{1}{2} + \sum_{n \in \mathbf{Z}} \left(\frac{1}{Z - 2\pi i n} + \frac{1}{2\pi i n} \right).$$

Thus for $k \geq 2$, $r > 1$, and $c \in \mathbf{Z} - r\mathbf{Z}$,

$$\begin{aligned}\frac{d^{k-1}}{dZ^{k-1}} \frac{e^Z}{e^Z - 1}\bigg|_{Z=\frac{2\pi i c}{r}} &= (-1)^{k-1}(k-1)!(2\pi i)^{-k} r^k \sum_{n \in \mathbf{Z}} \frac{1}{(c+nr)^k} \\ &= (-1)^{k-1}\Gamma(k)(2\pi i)^{-k} r^k (\zeta(c,r;k) + (-1)^k \zeta(-c,r;k)).\end{aligned}$$

Combining these formulas proves the lemma. □

Define

$$h_m(X) = \prod_{\beta \in (\mathbf{Z}_p^\times)_{\mathrm{tors}}} u_m((1+X)^\beta - 1)\bar{u}_m((1+X)^\beta - 1)$$

where $\bar{u}_m(X) = 1 - \zeta_m^{-1}(1+X)^{m^{-1}}$, and

$$\mathcal{H}_m(X) = \log h_m(X) - \frac{1}{p} \log h_m^{\mathrm{Fr}_p}((1+X)^p - 1).$$

For every $n > 1$ write $\Delta_n = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q})$ and $\Delta_n^+ = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_n)^+/\mathbf{Q})$.

Lemma 2.2. *Suppose $p > 2$, and let ω be the Teichmüller character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$. Suppose $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbf{Q}_p$, and $\chi : G_{\mathbf{Q}} \to \mathcal{O}^\times$ is a nontrivial even character of finite order, unramified at p. If m is the conductor of χ then*

$$\begin{aligned}&\sum_{\gamma \in \Delta_m^+} \chi^{-1}(\gamma) D^k \mathcal{H}_m^\gamma(\zeta_p - 1) \\ &\qquad = 2\Gamma(k)(-2\pi i)^{-k} L(\chi^{-1}\omega^k, k) \times \begin{cases} -\chi(p)p^k & \text{if } p-1 \nmid k \\ 1 - p^{k-1}\chi(p) & \text{if } p-1 \mid k. \end{cases}\end{aligned}$$

Proof. We have

$$D^k \mathcal{H}_m^\gamma(\zeta_p - 1) = D^k \log h_m^\gamma(\zeta_p - 1) - p^{k-1} D^k \log h_m^{\mathrm{Fr}_p \gamma}(0).$$

If $\zeta = \zeta_p$ or $\zeta = 1$,

$$\begin{aligned}D^k \log h_m^\gamma(\zeta - 1) &= \sum_{\beta \in (\mathbf{Z}_p^\times)_{\mathrm{tors}}} \beta^k D^k \log u_m^\gamma(\zeta^\beta - 1) + \beta^k D^k \log \bar{u}_m^\gamma(\zeta^\beta - 1) \\ &= \sum_{\sigma \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{mp})/\mathbf{Q}(\boldsymbol{\mu}_m)^+)} \omega^k(\sigma) D^k \log u_m^{\gamma\sigma}(\zeta^\sigma - 1).\end{aligned}$$

Thus by Lemma 2.1, writing $L_r(\chi^{-1}\omega^k, s)$ for the Dirichlet L-function with Euler factors for primes dividing r removed,

$$\begin{aligned}&\sum_{\gamma \in \Delta_m^+} \chi^{-1}(\gamma) D^k \mathcal{H}_m^\gamma(\zeta_p - 1) \\ &\quad = \sum_{\gamma \in \Delta_{mp}} \chi^{-1}\omega^k(\gamma) \Big(D^k \log u_m^\gamma(\zeta_p^\gamma - 1) - p^{k-1} D^k \log u_m^{\mathrm{Fr}_p \gamma}(0) \Big) \\ &\quad = (-1)^{k-1}\Gamma(k)(2\pi i)^{-k} p^k (1 + (-1)^k \chi^{-1}\omega^k(-1))\chi(p) L_{mp}(\chi^{-1}\omega^k, k) \\ &\qquad - \ p^{k-1}(-1)^{k-1}\Gamma(k)(2\pi i)^{-k}(1 + (-1)^k)\chi(p) L_m(\chi^{-1}, k) \sum_{\gamma \in \Delta_p} \omega^k(\gamma).\end{aligned}$$

Note that $\chi^{-1}\omega^k(-1) = (-1)^k$. If $p-1 \nmid k$ then $\sum_{\gamma\in\Delta_p} \omega^k(\gamma) = 0$, and we are left with

$$-2\Gamma(k)(-2\pi i)^{-k} p^k \chi(p) L(\chi^{-1}\omega^k, k).$$

If $p-1 \mid k$ then $\omega^k = 1$, and we get

$$\begin{aligned}2\Gamma(k)(-2\pi i)^{-k}\chi(p)L(\chi^{-1},k)(-p^k(1-\chi^{-1}(p)p^{-k}) + (p-1)p^{k-1})\\ = 2\Gamma(k)(-2\pi i)^{-k}L(\chi^{-1},k)(1-p^{k-1}\chi(p)).\end{aligned}$$

This completes the proof. $\square$

Bibliography

[Al] Alfohrs, L.: Complex Analysis (2nd edition), New York: McGraw-Hill (1966).

[BK] Bloch, S., Kato, K.: L-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift (Vol. I), P. Cartier, et al., eds., *Prog. in Math.* **86**, Boston: Birkhäuser (1990) 333–400.

[Bo] Bourbaki, N.: Lie groups and Lie algebras, Part I. Paris: Hermann (1975).

[BFH] Bump, D., Friedberg, S., Hoffstein, J.: Nonvanishing theorems for L-functions of modular forms and their derivatives. *Invent. math.* **102** (1990) 543–618.

[CW] Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer, *Invent. math.* **39** (1977) 223–251.

[Co] Coleman, R.: Division values in local fields, *Invent. math.* **53** (1979) 91–116.

[DR] Deligne, P., Ribet, K.: Values of abelian L-functions at negative integers over totally real fields, *Invent. math.* **59** (1980) 227–286.

[dS] de Shalit, E.: The Iwasawa theory of elliptic curves with complex multiplication, (*Perspec. in Math.***3**) Orlando: Academic Press (1987).

[Fl] Flach, M.: A finiteness theorem for the symmetric square of an elliptic curve, *Invent. math.* **109** (1992) 307–327.

[FPR] Fontaine, J-M., Perrin-Riou, B.: Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In: Motives (Part I), U. Jannsen et al., eds., *Proc. Symp. Pure Math.* **55**, 599–706 Providence: Amer. Math. Soc. (1994) 599–706.

[Fr] Fröhlich, A.: Local fields. In: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich, eds., Thompson Book Company, Washington, 1967, pp. 1–41.

[Gi] Gillard, R.: Unités cyclotomiques, unités semilocales et $\mathbf{Z}_\ell$-extensions, II, *Ann. Inst. Fourier* **29**, fasc. 4 (1979) 1–15.

[Gr1] Greenberg, R.: On p-adic L-functions and cyclotomic fields II, *Nagoya Math. J.* **67** (1977) 139–158.

[Gr2] ———: Iwasawa theory for p-adic representations, *Adv. Stud. in Pure Math.* **17** (1989) 97–137.

[Gr3] ———: Iwasawa theory for p-adic representations II, to appear.

[Gro1] Gross, B.: On the values of abelian L-functions at $s = 0$, *J. Fac. Sci. Univ. Tokyo* **35** (1988) 177–197.

[Gro2] ———: Kolyvagin's work on modular elliptic curves. In: L-functions and arithmetic (Durham, 1989), J. Coates and M. Taylor, eds. *London Math. Soc. Lect. Notes* **153** Cambridge: Cambridge Univ. Press (1991) 235–256.

[GZ] Gross, B., Zagier, D.: Heegner points and derivatives of L-series, *Invent. math.* **84** (1986) 225–320.

[Iw1] Iwasawa, K.: On some modules in the theory of cyclotomic fields, *J. Math. Soc. Japan* **16** (1964) 42–82.

[Iw2] ———: Lectures on p-adic L-functions, *Annals of Math. Studies* **74**, Princeton: Princeton University Press (1972).

[Iw3] ———: On $\mathbf{Z}_l$-extensions of algebraic number fields, *Annals of Math.* **98** (1973) 246–326.

[J] Jannsen, U.: Continuous étale cohomology, *Math. Annalen* **280** (1988) 207–245.

[Ka1] Kato, K.: Lectures in the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. In: Arithmetic Algebraic Geometry (Trento 1991), *Lecture Notes in Math.* **1553**, New York: Springer-Verlag (1993) 50–163.

[Ka2] ———: To appear.

[Ka3] ———: To appear.

[Ko1] Kolyvagin, V. A.: Finiteness of $E(\mathbf{Q})$ and $\text{Ш}(E, \mathbf{Q})$ for a subclass of Weil curves. (Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* **52** (1988) 522–540; English translation in *Math. USSR-Izv.* **32** (1989) 523–541.

[Ko2] ______: Euler systems. In: The Grothendieck Festschrift (Vol. II), P. Cartier, et al., eds., *Prog. in Math* **87**, Boston: Birkhäuser (1990) 435–483.

[Lan] Lang, S.: Cyclotomic fields I and II, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990).

[Laz] Lazard, M.: Groupes analytiques p-adiques, *Inst. Hautes Etudes Sci. Publ. Math.* **26** 1965.

[MSD] Mazur, B., Swinnerton-Dyer, H.P.F.: Arithmetic of Weil curves, *Inventiones math.* **25** (1974) 1–61.

[MTT] Mazur, B., Tate, J., Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. math.* **84** (1986) 1–48.

[MW] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbf{Q}$, *Invent. math.* **76** (1984) 179–330.

[Mi] Milne, J.S.: Arithmetic duality theorems, *Perspectives in Math.* **1**, Orlando: Academic Press (1986).

[MM] Murty, K., Murty, R.: Mean values of derivatives of modular L-series, *Annals of Math.* **133** (1991) 447–475.

[PR1] Perrin-Riou, B.: Théorie d'Iwasawa p-adique locale et globale, *Invent. math.* **99** (1990) 247–292.

[PR2] ______: Théorie d'Iwasawa des représentations p-adiques sur un corps local, *Invent. math.* **115** (1994) 81–149.

[PR3] ______: La fonction L p-adique de Kubota-Leopoldt. In: Arithmetic Geometry, *Contemp. math.* **174** (1994) 61–93.

[PR4] ______: Fonctions L p-adiques des représentations p-adiques, *Astérisque* **229** (1995).

[PR5] ______: Systèmes d'Euler p-adiques et théorie d'Iwasawa, to appear.

[Ro] Rohrlich, D.: On L-functions of elliptic curves and cyclotomic towers, *Invent. math.* **75** (1984) 409–423.

[Ru1] Rubin, K.: Global units and ideal class groups, *Invent. math.* **89** (1987) 511–526.

[Ru2] Rubin, K.: The work of Kolyvagin on the arithmetic of elliptic curves. In: Arithmetic of complex manifolds, *Lecture Notes in Math.* **1399**, New York: Springer-Verlag (1989) 128–136.

[Ru3] ______: The main conjecture. Appendix to: Cyclotomic fields I and II, S. Lang, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990) 397–419.

[Ru4] ______: Kolyvagin's system of Gauss sums. In: Arithmetic Algebraic Geometry, G. van der Geer, et al., eds., *Prog. in Math* **89**, Boston: Birkhäuser (1991) 435–324.

[Ru5] ______: The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. math.* **103** (1991) 25–68.

[Ru6] ______: Stark units and Kolyvagin's "Euler systems", *J. für die reine und angew. Math.* **425** (1992) 141–154.

[Ru7] ______: p-adic L-functions and rational points on elliptic curves with complex multiplication, *Invent. math.* **107** (1992) 323–350.

[Ru8] ______: A Stark conjecture "over $\mathbf{Z}$" for abelian L-functions with multiple zeros, *Annales de l'Institut Fourier***46**(1996) 33–62.

[Ru9] ______: Euler systems and modular elliptic curves. In: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds. *London Math. Soc. Lect. Notes* **254** Cambridge: Cambridge Univ. Press (1998) 351–367.

[RW] Rubin, K., Wiles, A.: Mordell-Weil groups of elliptic curves over cyclotomic fields. In: Number Theory related to Fermat's last theorem, *Progress in Math.***26**, Boston: Birkhauser (1982) 237–254.

[Schn] Schneider, P.: p-adic height pairings, II, *Inventiones math.* **79** (1985) 329–374.

[Scho] Scholl, A.: An introduction to Kato's Euler systems. In: Galois representations in arithmetic algebraic geometry, A. J. Scholl and R. L. Taylor, eds. *London Math. Soc. Lect. Notes* **254** Cambridge: Cambridge Univ. Press (1998) 379–460.

[Se1] Serre, J-P.: Classes des corps cyclotomiques (d'après K. Iwasawa), Séminaire Bourbaki exposé 174, December 1958. In: Séminaire Bourbaki vol. 5, Paris: Société Math. de France (1995) 83–93.

[Se2] ______: Cohomologie Galoisienne, Fifth edition. *Lecture Notes in Math.* **5** Berlin: Springer-Verlag (1994).

[Se3] ______: Corps Locaux, 2nd edition. Paris: Hermann (1968).

[Se4] ______: Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. math.* **15** (1972) 259–331.

[Sh] Shatz, S.: Profinite groups, arithmetic and geometry, *Annals of Math. Studies* **67** Princeton: Princeton University Press (1972).

[Si] Silverman, J.: The arithmetic of elliptic curves, *Graduate Texts in Math.* **106**, New York: Springer-Verlag (1986).

[T1] Tate, J.: Duality theorems in Galois cohomology over number fields, *Proc. Intern. Cong. Math.* Stockholm (1962) 234–241.

[T2] ______: Global class field theory. In: Algebraic Number Theory, J. W. S. Cassels and A. Frohlich, eds. London: Academic Press (1967) 162–203.

[T3] ______: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable (IV), *Lecture Notes in Math.* **476**, New York: Springer-Verlag (1975) 33–52.

[T4] ______: Relations between K_2 and Galois cohomology, *Invent. math.* **36** (1976) 257–274.

[T5] ______: Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$, *Prog. in Math.* **47**, Boston: Birkhäuser (1984).

[Th] Thaine, F.: On the ideal class groups of real abelian number fields, *Annals of Math.* **128** (1988) 1–18.

[Wa] Washington, L.: Introduction to cyclotomic fields, *Graduate Texts in Math.* **83**, New York: Springer-Verlag (1982).

[Wi] Wiles, A.: Higher explicit reciprocity laws, *Annals of Math.* **107** (1978) 235–254.

Notation Index

Subject Index