Contemporary Mathematics

# Introduction to Kolyvagin systems

Barry Mazur and Karl Rubin

## Introduction

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

Kolyvagin's method proceeds in three steps. The first step is to establish an Euler system as input to the machine. The second step gives as intermediate output a new collection of cohomology classes, which Kolyvagin calls "derivative" classes, with coefficients in certain quotient Galois modules. The third step uses this system of derivative classes to obtain an upper bound on the size of the dual Selmer group.

In [**MR**] we showed that Kolyvagin's systems of derivative classes satisfy even stronger interrelations than had previously been recognized. A system of cohomology classes satisfying these stronger interrelations, which we call a Kolyvagin system, has an interesting rigid structure which in many ways resembles (an enriched version of) the "leading term" of an $L$-function. See [**MR**], especially the introduction, for an explanation of what we mean by this. By making use of the extra rigidity, we prove in [**MR**] that Kolyvagin systems exist for many interesting representations for which no Euler system is known, and further that there are Kolyvagin systems for these representations which give rise to exact formulas for the size of the dual Selmer group, rather than just upper bounds.

The purpose of this paper is to present an introduction to the theory of Kolyvagin systems by describing in detail one of its simplest and most concrete settings. Namely, we take the Galois module $T$ to be a twist of the group $\boldsymbol{\mu}_{p^k}$ of $p^k$-th roots of unity by a Dirichlet character of conductor $p$, and then the dual Selmer group is a Galois-eigenspace in the ideal class group of the cyclotomic field $\mathbf{Q}(\boldsymbol{\mu}_p)$. For this $T$ there is an Euler system made from cyclotomic units, and we will see that every Kolyvagin system is a multiple of the one produced by Kolyvagin's machinery, a fact essentially equivalent to Iwasawa's main conjecture. We hope that removing the extra layers of notation and hypotheses that occur in the general case will make

2000 *Mathematics Subject Classification.* Primary 11R42, 11R29, 11R18; Secondary 11R34, 11G40, 11F80.

Both authors partially supported by the National Science Foundation.

the main ideas more transparent. The results in this cyclotomic setting have analogues for more general $p$-adic representations $T$, and we will discuss the general case briefly in §6.

## 1. The cyclotomic unit Euler system

Fix once and for all an odd prime $p$ and a power $p^k$ of $p$. Let $F = \mathbf{Q}(\boldsymbol{\mu}_p)$, the field of $p$-th roots of unity, and $\mathcal{O} = \mathbf{Z}[\boldsymbol{\mu}_p]$, its ring of integers. Define

$$\mathcal{P} = \{\text{rational primes } \ell \equiv 1 \pmod{p^k}\},$$
$$\mathcal{N} = \{\text{squarefree products of primes } \ell \in \mathcal{P}\}.$$

For every $\ell \in \mathcal{P} \cup \{p\}$ fix a primitive $\ell$-th root of unity $\zeta_\ell$, and if $n \in \mathcal{N}$ define a primitive $np$-th root of unity $\zeta_{np} = \prod_{\ell | np} \zeta_\ell$. As is well known, $1 - \zeta_{np} \in \mathbf{Z}[\boldsymbol{\mu}_{np}]^\times$ if $n \in \mathcal{N}$ is different from 1, and

$$\mathbf{N}_{F(\boldsymbol{\mu}_{n\ell})/F(\boldsymbol{\mu}_n)}(1 - \zeta_{np\ell}) = (1 - \zeta_{np})^{\mathrm{Fr}_\ell - 1} \tag{1}$$

where $\mathrm{Fr}_\ell$ is the Frobenius automorphism of $\ell$ in $\mathrm{Gal}(F(\boldsymbol{\mu}_n)/\mathbf{Q})$, the automorphism which sends $\zeta_{np}$ to $\zeta_{np}^\ell$.

Let $\Delta = \mathrm{Gal}(F/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$. If $n \in \mathcal{N}$ then we can identify $\Delta$ with $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{np})/\mathbf{Q}(\boldsymbol{\mu}_n)) \subset \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{np})/\mathbf{Q})$, so, for example, $\mathbf{Z}[\boldsymbol{\mu}_{np}]^\times$ is a $\mathbf{Z}[\Delta]$-module.

Fix a character $\chi : \Delta \to \mathbf{Z}_p^\times$. If $M$ is a $\mathbf{Z}_p[\Delta]$-module, we write

$$M^\chi = \{m \in M : \delta m = \chi(\delta) m \text{ for every } \delta \in \Delta\},$$

the "$\chi$-eigenspace" for the action of $\Delta$. If $M$ is a $\mathbf{Z}[\Delta]$-module then we write $M^\chi = (\varprojlim M/p^i M)^\chi$ (which coincides with the previous definition when $M$ is a $\mathbf{Z}_p$-module).

For every $n \in \mathcal{N}$ define $(1-\zeta_{np})^\chi$ to be the projection of $1-\zeta_{np}$ into $(F(\boldsymbol{\mu}_n)^\times)^\chi$. The relation (1) makes the collection $\{(1-\zeta_{np})^\chi : n \in \mathcal{N}\}$ an Euler system,[1] which we call the cyclotomic unit Euler system attached to $\chi$.

If $n \in \mathbf{Z}$ we will often write $M/n$ as an abbreviation for $M/nM$, so, for example, $F^\times/n = F^\times/(F^\times)^n$.

## 2. The cyclotomic unit Kolyvagin system for $\boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$

Kolyvagin's machine takes as input the cyclotomic unit Euler system attached to $\chi$, and gives as output an upper bound on the order of $A_F^\chi$, the $\chi$-component of the $p$-part $A_F$ of the ideal class group of $F$. As an essential intermediate step Kolyvagin's construction produces a collection of "derivative classes"

$$\{\kappa_n^{\mathrm{cycl}} \in (F^\times/p^k)^\chi : n \in \mathcal{N}\}.$$

The classes $\kappa_n^{\mathrm{cycl}}$ are a modified version of the classes defined in [**Ko**] or [**Ru1**] §2. See the Appendix for the definition. We content ourselves here with recording the essential properties of these classes.

For every $\ell \in \mathcal{P}$ fix a generator $\sigma_\ell$ of $\mathbf{F}_\ell^\times$, where as usual $\mathbf{F}_\ell$ denotes the finite field with $\ell$ elements. (The construction of the $\kappa_n^{\mathrm{cycl}}$ will depend on these choices. The choices could be removed, at the expense of carrying extra notation. For the

[1] See [**Ru3**] §§2.1 and 3.2. The definition of Euler system in [**Ko**] or [**Ru1**] included a congruence relation in addition to the norm relation above. However, the congruence is a consequence of the norm relation; see for example §4.8 of [**Ru3**].

canonical construction without these choices, see [**MR**].) If $\ell \in \mathcal{P}$ then $\ell$ splits completely in $F$, so if $\lambda$ is a prime of $F$ above $\ell$ then $\mathcal{O}/\lambda = \mathbf{F}_\ell$. We write $F_\lambda$ (resp. $\mathcal{O}_\lambda$) for the completion of $F$ (resp. $\mathcal{O}$) at such a $\lambda$, and we define the discrete logarithm map $\log_\lambda$ to be the composition

$$\begin{tikzcd}
\log_\lambda : \mathcal{O}_\lambda^\times \arrow[r] & (\mathcal{O}/\lambda)^\times \arrow[r, "\sim"] & \mathbf{F}_\ell^\times \arrow[r, "\sim"] & \mathbf{Z}/(\ell-1)\mathbf{Z}. \\
 & & \sigma_\ell^i \arrow[r, mapsto] & i
\end{tikzcd}$$

THEOREM 2.1 ([**Ko**], [**Ru1**] Proposition 2.4). *For every* $n \in \mathcal{N}$*,*

(i) $\kappa_1^{\mathrm{cycl}}$ *is the image of* $1-\zeta_p$ *in* $(F^\times/p^k)^\chi$*,*
(ii) $\mathrm{ord}_\lambda(\kappa_n^{\mathrm{cycl}}) \equiv 0 \pmod{p^k}$ *if* $\lambda$ *is a prime of* $F$ *not dividing* $n$*,*
(iii) $\mathrm{ord}_\lambda(\kappa_n^{\mathrm{cycl}}) \equiv \log_\lambda(\kappa_{n/\ell}^{\mathrm{cycl}}) \pmod{p^k}$ *if* $\lambda \mid \ell$ *and* $\ell \mid n$*.*

Properties (i)–(iii) of Theorem 2.1 are all that is needed (see [**Ru1**]) to apply Kolyvagin's machinery to bound ideal class groups. Namely, each $\kappa_n^{\mathrm{cycl}}$ gives a principal ideal (modulo $p^k$-th powers of ideals). One can view a principal ideal as giving a relation among the generators (the classes of prime ideals) in $A_F^\chi$, and by cleverly choosing a good sequence of integers $n$, one can produce enough relations to bound $(A_F/p^k)^\chi$.

REMARK 2.2. It is natural to ask whether the properties (i)–(iii) of Theorem 2.1 determine all of the $\kappa_n^{\mathrm{cycl}}$, and in general they do *not.* If one knows the $\kappa_d^{\mathrm{cycl}}$ for all $d$ properly dividing $n$, then these properties determine $\kappa_n^{\mathrm{cycl}}$ modulo the group

$$\{\alpha \in (F^\times/p^k)^\chi : \ \mathrm{ord}_\lambda \alpha \equiv 0 \ (\mathrm{mod}\ p^k) \text{ for every } \lambda\}.$$

This group is an extension of $(A_F/p^k)^\chi$ by $(\mathcal{O}^\times/p^k)^\chi$, which in general is nontrivial.

However, it turns out that Kolyvagin's derivative classes satisfy an additional property, which adds enough "rigidity" so that one $\kappa_n^{\mathrm{cycl}}$ (for a properly chosen $n$, see Theorem 5.6 below) determines all the others. We now describe this additional property.

DEFINITION 2.3. The exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{Z}_\ell^\times/p^k \arrow[r] & \mathbf{Q}_\ell^\times/p^k \arrow[r, "\mathrm{ord}_\ell"] & \mathbf{Z}/p^k\mathbf{Z} \arrow[r] \arrow[l, bend left, "\ell^i \longleftarrow\!\shortmid\, i"'] & 0
\end{tikzcd}$$

has a natural splitting, obtained by mapping $i \in \mathbf{Z}/p^k\mathbf{Z}$ to $\ell^i \in \mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^k}$. Define the *transverse subgroup* $(\mathbf{Q}_\ell^\times/p^k)_{\mathrm{tr}}$ to be the subgroup of $\mathbf{Q}_\ell^\times/p^k$ generated by $\ell$, so

$$\mathbf{Q}_\ell^\times/p^k = \mathbf{Z}_\ell^\times/p^k \oplus (\mathbf{Q}_\ell^\times/p^k)_{\mathrm{tr}}.$$

For every $\ell \in \mathcal{P}$ write

$$\mathcal{O}_\ell = \mathcal{O} \otimes \mathbf{Z}_\ell = \oplus_{\lambda|\ell}\mathcal{O}_\lambda, \qquad F_\ell = F \otimes \mathbf{Q}_\ell = \oplus_{\lambda|\ell} F_\lambda,$$

and if $\alpha \in F$ write $\alpha_\ell$ for the image of $\alpha$ in $F_\ell$. Since $\ell$ splits completely in $F/\mathbf{Q}$, choosing a prime $\lambda$ of $F$ above $\ell$ gives isomorphisms

$$(F_\ell)^\chi \cong \mathbf{Q}_\ell, \qquad \mathcal{O}_\ell^\chi \cong \mathbf{Z}_\ell. \tag{2}$$

Define $(F_\ell^\times/p^k)_{\mathrm{tr}}^\chi$ to be the subgroup of $(F_\ell^\times/p^k)^\chi$ corresponding to $(\mathbf{Q}_\ell^\times/p^k)_{\mathrm{tr}}$ under the isomorphism (2). (Choosing a different prime $\lambda^\sigma$ multiplies the isomorphisms (2) by $\chi^{-1}(\sigma)$, which does not affect this definition.) Then we have a splitting

$$(F_\ell^\times/p^k)^\chi \cong (\mathcal{O}_\ell^\times/p^k)^\chi \oplus (F_\ell^\times/p^k)_{\mathrm{tr}}^\chi \tag{3}$$

of $(F_\ell^\times/p^k)^\chi$ into a product of two cyclic groups of order $p^k$.

THEOREM 2.4 ([**MR**] Theorem 3.2.4). *If $n \in \mathcal{N}$ and $\ell \mid n$, then $(\kappa_n^{\mathrm{cycl}})_\ell \in (F_\ell^\times/p^k)^\chi_{\mathrm{tr}}$.*

See the Appendix for the proof of Theorem 2.4.

DEFINITION 2.5. For $n \in \mathcal{N}$ define a subgroup $H(n)$ of $(F^\times/p^k)^\chi$ by

$$H(n) = \{\alpha \in (F^\times/p^k)^\chi : \begin{cases} \alpha_\ell \in (\mathcal{O}_\ell^\times/p^k)^\chi & \text{if } \ell \nmid n, \\ \alpha_\ell \in (F_\ell^\times/p^k)^\chi_{\mathrm{tr}} & \text{if } \ell \mid n \end{cases}\}.$$

As we will see below in (4), $H(1)$ is related to the ideal class group of $F$. For arbitrary $n$ we view $H(n)$ as a modified "Selmer group", where we have changed the defining local condition at primes dividing $n$.

DEFINITION 2.6. If $\ell \in \mathcal{P}$ we define the isomorphism

$$\phi_\ell^{\mathrm{fs}} : (\mathcal{O}_\ell^\times/p^k)^\chi \xrightarrow{\sim} (F_\ell^\times/p^k)^\chi_{\mathrm{tr}}$$

to be the map induced via (2) by the isomorphism $\mathbf{Z}_\ell^\times/p^k \to (\mathbf{Q}_\ell^\times/p^k)_{\mathrm{tr}}$ which sends a lift of $\sigma_\ell$ to $\ell$. In other words, $\phi_\ell^{\mathrm{fs}}$ is the unique map which makes the diagram of isomorphisms

$$\begin{tikzcd}
(\mathcal{O}_\ell^\times/p^k)^\chi \arrow[rr, "\phi_\ell^{\mathrm{fs}}"] \arrow[dr, "\log_\lambda"'] & & (F_\ell^\times/p^k)^\chi_{\mathrm{tr}} \arrow[dl, "\mathrm{ord}_\lambda"] \\
& \mathbf{Z}/p^k\mathbf{Z} &
\end{tikzcd}$$

commute for every prime $\lambda$ of $F$ above $\ell$.

With notation as above, we can combine Theorems 2.1 and 2.4 to obtain the following proposition.

PROPOSITION 2.7. *For every $n \in \mathcal{N}$,*

(i) *$\kappa_1^{\mathrm{cycl}}$ is the image of $1 - \zeta_p$ in $(F^\times/p^k)^\chi$,*
(ii) *$\kappa_n^{\mathrm{cycl}} \in H(n)$,*
(iii) *if $\ell$ is a prime dividing $n$ then $(\kappa_n^{\mathrm{cycl}})_\ell = \phi_\ell^{\mathrm{fs}}((\kappa_{n/\ell}^{\mathrm{cycl}})_\ell)$.*

REMARK 2.8. Returning to the situation of Remark 2.2, we see now that if $\kappa_d^{\mathrm{cycl}}$ is known for every $d$ properly dividing $n$, then Proposition 2.7 determines $\kappa_n^{\mathrm{cycl}}$ modulo

$$\{\alpha \in (F^\times/p^k)^\chi : \alpha_\ell \in (\mathcal{O}_\ell^\times/p^k)^\chi \text{ for every prime } \ell, \text{ and } \alpha_\ell \equiv 1 \pmod{\ell} \text{ if } \ell \mid n\}.$$

For sufficiently divisible $n$, this group is trivial.

## 3. The Selmer sheaf attached to $\boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$

DEFINITION 3.1. Let $\mathcal{X}$ be the graph whose set of vertices is $\mathcal{N}$ and whose edges join vertices $n$ and $n\ell$ when $\ell$ is prime. A *sheaf* on $\mathcal{X}$ consists of the following data:

- a stalk (an abelian group) over every vertex,
- a stalk (an abelian group) over every edge,
- if $e$ is an edge and $v$ is one of its vertices, a homomorphism from the stalk over $v$ to the stalk over $e$.

We define the *Selmer sheaf* $\mathcal{H}$ on $\mathcal{X}$ as follows.

- The stalk at the vertex $n$ is $H(n) \subset (F^\times/p^k)^\chi$.
- If $e$ is the edge joining $n$ and $n\ell$, the stalk at $e$ is $(F_\ell/p^k)^\chi_{\mathrm{tr}}$, which we will also denote by $H(e)$.
- If $e$ is the edge joining $n$ and $n\ell$, we define $\psi^e_n, \psi^e_{nl}$ by

$$\begin{tikzcd} H(n) \arrow[r, "\psi^e_n"] & H(e) & H(n\ell) \arrow[l, "\psi^e_{nl}"'] \\ \alpha \arrow[r, mapsto] & \phi^{\mathrm{fs}}_\ell(\alpha_\ell),\ \beta_\ell & \beta \arrow[l, mapsto] \end{tikzcd}$$

A *global section* of $\mathcal{H}$ is a collection $\{\kappa_n \in H(n) : n \in \mathcal{N}\}$ such that if $n$ and $n\ell$ are vertices, and $e$ is an edge joining them, then $\psi^e_n(\kappa_n) = \psi^e_{nl}(\kappa_{n\ell})$ in $H(e)$.

Definition 3.2. A *Kolyvagin system* (for $\boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$) is a global section of $\mathcal{H}$. Equivalently, a Kolyvagin system is a collection $\{\kappa_n \in H(n) : n \in \mathcal{N}\}$ such that whenever $n, n\ell \in \mathcal{N}$ we have $\phi^{\mathrm{fs}}((\kappa_n)_\ell) = (\kappa_{n\ell})_\ell$ in $(F_\ell^\times/p^k)^\chi_{\mathrm{tr}}$.

The following proposition is immediate from Proposition 2.7.

Proposition 3.3. *The collection $\{\kappa^{\mathrm{cycl}}_n : n \in \mathcal{N}\}$ is a Kolyvagin system.*

Definition 3.4. Let **KS** denote the group of all Kolyvagin systems, and let $\boldsymbol{\kappa}^{\mathrm{cycl}} \in \mathbf{KS}$ denote the cyclotomic unit Kolyvagin system $\{\kappa^{\mathrm{cycl}}_n : n \in \mathcal{N}\}$.

## 4. The modified Selmer groups attached to $\boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$

Suppose from now on that $\chi$ is not the trivial character, and also not the Teichmüller character $\omega$ giving the action of $\Delta$ on $\boldsymbol{\mu}_p$. Define an invariant

$$r = r(\chi) = \begin{cases} 1 & \text{if } \chi \text{ is even,} \\ 0 & \text{if } \chi \text{ is odd.} \end{cases}$$

Then $(\mathcal{O}^\times/p^k)^\chi$ is free of rank $r$ over $\mathbf{Z}/p^k\mathbf{Z}$, and it is a standard exercise in algebraic number theory to show that there is an exact sequence

$$0 \longrightarrow (\mathcal{O}^\times/p^k)^\chi \longrightarrow H(1) \longrightarrow A^\chi_F[p^k] \longrightarrow 0. \tag{4}$$

From now on we will write our multiplicative groups additively. The following proposition is proved in [**MR**]. It follows from the exact sequence above when $n = 1$, and it is vacuous when $r = 0$.

Proposition 4.1 ([**MR**] Theorem 4.1.13). *For every $n \in \mathcal{N}$, $H(n)$ contains a free $\mathbf{Z}/p^k\mathbf{Z}$-submodule of rank $r$.*

Definition 4.2. For $n \in \mathcal{N}$ define $\lambda^*(n) = \dim_{\mathbf{F}_p} H(n)[p] - r$. We say that $n$ is a *core vertex* if $\lambda^*(n) = 0$. Equivalently, $n$ is a core vertex if and only if $H(n) \cong (\mathbf{Z}/p^k\mathbf{Z})^r$.

The next proposition is proved using (for (ii)) global duality and the Cebotarev Theorem.

Proposition 4.3 ([**MR**] Lemma 4.1.7 and Proposition 3.6.1).

(i) *If $n, n\ell \in \mathcal{N}$ then $|\lambda^*(n) - \lambda^*(n\ell)| \le 1$.*

(ii) *If $n \in \mathcal{N}$ and $\lambda^*(n) > 0$, then there is are infinitely many $\ell \in \mathcal{P}$ prime to $n$ such that $\lambda^*(n\ell) = \lambda^*(n) - 1$.*

Corollary 4.4. *If $n \in \mathcal{N}$ and $\lambda^*(n) = t$, then there is a path of length $t$ in the graph $\mathcal{X}$ from $n$ to a core vertex.*

Definition 4.5. Suppose $A$ is a finite abelian group and $d \geq 0$. We define the *$d$-stub* of $A$ to be the (unique) maximal subgroup $A' \subset A$ of the form $[A : C]A$, where $C$ runs through subgroups of $A$ generated by $d$ elements.

If $d = 0$ then $A' = 0$, and if $A$ can be generated by $d$ elements then $A' = A$. In general $[A : C]A \subset C$, so $A'$ can be generated by $d$ elements. In particular if $d = 1$ then $A'$ is a canonical cyclic subgroup of $A$.

If $n \in \mathcal{N}$ we define $H'(n) \subset H(n)$ to be the $r$-stub of $H(n)$ where $r = r(\chi)$ is 0 or 1 as above. Concretely (using Proposition 4.1)

$$H'(n) = \tfrac{|H(n)|}{p^{kr}} H(n).$$

If $\chi$ is odd then $r = 0$ so $H'(n) = 0$, and if $\chi$ is even then $H'(n)$ is cyclic. If $n$ is a core vertex then $H'(n) = H(n)$.

When $n = 1$ we see from (4) that

$$H'(1) = |A_F^\chi[p^k]| \cdot H(1). \tag{5}$$

The following theorem is central to the theory of Kolyvagin systems. It incorporates the "Kolyvagin induction", and allows one to use a Kolyvagin system to bound ideal class groups.

Theorem 4.6 ([**MR**] Theorem 4.4.1). *If $\{\kappa_n\}$ is a Kolyvagin system then $\kappa_n \in H'(n)$ for every $n$.*

Remark about the proof. The proof in [**MR**] is by induction on $\lambda^*(n)$. When $\lambda^*(n) = 0$ (i.e., $n$ is a core vertex), we have $H'(n) = H(n)$ and there is nothing to prove. When $\lambda^*(n) > 0$ one can use Proposition 4.3(ii) to choose a prime $\ell$ with $\lambda^*(n\ell) = \lambda^*(n) - 1$, and then use that (by induction) $\kappa_{n\ell} \in H'(n\ell)$. See [**MR**]. □

Since $H'(n) = 0$ for every $n$ when $r = 0$, we have the following immediate corollary of Theorem 4.6.

Corollary 4.7. *If $r = 0$ then there are no nonzero Kolyvagin systems.*

Remark 4.8. If $\chi$ is odd and $\chi \neq \omega$, then the cyclotomic units $(1 - \zeta_{np})^\chi$ used to define the cyclotomic unit Euler system are all 1, and hence so are the $\kappa_n \in (F^\times/p^k)^\chi$.

The following corollary is the standard application of Kolyvagin's machinery to ideal class groups.

Corollary 4.9 ([**Ko**], [**Ru1**] §4, [**MR**] Corollary 4.4.5). *If $\{\kappa_n\}$ is a Kolyvagin system for $\boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$ then*

$$|A_F^\chi[p^k]| \leq \max\{p^i : \kappa_1 \in (F^\times)^{p^i}/(F^\times)^{p^k}\}.$$

Proof. By Theorem 4.6 and (5), we have

$$\kappa_1 \in H'(1) = |A_F^\chi[p^k]| \cdot H(1)$$

and the corollary follows. □

## 5. The stub subsheaf

Definition 5.1. We define the stub subsheaf $\mathcal{H}' \subset \mathcal{H}$ by the following data.

- The stalk at the vertex $n$ is $H'(n)$.
- If $e$ is the edge joining $n$ and $n\ell$, the stalk $H'(e)$ at $e$ is $\psi_n^e(H'(n)) \subset H(e)$.
- If $e$ is an edge and $n$ is one of its vertices, the map $\bar{\psi}_n^e : H'(n) \to H'(e)$ is the restriction of $\psi_n^e$.

We use here the fact ([**MR**] Lemma 4.1.7(iii)) that if $e$ is the edge joining $n, n\ell$ then $\psi_n^e(H'(n)) = \psi_{nl}^e(H'(n\ell))$. As a consequence, all the vertex-to-edge maps $\bar{\psi}_n^e$ are surjective.

The following theorem is just a restatement of Theorem 4.6.

Theorem 5.2. *Every global section of the Selmer sheaf $\mathcal{H}$ is actually a global section of the stub subsheaf $\mathcal{H}'$.*

Definition 5.3. If $n$ and $m$ are vertices of $\mathcal{X}$, a *surjective path $P$* from $n$ to $m$ is a (directed) path

$$n = n_0 \xrightarrow{e_1} n_1 \xrightarrow{e_2} n_2 \xrightarrow{e_3} \cdots \xrightarrow{e_k} n_k = m,$$

where $e_i$ is the edge joining $n_{i-1}$ and $n_i$, such that for every $i$, $1 \le i \le n$, the map $\bar{\psi}_{n_i}^{e_i} : H'(n_i) \to H'(e_i)$ is an isomorphism. (We place no restriction on the map $\bar{\psi}_{n_{i-1}}^{e_i} : H'(n_{i-1}) \to H'(e_i)$, which is in any case surjective.)

If $P$ is such a surjective path from $n$ to $m$, then (since all the $\bar{\psi}_n^e$ are surjective) we have

$$\begin{tikzcd} \cdots H'(n_{i-1}) \arrow[r, two heads, "\bar{\psi}_{n_{i-1}}^{e_i}"'] & H'(e_i) & H'(n_i) \arrow[l, "\sim", "\bar{\psi}_{n_i}^{e_i}"'] \arrow[r, two heads, "\bar{\psi}_{n_i}^{e_{i+1}}"'] & H'(e_{i+1}) & H'(n_{i+1}) \cdots \arrow[l, "\sim", "\bar{\psi}_{n_{i+1}}^{e_{i+1}}"'] \end{tikzcd}$$

and so $P$ induces a surjective homomorphism $\psi_P : H'(n) \twoheadrightarrow H'(m)$.

The next two theorems, along with Theorem 5.2, summarize the “rigidity” of our Selmer sheaf. Theorem 5.5 is due to Benjamin Howard.

Theorem 5.4 ([**MR**] Theorem 4.3.4). *Suppose $n$ is a core vertex. Then for every vertex $m \in \mathcal{N}$, there is a surjective path from $n$ to $m$.*

Theorem 5.5 (Howard, Appendix B of [**MR**]). *If $m$ and $n$ are vertices of $\mathcal{X}$, and $P, Q$ are two surjective paths from $m$ to $n$, then the two maps $\psi_P, \psi_Q \in \mathrm{Hom}(H'(m), H'(n))$ are equal.*

*More generally, if $m$, $n$, and $n\ell$ are vertices, $e$ is the edge joining $n$ and $n\ell$, $P$ is a surjective path from $m$ to $n$ and $Q$ is a surjective path from $m$ to $n\ell$, then*

$$\psi_n^e \circ \psi_P = \psi_{nl}^e \circ \psi_Q \quad \in \mathrm{Hom}(H'(m), H'(e)).$$

Because of Theorem 5.5 we say that $\mathcal{H}'$ has *trivial monodromy.*

Recall that **KS** is the group of Kolyvagin systems attached to $\boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$.

Theorem 5.6. *If $n$ is a core vertex, then the map $\mathbf{KS} \to H(n)$ which specializes $\boldsymbol{\kappa} \in \mathbf{KS}$ to $\kappa_n \in H(n)$ is an isomorphism.*

*In other words, $\mathbf{KS}$ is cyclic of order $p^k$ and $\kappa_n$ determines $\kappa_m$ for every vertex $m$.*

Proof. Suppose $\boldsymbol{\kappa} \in \mathbf{KS}$ and $m$ is a vertex of $\mathcal{X}$. By Theorem 5.4 there is a surjective path $P$ from $n$ to $m$, and then by the definition of global section, $\kappa_m = \psi_P(\kappa_n)$. Thus if $\kappa_n = 0$ then $\boldsymbol{\kappa} = 0$, so the map $\mathbf{KS} \to H(n)$ is injective.

On the other hand, suppose $c \in H(n)$ and $m$ is a vertex. By Theorem 5.4 there is a surjective path $P$ from $n$ to $m$, and we define $\kappa_m = \psi_P(c)$. By Theorem 5.5 this is independent of the choice of $P$, and defines a global section. We have $\kappa_n = c$, so the map $\mathbf{KS} \to H(n)$ is surjective as well. □

We say that $\boldsymbol{\kappa} \in \mathbf{KS}$ is *primitive* if $\boldsymbol{\kappa}$ generates $\mathbf{KS}$.

Theorem 5.7. *Suppose $\boldsymbol{\kappa} \in \mathbf{KS}$. The following are equivalent.*

(i) *$\boldsymbol{\kappa}$ is primitive.*
(ii) *$\kappa_n$ generates $H'(n)$ for every $n \in \mathcal{N}$.*
(iii) *$\kappa_n$ generates $H'(n)$ for some $n \in \mathcal{N}$ with $H(n) \neq 0$.*

Proof. This follows from the proof of Theorem 5.6, since the maps $\psi_P$ : $H'(n) \to H'(m)$ induced by a surjective path are surjective. □

Corollary 5.8. *If $\boldsymbol{\kappa} \in \mathbf{KS}$ and $\kappa_1 \neq 0$, then $\boldsymbol{\kappa}$ is primitive if and only if*

$$|A_F^\chi[p^k]| = \max\{p^i : \kappa_1 \in (F^\times)^{p^i}/(F^\times)^{p^k}\}.$$

Proof. Let $p^d = |A_F^\chi[p^k]|$. By Theorem 4.6, (5), and (4),

$$\kappa_1 \in H'(1) = p^d H(1) = ((\mathcal{O}^\times)^{p^d}/(\mathcal{O}^\times)^{p^k})^\chi,$$

and by Theorem 5.7 $\boldsymbol{\kappa}$ is primitive if and only if $\kappa_1$ generates $((\mathcal{O}^\times)^{p^d}/(\mathcal{O}^\times)^{p^k})^\chi$. This proves the corollary. □

Remark 5.9. The results above apply to every Kolyvagin system, and prove the existence of Kolyvagin systems for even characters $\chi$ without making use of the cyclotomic unit Kolyvagin system $\boldsymbol{\kappa}^{\mathrm{cycl}}$ of §2.

Theorem 5.10. *The cyclotomic unit Kolyvagin system is primitive.*

Proof. By Corollary 4.7 we may assume that $\chi$ is even. Suppose first that $k$ is sufficiently large, for example $p^k > |A_F^\chi|$. Theorem 2.1(i) relates $\kappa_1^{\mathrm{cycl}}$ with cyclotomic units. The equality

$$|A_F^\chi[p^k]| = |A_F^\chi| = \max\{p^i : \kappa_1^{\mathrm{cycl}} \in (F^\times)^{p^i}/(F^\times)^{p^k}\},$$

once known as the Gras conjecture, was proved by the first author and Wiles in [**MW**] and then again by Kolyvagin using Corollary 4.9 above and the analytic class number formula. It follows by Corollary 5.8 that $\boldsymbol{\kappa}^{\mathrm{cycl}}$ is primitive.

Using Theorem 5.7, it is easy now to deduce that $\boldsymbol{\kappa}^{\mathrm{cycl}}$ is primitive for every $k$. □

Example 5.11. We conclude this section by illustrating in more detail the special case $k = 1$. This case plays an important role in the proof of Theorem 5.4.

Suppose $k = 1$ and $\chi$ is even, so $r = 1$. If $n$ is a core vertex then $H'(n) = H(n)$ is one-dimensional over $\mathbf{F}_p$, and if $n$ is not a core vertex then $H'(n) = 0$. It follows from Theorem 5.7 that if $\boldsymbol{\kappa} \in \mathbf{KS}$ is nonzero, then $\kappa_n \neq 0$ if and only if $n$ is a core vertex.

Define a subgraph $\mathcal{X}_0$ of $\mathcal{X}$ whose set of vertices is the set $\mathcal{N}_0$ of core vertices of $\mathcal{X}$, and whose edges are the edges $e$ joining $n, n\ell \in \mathcal{N}_0$ such that the maps

$\psi_n^e : H(n) \to H(e)$ and $\psi_{nl}^e : H(n\ell) \to H(e)$ are isomorphisms. Let $\mathcal{H}_0$ be the restriction of the sheaf $\mathcal{H}$ to $\mathcal{X}_0$, or equivalently the restriction of $\mathcal{H}'$ to $\mathcal{X}_0$. Then we can view $\mathcal{H}_0$ as a linear system of one-dimensional $\mathbf{F}_p$-vector spaces over $\mathcal{X}_0$, with isomorphisms between stalks over vertices which are adjacent in $\mathcal{X}_0$.

In this setting, Theorem 5.4 says simply that the graph $\mathcal{X}_0$ is connected. In other words, any two core vertices can be connected by a path in $\mathcal{X}_0$. If $n$ and $m$ are core vertices then a path from $n$ to $m$ induces an isomorphism $\mathcal{H}(n) \xrightarrow{\sim} \mathcal{H}(m)$, and Howard's Theorem 5.5 says that this isomorphism is independent of the path.

## 6. Kolyvagin systems for general Galois representations

In this final section we briefly describe the theory of Kolyvagin systems for more general $p$-adic representations. For the details, see [**MR**].

Keep our fixed prime power $p^k$, and let $R = \mathbf{Z}/p^k\mathbf{Z}$. (More generally, $R$ could be a principal artinian local ring.) Fix a free $R$ module $T$ of finite rank, with a continuous action of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

If $T = \boldsymbol{\mu}_{p^k} \otimes \chi^{-1}$ then we will recover the setting discussed in the previous sections of this paper. Another interesting case is where $T = E[p^k]$ with an elliptic curve $E$ defined over $\mathbf{Q}$.

We associate to $T$ a Selmer group $H(1) \subset H^1(\mathbf{Q}, T)$, defined by local conditions. In other words, for every prime $\ell$ we have a subgroup $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) \subset H^1(\mathbf{Q}_\ell, T)$, and then

$$H(1) = \{c \in H^1(\mathbf{Q}, T) : c_\ell \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) \text{ for every } \ell\}$$

where $c_\ell \in H^1(\mathbf{Q}_\ell, T)$ is the localization of $c$. We require that for all but finitely many $\ell$, $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ is the "unramified subgroup"

$$H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T) = \ker : H^1(\mathbf{Q}_\ell, T) \to H^1(\mathbf{Q}_\ell^{\mathrm{unr}}, T).$$

Define $\mathcal{P}$ to be the set of rational primes $\ell$ satisfying

- $T$ is unramified at $\ell$ (i.e., an inertia group $I_\ell \subset G_{\mathbf{Q}}$ acts trivially on $T$),
- $\ell \equiv 1 \pmod{p^k}$,
- $\det(1 - \mathrm{Fr}_\ell | T) = 0$, where $\mathrm{Fr}_\ell \in G_{\mathbf{Q}}$ is a Frobenius automorphism for $\ell$,
- $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T) = H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T)$.

As in §2 we let $\mathcal{N}$ be the set of squarefree products of primes in $\mathcal{P}$.

Proposition 6.1. *If $\ell \in \mathcal{P}$ then*

$$H^1(\mathbf{Q}_\ell, T) = H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T) \oplus H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$$

*where $H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T) = \ker : H^1(\mathbf{Q}_\ell, T) \to H^1(\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell), T)$. There is a map*

$$\phi_\ell^{\mathrm{fs}} : H^1_{\mathrm{unr}}(\mathbf{Q}_\ell, T) \to H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$$

*which depends only on the choice of a generator of $\mathbf{F}_\ell^\times$.*

If $n \in \mathcal{N}$ we define the modified Selmer group $H(n)$ to be the set of all classes $c \in H^1(\mathbf{Q}, T)$ such that $c_\ell \in H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ if $\ell \nmid n$, and $c_\ell \in H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$ if $\ell \mid n$, with $H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$ as in Proposition 6.1.

Definition 6.2. As in §3 we define a graph $\mathcal{X}$ with vertices $\mathcal{N}$ and edges joining vertices $n, n\ell$, and we define a Selmer sheaf $\mathcal{H}$ on $\mathcal{X}$ by

- the stalk at the vertex $n$ is $H(n)$,
- the stalk at the edge $e$ joining $n, n\ell$ is $H(e) = H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$,

- the vertex-to-edge maps are given by localization and the maps $\phi_\ell^{\mathrm{fs}}$ of Proposition 6.1.

A *Kolyvagin system* for $T$ (and the given collection of local Selmer conditions) is a global section of the sheaf $\mathcal{H}$. In other words, a Kolyvagin system is a collection $\{\kappa_n \in H(n) : n \in \mathcal{N}\}$ such that if $n, n\ell \in \mathcal{N}$ then $\phi_\ell^{\mathrm{fs}}((\kappa_n)_\ell) = (\kappa_{n\ell})_\ell$.

Remark 6.3. In [**MR**] we prove (Theorem 3.2.4) that if one starts with an Euler system for $T$ (in the sense of [**Ru3**]) and applies Kolyvagin's derivative construction, the resulting collection of derivative classes is a Kolyvagin system for $T$.

Definition 6.4. Let $T^* = \mathrm{Hom}(T, \boldsymbol{\mu}_{p^k})$ be the Cartier dual of $T$. For every $n \in \mathcal{N}$ we can define a modified Selmer group $H^*(n) \subset H^1(\mathbf{Q}, T^*)$ using the "dual local conditions". I.e., $H^*(n)$ is the set of all classes $c \in H^1(\mathbf{Q}, T^*)$ satisfying

- $c_\ell$ is orthogonal to $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$ if $\ell \nmid n$,
- $c_\ell$ is orthogonal to $H^1_{\mathrm{tr}}(\mathbf{Q}_\ell, T)$ if $\ell \mid n$,

orthogonal under the local Tate pairing $H^1(\mathbf{Q}_\ell, T) \times H^1(\mathbf{Q}_\ell, T^*) \to \mathbf{Z}/p^k\mathbf{Z}$.

For the strongest results we need to make some technical assumptions on $T$ and the local Selmer conditions $H^1_{\mathcal{F}}(\mathbf{Q}_\ell, T)$. Rather than formulate these conditions here, we will say simply that from now on we assume hypotheses (H.0) through (H.6) of §3.5 of [**MR**], and we refer the reader to [**MR**] for details.

Theorem 6.5. *With notation and hypotheses as above, there is an integer $r = r(T) \in \mathbf{Z}$ such that for every $n \in \mathcal{N}$ there is a noncanonical isomorphism*

$$H(n) \cong (\mathbf{Z}/p^k\mathbf{Z})^r \oplus H^*(n) \qquad \text{if } r \geq 0,$$
$$H(n) \oplus (\mathbf{Z}/p^k\mathbf{Z})^{-r} \cong H^*(n) \qquad \text{if } r \leq 0.$$

Definition 6.6. Define $\chi(T) = \max\{0, r\}$ with $r = r(T)$ as in Theorem 6.5.

For every $n \in \mathcal{N}$ define the *stub subgroup* $H'(n) = |H^*(n)| \cdot H(n)$. As in Definition 4.5 we have $H'(n) = 0$ if $\chi(T) = 0$, and in general $H'(n) \cong (\mathbf{Z}/p^d\mathbf{Z})^{\chi(T)}$ for some $d \leq k$.

Let $\mathbf{KS}(T)$ denote the group of Kolyvagin systems for $T$.

Theorem 6.7. (i) *If $\chi(T) = 0$ then $\mathbf{KS}(T) = 0$.*
(ii) *If $\chi(T) = 1$ then $\mathbf{KS}(T)$ is free of rank one over $\mathbf{Z}/p^k\mathbf{Z}$.*
(iii) *If $\chi(T) > 1$ then $\mathbf{KS}(T)$ contains a free $\mathbf{Z}/p^k\mathbf{Z}$-module of rank $d$ for every $d$.*

As with Theorem 5.6, Theorem 6.7 is proved in [**MR**] by studying the stub subsheaf of $\mathcal{H}$, and using a result of Howard from Appendix B of [**MR**]. We also have the following analogue of Theorems 4.6 and 5.7.

Theorem 6.8. *Suppose $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$. Then $\kappa_n \in H'(n)$ for every $n$, and the following are equivalent.*
(i) *$\boldsymbol{\kappa}$ generates $\mathbf{KS}(T)$.*
(ii) *$\kappa_n$ generates $H'(n)$ for every $n \in \mathcal{N}$.*
(iii) *$\kappa_n$ generates $H'(n)$ for some $n \in \mathcal{N}$ with $H(n) \neq 0$.*

Corollary 6.9. *Suppose $\chi(T) = 1$ and $\boldsymbol{\kappa} \in \mathbf{KS}(T)$. Then*

$$|H^*(1)| \leq \max\{p^i : \kappa_1 \in p^i H^1(\mathbf{Q}, T)\},$$

*with equality if $\kappa_1 \neq 0$ and $\boldsymbol{\kappa}$ generates $\mathbf{KS}(T)$.*

Proof. As with Corollaries 4.9 and 5.8, the inequality (resp., the equality) follows from the fact that $\kappa_1$ belongs to (resp., generates) $H'(1) = |H^*(1)| \cdot H(1)$ by Theorem 6.8. □

Remark 6.10. When $\chi(T) > 1$, it is still true under additional hypotheses that if $\boldsymbol{\kappa}$ is a Kolyvagin system then $\kappa_n \in H'(n)$ for every $n$. In those cases it follows, exactly as in Corollary 6.9, that $|H^*(1)| \leq \max\{p^i : \kappa_1 \in p^i H^1(\mathbf{Q}, T)\}$.

## Appendix

Keep the notation of §1. In this appendix we give the definition of the classes $\kappa_n^{\mathrm{cycl}} \in (F^\times/p^k)^\chi$ and prove Theorem 2.4. We will follow also the notation and setting of [**Ru1**].

For every $n \in \mathcal{N}$ write $G_n = \mathrm{Gal}(F(\boldsymbol{\mu}_n)/F) \cong \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_n)/\mathbf{Q})$, and write $\mathbf{N}_n$ for the norm operator

$$\mathbf{N}_n = \sum_{\tau \in G_n} \tau \in \mathbf{Z}[G_n].$$

If $mn \in \mathcal{N}$ we will identify $G_n$ with $\mathrm{Gal}(F(\boldsymbol{\mu}_{mn})/F(\boldsymbol{\mu}_m)) \subset G_{mn}$. With this identification there is a natural isomorphism $G_n = \prod_{\ell \mid n} G_\ell$ (product over primes $\ell$ dividing $n$), and $\mathbf{N}_n = \prod_{\ell \mid n} \mathbf{N}_\ell \in \mathbf{Z}[G_n]$. Recall that if $q \in \mathcal{P}$ we have fixed a generator $\sigma_q$ of $\mathbf{F}_q^\times$. We can view $\sigma_q$ as a generator of $G_q$ via the canonical isomorphism $G_q \cong \mathbf{F}_q^\times$, and we define

$$\mathbf{D}_q = \sum_{i=1}^{q-2} i\sigma_q^i \in \mathbf{Z}[G_q].$$

This "operator" is constructed to satisfy the identity

$$(\sigma_q - 1)\mathbf{D}_q = (q-1) - \mathbf{N}_q \tag{6}$$

in $\mathbf{Z}[G_q]$. For $n \in \mathcal{N}$ we define $\mathbf{D}_n = \prod_{q \mid n} \mathbf{D}_q \in \mathbf{Z}[G_n]$. If $q \mid n$ we write $\mathrm{Fr}_q$ for the Frobenius of $q$, and we view $\mathrm{Fr}_q \in G_{n/q} \subset G_n$. In other words, $\mathrm{Fr}_q$ is a Frobenius element for $q$ in $\mathrm{Gal}(F(\boldsymbol{\mu}_n)/F(\boldsymbol{\mu}_q))$.

To avoid ambiguity we will use the following notation. If $x \in F(\boldsymbol{\mu}_n)^\times$ and $\rho \in \mathbf{Z}[\mathrm{Gal}(F(\boldsymbol{\mu}_n)/\mathbf{Q})]$, then we will denote the action of $\rho$ on $x$ by $\rho \cdot x$. Thus if $a \in \mathbf{Z}$ we have $a \cdot x = x^a$ and $(a\rho) \cdot x = \rho \cdot (x^a)$. We will write the group operations in $F^\times/p^k$ and $F_\ell^\times/p^k$ additively instead of multiplicatively.

Let $\zeta_{np}$ be as in §1, and for $n \in \mathcal{N}$ define a new $\chi$-cyclotomic unit

$$\xi_n = \prod_{d \mid n} ((1 - \zeta_{pd})^\chi)^{\mu(n/d)} \in (\mathbf{Z}[\boldsymbol{\mu}_{np}]^\times)^\chi$$

where $\mu$ is the usual Möbius function.

Lemma A.1. (i) *If $q \mid n$ then $\mathbf{N}_q \cdot \xi_n = (\mathrm{Fr}_q - q) \cdot \xi_{n/q}$.*
(ii) *If $\ell \mid n$ then $\xi_n \equiv 1$ modulo every prime of $F(\boldsymbol{\mu}_n)$ above $\ell$.*

Proof. The first assertion follows directly from the distribution relation (1), and the second from the fact that $\zeta_\ell$ is congruent to 1 modulo every prime of $\mathbf{Q}(\boldsymbol{\mu}_n)$ above $\ell$. □

As in §2 of [**Ru1**], there is a unique $\kappa_n \in (F^\times/p^k)^\chi$ whose image in $F(\boldsymbol{\mu}_n)^\times/p^k$ is $\mathbf{D}_n \cdot \xi_n$. In other words, we can fix $\beta_n \in F(\boldsymbol{\mu}_n)^\times$ such that $(\mathbf{D}_n \cdot \xi_n)/\beta^{p^k} \in F^\times$, i.e.,

$$\kappa_n = (\mathbf{D}_n \cdot \xi_n)/\beta_n^{p^k} \quad \text{in } F^\times/p^k, \tag{7}$$

$$((\gamma - 1) \cdot \beta_n)^{p^k} = (\gamma - 1)\mathbf{D}_n \cdot \xi_n \quad \text{for every } \gamma \in G_n. \tag{8}$$

The classes $\kappa_n$ do not form a Kolyvagin system, because they do not satisfy Theorem 2.4. For each $n$ we will define $\kappa_n^{\mathrm{cycl}}$ (Definition A.3 below) to be an appropriate linear combination of the $\kappa_d$ for $d$ dividing $n$, and we will show that the $\kappa_n^{\mathrm{cycl}}$ satisfy Theorem 2.4.

If $n \in \mathcal{N}$ and $q$ is a prime dividing $n$, define a derivation $\partial_q : (\mathbf{Z}/p^k\mathbf{Z})[G_n] \longrightarrow \mathbf{Z}/p^k\mathbf{Z}$ by

$$\partial_q\Big(\prod_{\ell \mid n} \sigma_\ell^{a_\ell}\Big) = -a_q$$

extended by linearity to all of $(\mathbf{Z}/p^k\mathbf{Z})[G_n]$. By our convention on $\mathrm{Fr}_q$ we have $\partial_q(\mathrm{Fr}_q) = 0$.

Write $(\kappa_n)_\ell$ for the image of $\kappa_n$ in $(F_\ell^\times/p^k)^\chi$, and $(\kappa_n)_{\ell,\mathrm{f}}$ for the "finite projection" of $(\kappa_n)_\ell$, the image of $(\kappa_n)_\ell$ under the projection map $(F_\ell^\times/p^k)^\chi \to (\mathcal{O}_\ell^\times/p^k)^\chi$ of (3).

If $n \in \mathcal{N}$ let $\mathfrak{S}(n)$ denote the set of permutations of the primes dividing $n$, and let $\mathfrak{S}_1(n) \subset \mathfrak{S}(n)$ be the subset

$$\{\pi \in \mathfrak{S}(n) : \text{the } q \text{ not fixed by } \pi \text{ form a single } \pi\text{-orbit}\}.$$

If $\pi \in \mathfrak{S}(n)$ let $d_\pi = \prod_{\pi(q)=q} q$.

Proposition A.2. *If $n \in \mathcal{N}$ and $\ell \mid n$ then*

$$(\kappa_n)_{\ell,\mathrm{f}} = \sum_{\substack{\pi \in \mathfrak{S}_1(n) \\ \pi(\ell) \neq \ell}} \Big(\prod_{q \mid (n/d_\pi)} \partial_q(\mathrm{Fr}_{\pi(q)})\Big)(\kappa_{d_\pi})_{\ell,\mathrm{f}}.$$

We will prove Proposition A.2 below, after using it to prove Theorem 2.4.

Definition A.3. For every $n \in \mathcal{N}$ define

$$\kappa_n^{\mathrm{cycl}} = \sum_{\pi \in \mathfrak{S}(n)} \epsilon(\pi)\Big(\prod_{q \mid (n/d_\pi)} \partial_q(\mathrm{Fr}_{\pi(q)})\Big)\kappa_{d_\pi}$$

where $\epsilon(\pi)$ is the number of cycles of length greater than one in the cycle decomposition of $\pi$. Note that $\kappa_1^{\mathrm{cycl}} = \kappa_1$ is the image of $1 - \zeta_p$ in $(\mathcal{O}^\times/p^k)^\chi$.

Proof of Theorem 2.4. If $\ell \mid n$ then we can group the terms in the definition of $\kappa_n^{\mathrm{cycl}}$ as

$$\begin{aligned}\kappa_n^{\mathrm{cycl}} &= \sum_{\substack{\pi\in\mathfrak{S}(n)\\ \pi(\ell)=\ell}} \epsilon(\pi)\Big(\prod_{q\mid(n/d_\pi)} \partial_q(\mathrm{Fr}_{\pi(q)})\Big)\kappa_{d_\pi} \\ &\qquad + \sum_{\substack{\pi\in\mathfrak{S}(n)\\ \pi(\ell)=\ell}} \sum_{\substack{\pi'\in\mathfrak{S}_1(d_\pi)\\ \pi'(\ell)\neq\ell}} \epsilon(\pi\pi')\Big(\prod_{q\mid(n/d_{\pi'})} \partial_q(\mathrm{Fr}_{\pi\pi'(q)})\Big)\kappa_{d_{\pi'}} \\ &= \sum_{\substack{\pi\in\mathfrak{S}(n)\\ \pi(\ell)=\ell}} \epsilon(\pi)\Big(\prod_{q\mid(n/d_\pi)} \partial_q(\mathrm{Fr}_{\pi(q)})\Big)s_\pi\end{aligned}$$

where

$$s_\pi = \kappa_{d_\pi} - \sum_{\substack{\pi'\in\mathfrak{S}_1(d_\pi)\\ \pi'(\ell)\neq\ell}} \Big(\prod_{q\mid(d_\pi/d_{\pi'})} \partial_q(\mathrm{Fr}_{\pi'(q)})\Big)\kappa_{d_{\pi'}}.$$

Proposition A.2 shows that $(s_\pi)_{\ell,\mathrm{f}} = 0$ for every $\pi$, so $(\kappa_n^{\mathrm{cycl}})_{\ell,\mathrm{f}} = 0$. □

The rest of this appendix is devoted to the proof of Proposition A.2. Fix a prime $\ell \in \mathcal{P}$ and an $n \in \mathcal{N}$ divisible by $\ell$. Let $\mathcal{A}$ denote the augmentation ideal of $\mathbf{Z}[G_n]$.

Lemma A.4. *If $m \mid n$ and $\rho \in \mathcal{A} + p^k\mathbf{Z}[G_n]$, then $\rho\mathbf{D}_m \cdot \xi_m$ has a unique $p^k$-th root in $(\mathbf{Z}[\boldsymbol{\mu}_n]^\times)^\chi$.*

Proof. Equation (8) exhibits a $p^k$-th root of $(\gamma-1)\mathbf{D}_m \cdot \xi_m$ for every $\gamma \in G_n$, so every such $\rho\mathbf{D}_m \cdot \xi_m$ is a $p^k$-th power. The $p^k$-th root is unique because (since $\chi$ is not the Teichmüller character) $(\mathbf{Z}[\boldsymbol{\mu}_{np}]^\times)^\chi$ is torsion-free. □

We will write $p^{-k}\rho\mathbf{D}_m \cdot \xi_m$ for the $p^k$-th root of $\rho\mathbf{D}_m \cdot \xi_m$ given by Lemma A.4. Let $\lambda$ denote the product of all primes of $F(\boldsymbol{\mu}_n)$ above $\ell$, and let $X = (\mathbf{Z}[\boldsymbol{\mu}_{np}]/\lambda)^\times$, which we will write additively. If $\alpha \in \mathbf{Z}[\boldsymbol{\mu}_{np}]^\times$ we will write $\bar\alpha$ for the image of $\alpha$ in $X$.

Lemma A.5. *Suppose $m\ell \mid n$.*

(i) *If $\rho \in \mathcal{A}^2 + p^k\mathbf{Z}[G_n]$, then $\overline{p^{-k}\rho\mathbf{D}_{m\ell} \cdot \xi_{m\ell}} = 0$ in $X$.*

(ii) *If $\rho \in \mathcal{A} + p^k\mathbf{Z}[G_n]$, then*

$$\overline{p^{-k}\rho\mathbf{D}_{m\ell} \cdot \xi_{m\ell}} = \sum_{q\mid m\ell} \partial_q(\rho)\overline{p^{-k}(\mathrm{Fr}_q - q)\mathbf{D}_{m\ell/q} \cdot \xi_{m\ell/q}}$$

*in $X$.*

Proof. If $q \nmid m\ell$ then $p^{-k}\rho\mathbf{D}_{m\ell} \cdot \xi_{m\ell} \in \mathbf{Z}[G_n]\mathbf{D}_{m\ell} \cdot \xi_{m\ell}$, so $\overline{p^{-k}\rho\mathbf{D}_{m\ell} \cdot \xi_{m\ell}} = 0$ by Lemma A.1(ii). If $q \mid m\ell$, then using (6) and Lemma A.1(i) we see that

$$\begin{aligned}(1-\sigma_q)\mathbf{D}_{m\ell} \cdot \xi_{m\ell} &= (\mathbf{N}_q - (q-1))\mathbf{D}_{m\ell/q} \cdot \xi_{m\ell} \\ &= (\mathrm{Fr}_q - q)\mathbf{D}_{m\ell/q} \cdot \xi_{m\ell/q} - (q-1)\mathbf{D}_{m\ell/q} \cdot \xi_{m\ell}\end{aligned}$$

in $\mathbf{Z}[\boldsymbol{\mu}_{np}]^\times$. Dividing by $p^k$, projecting into $X$, and using Lemma A.1(ii) proves (ii) when $\rho = 1 - \sigma_q$. (Note that each $\mathrm{Fr}_q - q$ belongs to $\mathcal{A} + p^k\mathbf{Z}[G_n]$ because $q \equiv 1 \pmod{p^k}$.) We will use this to prove (i), and then use (i) to complete the proof of (ii).

We will prove (i) by induction on the number of primes dividing $m$. If $\rho \in p^k\mathbf{Z}[G_n]$, then (i) follows from Lemma A.1(ii). Thus it is enough to prove (i) when $\rho = (1-\sigma_q)(1-\sigma_{q'})$. If $q \neq \ell$, then the case of (ii) already done shows that

$$\overline{p^{-k}\rho\mathbf{D}_{m\ell}\cdot\xi_{m\ell}} = \overline{p^{-k}(\mathrm{Fr}_q - q)(1-\sigma_{q'})\mathbf{D}_{m\ell/q}\cdot\xi_{m\ell/q}}$$

which is zero by induction. If $q = \ell$, then

$$\overline{p^{-k}\rho\mathbf{D}_{m\ell}\cdot\xi_{m\ell}} = (\mathrm{Fr}_\ell - \ell)\overline{p^{-k}(1-\sigma_{q'})\mathbf{D}_{m\ell}\cdot\xi_{m\ell}}$$

which is zero because $(\mathrm{Fr}_\ell - \ell)$ kills $X$. This proves (i).

The right-hand side of (ii) is a linear function of

$$\rho \in (\mathcal{A} + p^k\mathbf{Z}[G_n])/(\mathcal{A}^2 + p^k\mathbf{Z}[G_n]),$$

and thanks to (i), the left-hand side is as well. We have shown that (ii) holds for the generators $1-\sigma_q$ of $(\mathcal{A}+p^k\mathbf{Z}[G_n])/(\mathcal{A}^2+p^k\mathbf{Z}[G_n])$, so (ii) holds for all $\rho$. □

Proposition A.6.

$$\overline{p^{-k}(\mathrm{Fr}_\ell - \ell)\mathbf{D}_n\cdot\xi_n} = \sum_{\substack{\pi\in\mathfrak{S}_1(n)\\ \pi(\ell)\neq\ell}} \Big(\prod_{q\mid(n/d_\pi)} \partial_q(\mathrm{Fr}_{\pi(q)})\Big)\,\overline{p^{-k}(\mathrm{Fr}_\ell-\ell)\mathbf{D}_{d_\pi}\cdot\xi_{d_\pi}}$$

Proof. Apply Lemma A.5 repeatedly, beginning with $m = n$ and $\rho = (\mathrm{Fr}_\ell - \ell)$. Expand all terms of the form $\overline{p^{-k}\rho D_m\cdot x_m}$ with $m$ divisible by $\ell$, but not those with $m$ prime to $\ell$. The summand corresponding to $\pi$ occurs as follows:

- expand $\overline{p^{-k}(\mathrm{Fr}_\ell-\ell)\mathbf{D}_n\cdot\xi_n}$,
- take the resulting term $\overline{p^{-k}(\mathrm{Fr}_{\pi(\ell)}-\pi(\ell))\mathbf{D}_{n/\pi(\ell)}\cdot\xi_{n/\pi(\ell)}}$ and expand that,
- take the new term $\overline{p^{-k}(\mathrm{Fr}_{\pi^2(\ell)}-\pi^2(\ell))\mathbf{D}_{n/(\pi(\ell)\pi^2(\ell))}\cdot\xi_{n/(\pi(\ell)\pi^2(\ell))}}$ and expand that,

and so forth until $\pi^i(\ell) = \ell$, which leaves us with the desired multiple of the term $\overline{p^{-k}(\mathrm{Fr}_\ell-\ell)D_{d_\pi}\cdot\xi_{d_\pi}}$. □

Lemma A.7. *The natural map $(F_\ell^\times/p^k)^\chi \to (F(\boldsymbol{\mu}_\ell)_\ell^\times/p^k)^\chi$ factors through*

$$(F_\ell^\times/p^k)^\chi \twoheadrightarrow (\mathcal{O}_\ell^\times/p^k)^\chi \hookrightarrow (F(\boldsymbol{\mu}_\ell)_\ell^\times/p^k)^\chi$$

*where the first map is the projection induced by* (3) *and the second is injective.*

Proof. Using the definition of $(F_\ell^\times/p^k)^\chi_{\mathrm{tr}}$ it is enough to show that $\ell$ is in the kernel of the map $\mathbf{Q}_\ell^\times/p^k \to \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times/p^k$ and that the map $\mathbf{Z}_\ell^\times/p^k \to \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times/p^k$ is injective.

For the first statement, we have $\mathbf{N}_{\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell}(\zeta_\ell - 1) = \ell$, so

$$\frac{\ell}{(\zeta_\ell-1)^{\ell-1}} = \prod_{i=1}^{\ell-1}\frac{\zeta_\ell^i - 1}{\zeta_\ell - 1} \equiv (\ell-1)! \equiv -1 \pmod{\zeta_\ell - 1}.$$

Thus by Hensel's Lemma, $\ell \in (\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)^\times)^{p^k}$, as desired.

For the second statement, since $\mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)/\mathbf{Q}_\ell$ is totally ramified, we have

$$\mathbf{Z}_\ell^\times/p^k \xrightarrow{\sim} \mathbf{F}_\ell^\times/p^k \xleftarrow{\sim} \mathbf{Z}_\ell[\boldsymbol{\mu}_\ell]^\times/p^k. \qquad \square$$

Recall that $\lambda$ is the product of all primes of $F(\boldsymbol{\mu}_n)$ above $\ell$. There are injective maps

$$\mathcal{O}_\ell^\times/p^k \xhookrightarrow{(\ell-1)/p^k} (\mathcal{O}_\ell/\ell)^\times \xhookrightarrow{\qquad} (\mathcal{O}[\boldsymbol{\mu}_n]_\ell/\lambda)^\times. \tag{9}$$

Proposition A.8. *If $m \mid n$, then the image of $(\kappa_m)_{\ell,\mathrm{f}}$ under the map* (9) *is* $-\overline{p^{-k}(\mathrm{Fr}_\ell - \ell)\mathbf{D}_m \cdot \xi_m}$.

Proof. By (8), the principal ideal generated by $\beta_m$ is fixed by $G_n$. Hence we can find $\eta_m \in \mathbf{F}(\boldsymbol{\mu}_\ell)^\times$ such that $\beta_m/\eta_m$ is a unit at all primes above $\ell$. Define $\beta'_m = \beta_m/\eta_m$ and $\kappa'_m = (\mathbf{D}_m \cdot \xi_m)/(\beta'_m)^{p^k}$. Since $\kappa_m = \kappa'_m$ in $F(\boldsymbol{\mu}_\ell)_\ell^\times/p^k$, Lemma A.7 shows that the image of $(\kappa_m)_{\ell,\mathrm{f}}$ in $F(\boldsymbol{\mu}_\ell)_\ell^\times/p^k$ is $\kappa'_m$. Hence to prove the lemma we need to show that $(\kappa'_m)^{(\ell-1)/p^k}$ is congruent to $p^{-k}(\mathrm{Fr}_\ell - 1)\mathbf{D}_m \cdot \xi_m$ modulo every prime above $\ell$.

We have

$$(\kappa'_m)^{(\ell-1)/p^k} = (\mathbf{D}_m \cdot \xi_m)^{(\ell-1)/p^k}/(\beta'_m)^{\ell-1}.$$

Since $\beta'_m$ is a unit all primes above $\ell$, modulo such primes we have (using (8) and the fact that $\eta_m$ is fixed by $\mathrm{Fr}_\ell$)

$$(\beta'_m)^{\ell-1} \;\equiv\; (\mathrm{Fr}_\ell - 1)\cdot\beta'_m \;=\; (\mathrm{Fr}_\ell - 1)\cdot\beta_m \;=\; p^{-k}(\mathrm{Fr}_\ell - 1)\mathbf{D}_m \cdot \xi_m.$$

Thus

$$(\kappa'_m)^{(\ell-1)/p^k} \;\equiv\; p^{-k}(\ell - \mathrm{Fr}_\ell)\mathbf{D}_m \cdot \xi_m \pmod{\lambda}$$

as desired. □

Proof of Proposition A.2. Proposition A.2 is now immediate from Propositions A.6 and A.8, and the injectivity of (9). This concludes the proof of Theorem 2.4 as well. □

## References

[Ko] Kolyvagin, V.: Euler systems, in: The Grothendieck Festschrift (Vol. II), P. Cartier et al., eds., *Prog. in Math* **87**, Boston: Birkhäuser (1990) 435–483.

[MR] Mazur, B., Rubin, K.: Kolyvagin Systems. To appear.

[MW] Mazur, B., Wiles, A.: Class fields of abelian extensions of **Q**, *Invent. math.* **76** (1984) 179–330.

[Ru1] Rubin, K.: The main conjecture. Appendix to: Cyclotomic fields I and II, S. Lang, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990) 397–419.

[Ru2] ———: 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.

[Ru3] ———: Euler Systems. *Annals of Math. Studies* **147**, Princeton: Princeton University Press (2000).

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

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