Canad. J. Math. Vol. **55** (4), 2003 pp. 673–692

A Note on Cyclotomic Euler Systems and the Double Complex Method

Greg W. Anderson and Yi Ouyang

Abstract. Let $\mathbb{F}$ be a finite real abelian extension of $\mathbb{Q}$. Let M be an odd positive integer. For every squarefree positive integer r the prime factors of which are congruent to 1 modulo M and split completely in $\mathbb{F}$, the corresponding Kolyvagin class $\kappa_r \in \mathbb{F}^\times/\mathbb{F}^{\times M}$ satisfies a remarkable and crucial recursion which for each prime number ℓ dividing r determines the order of vanishing of κ_r at each place of $\mathbb{F}$ above ℓ in terms of $\kappa_{r/\ell}$. In this note we give the recursion a new and universal interpretation with the help of the double complex method introduced by Anderson and further developed by Das and Ouyang. Namely, we show that the recursion satisfied by Kolyvagin classes is the specialization of a universal recursion independent of $\mathbb{F}$ satisfied by universal Kolyvagin classes in the group cohomology of the universal ordinary distribution *à la* Kubert tensored with $\mathbb{Z}/M\mathbb{Z}$. Further, we show by a method involving a variant of the diagonal shift operation introduced by Das that certain group cohomology classes belonging (up to sign) to a basis previously constructed by Ouyang also satisfy the universal recursion.

1 Introduction

Let $\mathbb{F}$ be a finite real abelian extension of $\mathbb{Q}$. Let M be an odd positive integer. For every squarefree positive integer r the prime factors of which are congruent to 1 modulo M and split completely in $\mathbb{F}$, the corresponding Kolyvagin class $\kappa_r \in \mathbb{F}^\times/\mathbb{F}^{\times M}$ satisfies a remarkable and crucial recursion which for each prime number ℓ dividing r determines the order of vanishing of κ_r at each place of $\mathbb{F}$ above ℓ in terms of $\kappa_{r/\ell}$. See Proposition 2.4 of the Rubin appendix to Lang's text [4] for a formulation of this recursion commonly employed in the literature. In this note we actually work with a formulation of the recursion slightly different from but equivalent to Rubin's formulation (see Proposition 2.5 below).

The purpose of this note is to give the recursion satisfied by Kolyvagin classes a new and universal interpretation with the help of the double complex method introduced by Anderson [1] and further developed by Das [2] and Ouyang [5]. We show that the recursion is the specialization of a universal recursion independent of $\mathbb{F}$ satisfied by universal Kolyvagin classes in the group cohomology of the universal ordinary distribution *à la* Kubert tensored with $\mathbb{Z}/M\mathbb{Z}$ (see Proposition 4.5). Further, we show by a method involving a variant of the diagonal shift operation introduced by Das [2] that certain group cohomology classes belonging (up to sign) to a basis previously constructed by Ouyang [5] also satisfy the universal recursion (see Corollary 5.9). Taken together, our results show that it is possible to construct classes in $\mathbb{F}^\times/\mathbb{F}^{\times M}$ satisfying a useful recursion of Kolyvagin type by methods somewhat more conceptual than have heretofore been employed.

Received by the editors October 31, 2001; revised April 24, 2002.
AMS subject classification: Primary: 11R18, 11R23; secondary: 11R34.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

It is natural to expect that results similar to those presented in this note hold for general universal Euler systems. Indeed, the many beautiful results proved in Chapter 4 of Rubin's book [6] strongly suggest the existence of a general theory of universal Kolyvagin recursions. But since there are significant technical difficulties to deal with before the double complex method can be brought to bear on the general theory of Euler systems, we can for now but affirm our hope to generalize the results of this note. In any case, we hope that our point of view might prove helpful to others in the search for new applications and new examples of Euler systems.

2 A Brief Review of Cyclotomic Euler Systems

2.1 Notation and Setting

Let $\mathbb{F}$ be a finite real abelian extension of the field $\mathbb{Q}$ of rational numbers and let $\bar{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$. Let M be an odd positive integer, and for every abelian group A let the M-torsion subgroup be denoted A_M. Let $\mathbf{r}$ be the formal product of all odd primes $\ell \equiv 1 \bmod M$ that split completely in $\mathbb{F}$. In the sequel we refer to formal products of prime numbers as *supernatural numbers*. Let G be the Galois group over $\mathbb{F}$ of the field generated over $\mathbb{F}$ by all roots of unity in $\bar{\mathbb{F}}$ of order dividing $\mathbf{r}$. For each prime number ℓ dividing $\mathbf{r}$:

- Let $G_\ell \subset G$ be the inertia subgroup at some place (hence all places) above ℓ.
  - Note that G_ℓ is cyclic of order $\ell - 1$.
- Let σ_ℓ be a generator of G_ℓ.
- Let $N_\ell := \sum_{i=0}^{\ell-2} \sigma_\ell^i \in \mathbb{Z}[G_\ell]$ and $N'_\ell := \sum_{i=1}^{\ell-2} i\sigma_\ell^i \in \mathbb{Z}[G_\ell]$.
  - Note the crucial identity $N'_\ell(\sigma_\ell - 1) = \ell - 1 - N_\ell$.
- Let $\mathrm{Frob}_\ell \in G/G_\ell$ be the arithmetic Frobenius automorphism at some place (hence all places) above ℓ.
  Let ord_ℓ be the normalized additive valuation of $\mathbb{Q}$ corresponding to ℓ.

For each positive integer r dividing $\mathbf{r}$:

- Let $G_r \subset G$ be the subgroup generated by $\bigcup_{\ell | r} G_\ell$.
  - Note that the evident homomorphism $\prod_{\ell|r} G_\ell \to G_r$ is bijective.
- Let $N'_r := \prod_{\ell|r} N'_\ell \in \mathbb{Z}[G_r]$.
- Let $\mathbb{F}_r$ be the extension of $\mathbb{F}$ generated by the r-th roots of unity in $\bar{\mathbb{F}}$. Put $\mathbb{F}_{\mathbf{r}} := \bigcup_{r|\mathbf{r}} \mathbb{F}_r$.
- Let $\mathcal{O}_r$ be the ring of algebraic integers of $\mathbb{F}_r$. Put $\mathcal{O} := \mathcal{O}_1$ and $\mathcal{O}_{\mathbf{r}} := \bigcup_{r|\mathbf{r}} \mathcal{O}_r$.

For each positive integer r dividing $\mathbf{r}$ and prime number ℓ:

- Let $\mathcal{O}_{r,(\ell)}$ be the localization of $\mathcal{O}_r$ by the multiplicative system of elements prime to ℓ. Put $\mathcal{O}_{(\ell)} := \mathcal{O}_{1,(\ell)}$ and $\mathcal{O}_{\mathbf{r},(\ell)} := \bigcup_{r|\mathbf{r}} \mathcal{O}_{r,(\ell)}$.

We fix a collection

$$\{\xi_r \in \mathcal{O}_r^\times\}_{r|\mathbf{r}}$$

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

of global units such that for all positive integers r dividing $\mathbf{r}$ and prime numbers ℓ dividing r the following relations hold:

- $\xi_r^{N_\ell} = \xi_{r/\ell}^{\mathrm{Frob}_\ell - 1}$.
- $\xi_r \equiv \xi_{r/\ell}$ modulo the radical of the ideal of $\mathcal{O}_r$ generated by ℓ.

Such a collection $\{\xi_r\}$ is called an *Euler system*.

Lemma 2.2 *Let r be any positive integer dividing* $\mathbf{r}$. *The sequence*

$$1 \to \mathbb{F}_r^\times \xrightarrow{x \mapsto x^M} \mathbb{F}_r^\times \to \mathbb{F}_r^\times / \mathbb{F}_r^{\times M} \to 1$$

is exact and so is the sequence

$$1 \to \mathbb{F}^\times \xrightarrow{x \mapsto x^M} \mathbb{F}^{\times M} \to H^0(G_r, \mathbb{F}_r^\times / \mathbb{F}_r^{\times M}) \to 1$$

of G_r-invariants. Via the latter sequence make now the identification

$$H^0(G_r, \mathbb{F}_r^\times / \mathbb{F}_r^{\times M}) = \mathbb{F}^\times / \mathbb{F}^{\times M}.$$

We have

$$\big(\textit{image of } H^0(G_r, \mathcal{O}_r^\times / \mathcal{O}_r^{\times M}) \textit{ in } H^0(G_r, \mathbb{F}_r^\times / \mathbb{F}_r^{\times M})\big) \subset \mathcal{O}_{(\ell)}^\times / \mathcal{O}_{(\ell)}^{\times M}$$

for all prime numbers ℓ not dividing r.

Proof The first sequence is exact because under our hypotheses the field $\mathbb{F}_r$ contains no nontrivial M-th roots of unity. The second sequence is exact by Satz 90. We turn to the proof of the last assertion. Fix $\xi \in \mathcal{O}_r^\times$ representing a class in $H^0(G_r, \mathcal{O}_r^\times / \mathcal{O}_r^{\times M})$ and write

$$\xi = \alpha\beta^M (\alpha \in \mathbb{F}^\times, \beta \in \mathbb{F}_r^{\times M}).$$

It suffices to verify that α up to a factor in $\mathbb{F}^{\times M}$ belongs to $\mathcal{O}_{(\ell)}^\times$. Since $\mathcal{O}_{(\ell)}$ is a principal ideal domain, it suffices to verify that for each prime P of $\mathcal{O}$ dividing ℓ the order with which P divides α is divisible by M. But the latter is obvious because any prime of $\mathcal{O}$ dividing ℓ cannot divide r and hence is unramified in $\mathcal{O}_r$. ■

2.3 Kolyvagin Classes

Fix a positive integer r dividing $\mathbf{r}$. For each prime number ℓ dividing r one has

$$\xi_r^{N_r'(1-\sigma_\ell)} \equiv \xi_r^{N_{r/\ell}' N_\ell} \equiv \xi_{r/\ell}^{N_{r/\ell}'(\mathrm{Frob}_\ell - 1)} \equiv 1 \bmod \mathcal{O}_r^{\times M}$$

by induction on the number of prime divisors of r and hence

$$\xi_r^{N_r'} \bmod \mathcal{O}_r^{\times M} \in H^0(G_r, \mathcal{O}_r^\times / \mathcal{O}_r^{\times M}).$$

By Lemma 2.2 there exists a unique class

$$\kappa_r \in \mathbb{F}^\times/\mathbb{F}^{\times M}$$

such that

$$\xi_r^{N_r'} \equiv \kappa_r \bmod \mathbb{F}_r^{\times M}$$

and moreover we have

$$(\ell, r) = 1 \Rightarrow \kappa_r \in \mathcal{O}_{(\ell)}^\times/\mathcal{O}_{(\ell)}^{\times M}$$

for all prime numbers ℓ. We call κ_r the *Kolyvagin class* indexed by r.

2.4 The Operations ν_ℓ, $[\cdot]_\ell$ and $\exp_\ell$

Let a prime number ℓ dividing $\mathbf{r}$ be given. Let

$$\nu_\ell \colon \mathcal{O}_{(\ell)}^\times/\mathcal{O}_{(\ell)}^{\times M} \to (\mathcal{O}/\ell)_M^\times$$

be the unique homomorphism such that

$$\nu_\ell(x \bmod \mathcal{O}_{(\ell)}^{\times M}) \equiv x^{\frac{\ell-1}{M}} \bmod \ell\mathcal{O}_{(\ell)}$$

for all $x \in \mathcal{O}_{(\ell)}^\times$. Let

$$[\cdot]_\ell \colon \mathbb{F}^\times/\mathbb{F}^{\times M} \to (\text{group of fractional } \mathcal{O}_{(\ell)}\text{-ideals }) \otimes (\mathbb{Z}/M\mathbb{Z})$$

be the unique homomorphism such that

$$[x \bmod \mathbb{F}^{\times M}]_\ell = (\text{fractional } \mathcal{O}_{(\ell)}\text{-ideal generated by } x)$$
$$\bmod\ (M\text{-th powers of fractional } \mathcal{O}_{(\ell)}\text{-ideals})$$

for all $x \in \mathbb{F}^\times$. We claim that there exists a unique isomorphism

$$\exp_\ell \colon (\text{group of fractional } \mathcal{O}_{(\ell)}\text{-ideals}) \otimes (\mathbb{Z}/M\mathbb{Z}) \xrightarrow{\sim} (\mathcal{O}/\ell)_M^\times$$

such that

$$\exp_\ell\bigl((\text{fractional } \mathcal{O}_{(\ell)}\text{-ideal generated by } x^{N_\ell}) \otimes (1 \bmod M)\bigr)$$
$$\equiv (x^{1-\sigma_\ell})^{\frac{\ell-1}{M}} \bmod \sqrt{\ell\mathcal{O}_{\ell,(\ell)}}$$

for all $x \in \mathbb{F}_\ell^\times$ where $\sqrt{\ell\mathcal{O}_{\ell,(\ell)}}$ denotes the radical of the ideal of $\mathcal{O}_{\ell,(\ell)}$ generated by ℓ. Now each maximal ideal of $\mathcal{O}_{(\ell)}$ is totally ramified in $\mathcal{O}_{\ell,(\ell)}$, hence every fractional $\mathcal{O}_{(\ell)}$-ideal is generated by x^{N_ℓ} for some $x \in \mathbb{F}_\ell^\times$ unique up to a factor in $\mathcal{O}_{\ell,(\ell)}^\times$ and hence $\exp_\ell$ is well defined. Upon completing the extension $\mathbb{F}_\ell/\mathbb{F}$ at any place of $\mathbb{F}_\ell$ above ℓ, one obtains a Kummer extension with Galois group G_ℓ and hence $\exp_\ell$ is an isomorphism. The claim is proved.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

Proposition 2.5 *For all positive integers r dividing* $\mathbf{r}$ *and prime numbers ℓ dividing r the identity*

$$\exp_\ell[\kappa_r]_\ell \equiv \sqrt[M]{\xi_r^{N_r'(\sigma_\ell-1)}} \equiv \sqrt[M]{\xi_{r/\ell}^{N_{r/\ell}'(\ell-\mathrm{Frob}_\ell)}} \equiv \nu_\ell\kappa_{r/\ell} \bmod \sqrt{\ell\mathcal{O}_{r,(\ell)}}$$

holds, where the M-th roots are chosen to be the unique such existing in $\mathcal{O}_r^\times$ and $\sqrt{\ell\mathcal{O}_{r,(\ell)}}$ denotes the radical of the ideal of $\mathcal{O}_{r,(\ell)}$ generated by ℓ. (This is a reformulation of Proposition 2.4 of the Rubin appendix to Lang's text [4].)

Proof Write

$$\xi_r^{N_r'} = \alpha_r\beta_r^M(\alpha_r \in \mathbb{F}^\times,\ \beta_r \in \mathbb{F}_r^\times)$$

and

$$\xi_{r/\ell}^{N_{r/\ell}'} = \alpha_{r/\ell}\beta_{r/\ell}^M(\alpha_{r/\ell} \in \mathcal{O}_{(\ell)}^\times, \beta_{r/\ell} \in \mathcal{O}_{r/\ell,(\ell)}^\times).$$

Choose $\gamma_r \in \mathbb{F}_\ell^\times$ such that

$$\gamma_r^{N_\ell} \text{ and } \alpha_r \text{ generate the same fractional } \mathcal{O}_{(\ell)}\text{-ideal.}$$

One then has

$$\gamma_r^{\frac{\ell-1}{M}}\beta_r \in \mathcal{O}_{r,(\ell)}^\times.$$

Further, one has

$$\xi_r^{N_r'(\sigma_\ell-1)} = \beta_r^{M(\sigma_\ell-1)} = \xi_r^{N_{r/\ell}'(\ell-1)}\beta_{r/\ell}^{M(1-\mathrm{Frob}_\ell)}$$

and hence

$$\beta_r^{\sigma_\ell-1} = (\xi_r^{N_{r/\ell}'})^{\frac{\ell-1}{M}}\beta_{r/\ell}^{1-\mathrm{Frob}_\ell}$$

because there are no nontrivial M-th roots of unity in $\mathbb{F}_r$. Finally, one has

$$(\gamma_r^{1-\sigma_\ell})^{\frac{\ell-1}{M}} \equiv \beta_r^{\sigma_\ell-1} \equiv \alpha_{r/\ell}^{\frac{\ell-1}{M}}\beta_{r/\ell}^{\ell-\mathrm{Frob}_\ell} \equiv \alpha_{r/\ell}^{\frac{\ell-1}{M}} \bmod \sqrt{\ell\mathcal{O}_{r,(\ell)}}$$

which by the definitions proves the result. ■

2.6 The Kolyvagin Recursion

We say that a system of classes

$$\{\lambda_r \in \mathbb{F}^\times/\mathbb{F}^{\times M}\}_{r|\mathbf{r}}$$

indexed by the positive integers dividing $\mathbf{r}$ satisfies the *Kolyvagin recursion* if for all positive integers r dividing $\mathbf{r}$ and prime numbers ℓ the following hold:

- $(\ell, r) = 1 \Rightarrow \lambda_r \in \mathcal{O}_{(\ell)}^\times/\mathcal{O}_{(\ell)}^{\times M}$.
- $\ell | r \Rightarrow \exp_\ell[\lambda_r]_\ell = \nu_\ell\lambda_{r/\ell}$.

In this language Proposition 2.5 and the discussion leading up to it can be condensed to the assertion that the system of Kolyvagin classes satisfies the Kolyvagin recursion.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

3 Universal Constructions

3.1 The Free Abelian Group $\mathcal{A}$

For each supernatural number $\mathbf{s}$ put

$$\frac{1}{\mathbf{s}}\mathbb{Z} := \bigcup_{s|\mathbf{s}} \frac{1}{s}\mathbb{Z},$$

the union being extended over all positive integers s dividing $\mathbf{s}$. Let $\mathcal{A}$ be the free abelian group generated by the family of symbols of the form

$$[a]\left(a \in \frac{1}{\mathbf{r}}\mathbb{Z}/\mathbb{Z}\right).$$

We equip $\mathcal{A}$ with an action of G by the rule

$$\sigma[a] = [b] \Leftrightarrow \sigma\phi(a) = \phi(b)$$

for all $a, b \in \frac{1}{\mathbf{r}}\mathbb{Z}/\mathbb{Z}$, injective homomorphisms $\phi\colon \frac{1}{\mathbf{r}}\mathbb{Z}/\mathbb{Z} \to \mathbb{F}_{\mathbf{r}}^{\times}$, and $\sigma \in G$. For each supernatural number $\mathbf{s}$ dividing $\mathbf{r}$, let $\mathcal{A}(\mathbf{s})$ be the subgroup of $\mathcal{A}$ generated by symbols of the form

$$[a]\left(a \in \frac{1}{\mathbf{s}}\mathbb{Z}/\mathbb{Z}\right).$$

Note that $\mathcal{A}(\mathbf{s})$ is stable under the action of G. Note that for each prime number ℓ dividing $\mathbf{r}$ the group $\mathcal{A}(\mathbf{r}/\ell)$ can be viewed as a G/G_ℓ-module. Note that

$$\mathcal{A} = \bigcup_{r|\mathbf{r}} \mathcal{A}(r)$$

where r ranges over the positive integers dividing $\mathbf{r}$.

3.2 The Universal Ordinary Distribution

Given any supernatural number $\mathbf{s}$ dividing $\mathbf{r}$, let $U_{\mathbf{s}}$ be the quotient of $\mathcal{A}(\mathbf{s})$ by the subgroup generated by all elements of the form

$$[a] - \sum_{\ell b = a}[b]\left(\ell\text{: a prime number dividing } \mathbf{s}, a \in \frac{\ell}{\mathbf{s}}\mathbb{Z}/\mathbb{Z}\right).$$

Notice that the action of G on $\mathcal{A}(\mathbf{s})$ descends to $U_{\mathbf{s}}$. Note that for every prime number ℓ dividing $\mathbf{r}$ the group $U_{\mathbf{r}/\ell}$ can be viewed as a G/G_ℓ-module. The map

$$\left(a \mapsto (\text{class in } U_{\mathbf{s}} \text{ represented by } [a])\right) : \frac{1}{\mathbf{s}}\mathbb{Z}/\mathbb{Z} \to U_{\mathbf{s}}$$

is the universal example of a *one-dimensional ordinary distribution* of *level* $\mathbf{s}$ *à la* Kubert. Put

$$U := U_{\mathbf{r}}.$$

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

Abusing language slightly, we call U the *universal ordinary distribution*. See Kubert [3], Lang [4] or Anderson's appendix to Ouyang's paper [5] for background on the theory of the universal ordinary distribution. By the classical results of Kubert [3], for any supernatural number **s** dividing **r**, the map

$$U_{\mathbf{s}} \to U$$

induced by the inclusion $\mathcal{A}(\mathbf{s}) \subseteq \mathcal{A}$ is an injective homomorphism of free abelian groups with free cokernel and hence the induced map

$$H^0(G, U_{\mathbf{s}}/MU_{\mathbf{s}}) \to H^0(G, U/MU)$$

is also injective. Thus we may and we do henceforth identify $U_{\mathbf{s}}$ (resp. $H^0(G, U_{\mathbf{s}}/MU_{\mathbf{s}})$) with a subgroup of U (resp. $H^0(G, U/MU)$). Note that we have

$$U_{\mathbf{s}} = \bigcup_{s|\mathbf{s}} U_s, \quad H^0(G, U_{\mathbf{s}}/MU_{\mathbf{s}}) = \bigcup_{s|\mathbf{s}} H^0(G, U_s/MU_s)$$

where the index s in both unions ranges over the positive integers dividing **s**.

Lemma 3.3 *For every prime number ℓ dividing* **r** *the equation*

$$(\ell - \mathrm{Frob}_\ell)x = 0$$

has no nonzero solution $x \in U_{\mathbf{r}/\ell}$.

Proof Fix a solution $x \in U_{\mathbf{r}/\ell}$ of the equation in question. Choose a positive integer r dividing $\mathbf{r}/\ell$ such that $x \in U_r$. Choose $\phi \in G_r$ inducing the same automorphism of $\mathcal{A}(r)$ as does Frob_ℓ. Let m be the order of ϕ in the group G_r. Then one has an identity

$$(\ell^m - 1)x = (\ell^{m-1} + \ell^{m-2}\phi + \cdots + \ell\phi^{m-2} + \phi^{m-1})(\ell - \phi)x = 0.$$

It follows that $x = 0$ because $U_{\mathbf{r}/\ell}$ is a torsion-free abelian group. ■

3.4 The Submodule I_ℓ

Let a prime number ℓ dividing **r** be given. We define

$$I_\ell \subset U$$

to be the subgroup generated by all elements of U represented by expressions of the form

$$[a] - [b] \left(a, b \in \frac{1}{\mathbf{r}}\mathbb{Z}/\mathbb{Z}, a - b \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \right).$$

Note that since I_ℓ is G-stable and

$$(\sigma_\ell - 1)U \subset I_\ell,$$

the quotient U/I_ℓ can be viewed as a G/G_ℓ-module.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

3.5 The Resolution L

Let L be the free abelian group generated by symbols of the form

$$[a,g]\Big(g\colon \text{positive integer dividing } \mathbf{r},\, a\in \frac{g}{\mathbf{r}}\mathbb{Z}/\mathbb{Z}\Big).$$

We equip the abelian group L with an action of G by the rule

$$\sigma[a,g]=[a',g']\Leftrightarrow \sigma\phi(a)=\phi(a') \text{ and } g=g'$$

for all symbols $[a,g]$ and $[a',g']$ in the canonical basis of L, injective homomorphisms $\phi\colon \frac{1}{\mathbf{r}}\mathbb{Z}/\mathbb{Z}\to\mathbb{F}_{\mathbf{r}}^{\times}$ and $\sigma\in G$. We equip the group L with a G-stable grading by declaring that

$$(\text{degree of } [a,g]) := -\sum_{\ell}\operatorname{ord}_\ell g = -(\text{number of prime divisors of } g).$$

Here and in analogous summations below the indices ℓ, ℓ' and p are understood to range over prime numbers dividing $\mathbf{r}$, subject to further restrictions as noted. We equip L with a G-equivariant differential d of degree 1 by the rule

$$d[a,g] := \sum_{\ell\mid g}(-1)^{\sum_{\ell'<\ell}\operatorname{ord}_{\ell'} g}\Big([a,g/\ell]-\sum_{\ell b=a}[b,g/\ell]\Big).$$

Now let $\mathbf{s}$ be any supernatural number dividing $\mathbf{r}$. Let $L(\mathbf{s})$ be the subgroup of L generated by symbols of the form

$$[a,g]\Big(g\colon \text{positive integer dividing } \mathbf{s},\, a\in \frac{g}{\mathbf{s}}\mathbb{Z}/\mathbb{Z}\Big).$$

Then $L(\mathbf{s})$ is a G- and d-stable graded subgroup of L. It is known that

$$H^0(L(\mathbf{s}),d)=U_{\mathbf{s}}$$

via the isomorphism induced by the G-equivariant mapping

$$([a,1]\mapsto[a])\colon (\text{degree zero component of } L(\mathbf{s}))\to\mathcal{A}(\mathbf{s})$$

and that

$$H^n(L(\mathbf{s}),d)=0 \quad \text{for } n\neq 0.$$

In other words, $\big(L(\mathbf{s}),d\big)$ is a resolution of $U_{\mathbf{s}}$ in the category of G-modules. See Anderson's appendix to Ouyang's paper [5] for details and further discussion.

Proposition 3.6 *The sequence*

$$0\longrightarrow U_{\mathbf{r}/\ell}\xrightarrow{\ell-\mathrm{Frob}_\ell}U_{\mathbf{r}/\ell}\longrightarrow U/I_\ell\longrightarrow 0$$

is exact where the map $U_{\mathbf{r}/\ell}\to U/I_\ell$ is that induced by the inclusion $U_{\mathbf{r}/\ell}\subset U$.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

Proof Let

$$s_\ell \colon L \to L(\mathbf{r}/\ell)$$

be the unique homomorphism such that

$$s_\ell[a,g] \equiv \begin{cases} (-1)^{\sum_{\ell'<\ell} \operatorname{ord}_{\ell'} g}[a,g/\ell] & \text{if } \ell | g \\ 0 & \text{otherwise} \end{cases}$$

for all symbols $[a,g]$ in the canonical basis of L. The homomorphism s_ℓ is of degree 1 and satisfies the relation

$$s_\ell d = -ds_\ell$$

as can be verified by a straightforward calculation. Now consider the sequence

$$\Sigma \colon 0 \to L(\mathbf{r}/\ell) \longrightarrow L/L' \xrightarrow{s_\ell} L(\mathbf{r}/\ell) \to 0$$

where L' is the subgroup of L generated by all elements of the form

$$[a,g] - [b,g] \Big(g \;\Big|\; \frac{\mathbf{r}}{\ell}, a, b \in \frac{g}{\mathbf{r}}\mathbb{Z}/\mathbb{Z}, a-b \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \Big)$$

and the map $L(\mathbf{r}/\ell) \to L/L'$ is that induced by the inclusion $L(\mathbf{r}/\ell) \subset L$. It is easy to verify that Σ is short exact. Since L' is a graded d- and G-stable subgroup of L and $(\sigma_\ell - 1)L \subset L'$, it follows that Σ can be viewed as a short exact sequence of complexes of G/G_ℓ-modules. Because $H^*(L(\mathbf{r}/\ell), d)$ is concentrated in degree 0, the long exact sequence of G/G_ℓ-modules deduced from Σ by taking d-cohomology has at most four nonzero terms and after making the evident identifications takes the form

$$\cdots \to 0 \to H^{-1}(L/L', d) \to U_{\mathbf{r}/\ell} \xrightarrow{1-\operatorname{Frob}_\ell^{-1}\ell} U_{\mathbf{r}/\ell} \longrightarrow U/I_\ell \to 0 \to \cdots$$

where the map $U_{\mathbf{r}/\ell} \to U/I_\ell$ is that induced by the inclusion $U_{\mathbf{r}/\ell} \subset U$. By Lemma 3.3 we have

$$H^{-1}(L/L', d) = \ker\Big(U_{\mathbf{r}/\ell} \xrightarrow{-\operatorname{Frob}_\ell^{-1}(\ell - \operatorname{Frob}_\ell)} U_{\mathbf{r}/\ell} \Big) = 0,$$

whence the result. ■

Proposition/Definition 3.7 *For every prime number ℓ dividing $\mathbf{r}$ there exists a unique homomorphism*

$$D_\ell \colon H^0(G, U/MU) \to H^0(G, U_{\mathbf{r}/\ell}/MU_{\mathbf{r}/\ell})$$

such that

$$\frac{(\sigma_\ell - 1)x}{M} \equiv \frac{(\ell - \operatorname{Frob}_\ell)y}{M} \bmod I_\ell \iff D_\ell(x \bmod MU) = y \bmod MU_{\mathbf{r}/\ell}$$

for all $x \in U$ representing a class in $H^0(G, U/MU)$ and $y \in U_{\mathbf{r}/\ell}$ representing a class in $H^0(G, U_{\mathbf{r}/\ell}/MU_{\mathbf{r}/\ell})$. Moreover one has

$$D_\ell H^0(G, U_r/MU_r) \subset H^0(G, U_{r/\ell}/MU_{r/\ell})$$

for all positive integers r dividing $\mathbf{r}$ and divisible by ℓ.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

Proof Put

$$X := \{x \in U | x \text{ represents a class in } H^0(G, U/MU)\},$$
$$Y := \{y \in U_{\mathbf{r}/\ell} | (\ell - \mathrm{Frob}_\ell) y \in MU_{\mathbf{r}/\ell}\},$$
$$Z := \left\{ (x, y) \in X \times Y \;\middle|\; \frac{(\sigma_\ell - 1)x}{M} \equiv \frac{(\ell - \mathrm{Frob}_\ell)y}{M} \bmod I_\ell \right\}.$$

Fix a positive integer r dividing $\mathbf{r}$ and divisible by ℓ. To prove the proposition it is enough to prove the following three claims:

1. $Z \cap (MU \times Y) = MU \times MU_{\mathbf{r}/\ell}$.
2. $(\sigma - 1)Z \subset MU \times MU_{\mathbf{r}/\ell}$ for all $\sigma \in G$.
3. For all $x \in X \cap U_r$ there exists $y \in Y \cap U_{r/\ell}$ such that $(x, y) \in Z$.

We turn to the proof of the first claim. Only the containment $\subset$ requires proof; the containment $\supset$ is trivial. Suppose we are given $(x, y) \in Z \cap (MU \times Y)$. Then $\frac{(\ell - \mathrm{Frob}_\ell)y}{M} \in I_\ell \cap U_{\mathbf{r}/\ell}$ and hence by Proposition 3.6 there exists $z \in U_{\mathbf{r}/\ell}$ such that $(\ell - \mathrm{Frob}_\ell)y = M(\ell - \mathrm{Frob}_\ell)z$. By Lemma 3.3 it follows that $y = Mz$. Thus the first claim is proved. The second claim follows immediately from the first.

We turn finally to the proof of the third claim. Let

$$\rho_\ell \colon \mathcal{A}(r) \to \mathcal{A}(r/\ell)$$

be the unique homomorphism such that

$$\rho_\ell[a + b] := [a]$$

for all $a \in \frac{\ell}{r}\mathbb{Z}/\mathbb{Z}$ and $b \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$. For each prime number p dividing r, let

$$\gamma_p \colon \mathcal{A}(r/p) \to \mathcal{A}(r)$$

be the unique homomorphism such that

$$\gamma_p[a] := [a] - \sum_{pb=a} [b]$$

for all $a \in \frac{p}{r}\mathbb{Z}/\mathbb{Z}$. Note that ρ_ℓ commutes with γ_p for $p \neq \ell$ and that the composite homomorphism $\rho_\ell\gamma_\ell$ induces the endomorphism $(1 - \mathrm{Frob}_\ell^{-1}\ell)$ of $\mathcal{A}(r/\ell)$. Choose a lifting $\mathbf{a} \in \mathcal{A}(r)$ of x. By hypothesis there exists an identity

$$(\sigma_\ell - 1)\mathbf{a} = M\mathbf{b} + \sum_{p|r} \gamma_p \mathbf{b}_p \big(\mathbf{b} \in \mathcal{A}(r), \mathbf{b}_p \in \mathcal{A}(r/p)\big),$$

and hence also an identity

$$0 = M\rho_\ell\mathbf{b} - (\ell - \mathrm{Frob}_\ell)(\mathrm{Frob}_\ell^{-1}\mathbf{b}_\ell) + \sum_{p|\frac{r}{\ell}} \gamma_p\rho_\ell\mathbf{b}_p.$$

Then the element $y \in U_{r/\ell}$ represented by $\mathrm{Frob}_\ell^{-1}\mathbf{b}_\ell$ has the desired property, namely that $(x, y) \in Z$. Thus the third claim is proved and with it the result. ■

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

3.8 The Universal Kolyvagin Recursion

We say that a family of classes

$$\{c_r \in H^0(G, U/MU)\}_{r|\mathbf{r}}$$

indexed by the positive integers r dividing $\mathbf{r}$ satisfies the *universal Kolyvagin recursion* if the following conditions hold for all positive integers r dividing $\mathbf{r}$ and prime numbers ℓ:

- $c_r \in H^0(G_r, U_r/MU_r) = H^0(G, U_r/MU_r) \subset H^0(G, U/MU)$.
- $\ell | r \Rightarrow D_\ell c_r = c_{r/\ell}$.

The terminology is justified by the next result.

Proposition 3.9 *Let*

$$\xi \colon U \to \mathcal{O}_{\mathbf{r}}^{\times}$$

be any G-equivariant homomorphism such that

$$\xi I_\ell \subset 1 + \sqrt{\ell \mathcal{O}_{\mathbf{r},(\ell)}}$$

for all primes ℓ dividing $\mathbf{r}$ where $\sqrt{\ell \mathcal{O}_{\mathbf{r},(\ell)}}$ denotes the radical of the ideal of $\mathcal{O}_{\mathbf{r},(\ell)}$ generated by ℓ. Let

$$\kappa \colon H^0(G, U/MU) \to H^0(G, \mathbb{F}_{\mathbf{r}}^{\times}/\mathbb{F}_{\mathbf{r}}^{\times M}) \overset{\text{Satz 90}}{=\!=} \mathbb{F}^{\times}/\mathbb{F}^{\times M}$$

be the homomorphism induced by ξ. Let

$$\{c_r \in H^0(G, U/MU)\}_{r|\mathbf{r}}$$

be any system of classes satisfying the universal Kolyvagin recursion. Then the corresponding system of classes

$$\{\kappa c_r \in \mathbb{F}^{\times}/\mathbb{F}^{\times M}\}_{r|\mathbf{r}}$$

satisfies the Kolyvagin recursion.

Proof Fix a positive integer r dividing $\mathbf{r}$ and a prime number ℓ. It suffices to prove the following two assertions:

1. $(\ell, r) = 1 \Rightarrow \kappa c_r \in \mathcal{O}_{(\ell)}^{\times}/\mathcal{O}_{(\ell)}^{\times M}$.
2. $\ell | r \Rightarrow \exp_\ell[\kappa c_r]_\ell = \nu_\ell \kappa c_{r/\ell}$.

We have $\xi U_r \subset \mathcal{O}_r^{\times}$ by the G-equivariance of ξ, whence assertion 1 via Lemma 2.2. We turn to the proof of assertion 2. By hypothesis ℓ divides r. Fix

$$\tilde{c}_r \in U_r, \quad \tilde{c}_{r/\ell} \in U_{r/\ell}$$

representing the classes c_r and $c_{r/\ell}$, respectively. Write

$$\xi \tilde{c}_r := \alpha_r \beta_r^M (\alpha_r \in \mathbb{F}^{\times}, \beta_r \in \mathbb{F}_r^{\times})$$

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

and

$$\xi\tilde{c}_{r/\ell} = \alpha_{r/\ell}\beta^{M}_{r/\ell}(\alpha_{r/\ell} \in \mathcal{O}^{\times}_{(\ell)}, \beta_{r/\ell} \in \mathcal{O}^{\times}_{r,(\ell)}).$$

One then has

$$\xi\left(\frac{(\sigma_\ell - 1)\tilde{c}_r}{M}\right) = \beta_r^{(\sigma_\ell - 1)}, \quad \xi\left(\frac{(\ell - \mathrm{Frob}_\ell)\tilde{c}_{r/\ell}}{M}\right) = \alpha_{r/\ell}^{\frac{(\ell-1)}{M}}\beta_{r/\ell}^{\ell - \mathrm{Frob}_\ell}$$

since there are no nontrivial M-th roots of unity in $\mathcal{O}_r^{\times}$. Choose $\gamma_r \in \mathbb{F}_\ell^{\times}$ such that

$$\gamma_r^{N_\ell} \text{ and } \alpha_r \text{ generate the same fractional } \mathcal{O}_{(\ell)}\text{-ideal.}$$

One then has

$$\gamma_r^{\frac{\ell-1}{M}}\beta_r \in \mathcal{O}^{\times}_{r,(\ell)}.$$

Finally, one has

$$(\gamma_r^{1-\sigma_\ell})^{\frac{\ell-1}{M}} \equiv \beta_r^{\sigma_\ell - 1} \equiv \alpha_{r/\ell}^{\frac{\ell-1}{M}}\beta_{r/\ell}^{\ell-\mathrm{Frob}_\ell} \equiv \alpha_{r/\ell}^{\frac{\ell-1}{M}} \mod \sqrt{\ell\mathcal{O}_{r,(\ell)}}$$

where the crucial middle congruence holds by Proposition/Definition 3.7 and hypothesis. Therefore assertion 2 holds and the proposition is proved. ■

4 Comparisons

4.1 The Universal Euler System

For each positive integer r dividing $\mathbf{r}$, let

$$x_r \in U_r \subset U$$

be the class represented by

$$\left[\sum_{p|r}\frac{1}{p}\right] \in \mathcal{A}(r)$$

where the interior sum is extended over all primes p dividing r. For all positive integers r dividing $\mathbf{r}$ and prime numbers ℓ dividing r the following clearly hold:

- $N_\ell x_r = (\mathrm{Frob}_\ell - 1)x_{r/\ell}$.
- $x_r \equiv x_{r/\ell} \bmod I_\ell$.

We call the family

$$\{x_r \in U\}_{r|\mathbf{r}}$$

the *universal Euler system*.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

4.2 Recovery of the Euler System by Specialization

One can easily verify the existence of a unique G-equivariant homomorphism

$$\xi\colon U \to \mathcal{O}_{\mathbf{r}}^{\times}$$

such that

$$\xi x_r = \xi_r$$

for all positive integers r dividing $\mathbf{r}$. Thus the given Euler system $\{\xi_r\}$ is recovered by specialization via the homomorphism ξ from the universal Euler system $\{x_r\}$. Note that

$$\xi I_\ell \subset 1 + \sqrt{\ell \mathcal{O}_{\mathbf{r},(\ell)}}$$

for all primes ℓ dividing $\mathbf{r}$.

4.3 Universal Kolyvagin Classes

Fix a positive integer r dividing $\mathbf{r}$. We claim that

$$N_r' x_r \in U_r \subset U$$

represents a class

$$c_r \in H^0(G_r, U_r/MU_r) = H^0(G, U_r/MU_r) \subset H^0(G, U/MU).$$

For each prime ℓ dividing r one has

$$(\sigma_\ell - 1)N_r' x_r \equiv -N_\ell N_{r/\ell}' x_r \equiv -(\mathrm{Frob}_\ell - 1)N_{r/\ell}' x_{r/\ell} \equiv 0 \bmod MU_r$$

by induction on the number of prime divisors of r. Therefore c_r is indeed G_r-invariant. We call c_r the *universal Kolyvagin class* indexed by r.

4.4 Recovery of the Kolyvagin Classes By Specialization

Let

$$\kappa\colon H^0(G, U/MU) \to H^0(G, \mathbb{F}_{\mathbf{r}}^{\times}/\mathbb{F}_{\mathbf{r}}^{\times M}) \overset{\text{Satz 90}}{=\!=} \mathbb{F}^{\times}/\mathbb{F}^{\times M}$$

be the homomorphism induced by ξ. For all positive integers r dividing $\mathbf{r}$ one has

$$\xi N_r' x_r = \xi_r^{N_r'}$$

and hence

$$\kappa c_r = \kappa_r.$$

Thus the system $\{\kappa_r\}$ of Kolyvagin classes is recovered by specialization via the homomorphism κ from the system $\{c_r\}$ of universal Kolyvagin classes.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

Proposition 4.5 *The universal Kolyvagin classes satisfy the universal Kolyvagin recursion.*

Proof Fix a positive integer r dividing $\mathbf{r}$. By definition the universal Kolyvagin class c_r is represented by $N_r' x_r \in U_r$ and hence $c_r \in H^0(G, U_r/MU_r)$. One has an identity

$$\frac{(\sigma_\ell - 1)N_r' x_r}{M} = \frac{\ell - 1}{M} \cdot N_{r/\ell}'(x_r - x_{r/\ell}) + \frac{(\ell - \mathrm{Frob}_\ell)N_{r/\ell}' x_{r/\ell}}{M}$$

and hence $D_\ell c_r = c_{r/\ell}$ by Proposition/Definition 3.7. ■

4.6 Remark

From Propositions 3.9 and 4.5 one recovers the Proposition 2.5 (the latter being a reformulation of the well known Proposition 2.4 of the Rubin appendix to Lang's text [4]) by somewhat more conceptual means. We wonder if various well known generalizations of Proposition 2.5 (we have uppermost in mind Theorem 4.5.4 on p. 91 of Rubin's book [6]) could be analogously recovered.

5 The Action of D_ℓ on the Canonical Basis For $H^0(G, U/MU)$

5.1 The Bigraded $\mathbb{Z}[G]$-Module K

Let K be the free abelian group on symbols of the form

$$[a, g, h] \left(\begin{array}{c} g\text{: positive integer dividing } \mathbf{r} \\ h\text{: positive integer dividing some power of } \mathbf{r} \\ a \in \frac{g}{\mathbf{r}}\mathbb{Z}/\mathbb{Z} \end{array} \right).$$

We equip the group K with a bigrading and associated total grading by declaring that

$$(\text{bidegree of } [a, g, h]) := \Big(-\sum_\ell \mathrm{ord}_\ell\, g, \sum_\ell \mathrm{ord}_\ell\, h \Big),$$

$$(\text{total degree of } [a, g, h]) := -\sum_\ell \mathrm{ord}_\ell\, g + \sum_\ell \mathrm{ord}_\ell\, h.$$

We equip the group K with the unique structure of bigraded $\mathbb{Z}[G]$-module such that

$$\sigma[a, g, h] = [a', g', h'] \Leftrightarrow \big(\sigma\phi(a) = \phi(b) \text{ and } g = g' \text{ and } h = h' \big)$$

for all symbols $[a, g, h]$ and $[a', g', h']$ in the canonical basis of K, injective homomorphisms $\phi\colon \frac{1}{\mathbf{r}}\mathbb{Z}/\mathbb{Z} \to \mathbb{F}_{\mathbf{r}}^\times$ and $\sigma \in G$.

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

5.2 The Differentials d and δ

For each prime number ℓ dividing $\mathbf{r}$ we define a G-equivariant differential $d_\ell \colon K \to K$ of bidegree $(1,0)$ by the rule

$$d_\ell[a,g,h] := \begin{cases} (-1)^{\sum_{\ell'<\ell} \operatorname{ord}_{\ell'} gh}([a,g/\ell,h] - \sum_{\ell b = a}[b,g/\ell,h]) & \text{if } \ell | g, \\ 0 & \text{otherwise,} \end{cases}$$

and a G-equivariant differential $\delta_\ell \colon K \to K$ of bidegree $(0,1)$ by the rule

$$\delta_\ell[a,g,h] := (-1)^{\operatorname{ord}_\ell g + \sum_{\ell'<\ell} \operatorname{ord}_\ell gh} \begin{cases} (1-\sigma_\ell)[a,g,h\ell] & \text{if } \operatorname{ord}_\ell h \equiv 0 \bmod 2, \\ N_\ell[a,g,h\ell] & \text{if } \operatorname{ord}_\ell h \equiv 1 \bmod 2. \end{cases}$$

One can verify by a straightforward calculation that any two distinct operators in the family $\{d_\ell\} \cup \{\delta_\ell\}$ anticommute. We equip K with anti-commuting differentials d and δ of bidegree $(1,0)$ and $(0,1)$, respectively by the rules

$$d[a,g,h] := \sum_\ell d_\ell[a,g,h], \qquad \delta[a,g,h] := \sum_\ell \delta_\ell[a,g,h].$$

Since the sums above contain but finitely many nonzero terms, in fact d and δ are well-defined. Thus we have defined a double complex (K,d,δ) in the category of G-modules.

5.3 Comparison With Ouyang's Definitions

We define an involutive G-equivariant bigraded automorphism ϵ of K by the rule

$$\epsilon[a,g,h] := (-1)^{\sum_{\ell'<\ell}(\operatorname{ord}_\ell g)\cdot(\operatorname{ord}_{\ell'} h)}[a,g,h].$$

By a straightforward calculation one finds that

$$\epsilon d_\ell \epsilon[a,g,h] = \begin{cases} (-1)^{\sum_{\ell'<\ell} \operatorname{ord}_{\ell'} g}([a,g/\ell,h] - \sum_{\ell b = a}[b,g/\ell,h]) & \text{if } \ell | g \\ 0 & \text{otherwise.} \end{cases}$$

and

$$\epsilon\delta_\ell\epsilon[a,g,h] = (-1)^{\sum_{\ell'} \operatorname{ord}_{\ell'} g + \sum_{\ell'<\ell} \operatorname{ord}_{\ell'} h} \begin{cases} (1-\sigma_\ell)[a,g,h\ell] & \text{if } \operatorname{ord}_\ell h \equiv 0 \bmod 2, \\ N_\ell[a,g,h\ell] & \text{if } \operatorname{ord}_\ell h \equiv 1 \bmod 2. \end{cases}$$

It follows that d (resp. δ) as defined in this paper is ϵ-conjugate to d (resp. δ) as defined by the rule appearing on p. 14 of Ouyang's paper [5] and hence *mutatis mutandis* Ouyang's theory applies to the double complex (K,d,δ).

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

5.4 Identification of $H^0(K/MK, d+\delta)$ With $H^0(G, U/MU)$

For any positive integer r dividing $\mathbf{r}$ let $K(r)$ be the subgroup of K generated by all symbols of the form

$$[a,g,h]\left(\begin{array}{c} g\text{: positive integer dividing } r\\ h\text{: positive integer dividing some power of } r\\ a\in \frac{g}{r}\mathbb{Z}/\mathbb{Z}\end{array}\right)$$

Then $K(r)$ is G-, d-, and δ-stable. It is explained in detail in Ouyang's paper [5] how to make the identification

$$H^*\big(K(r)/MK(r), d+\delta\big) = H^*(G_r, U_r/MU_r).$$

For our purposes in this note it is enough simply to know that the G-equivariant homomorphism

$$\begin{gathered}\big((\text{class represented by } [a,1,1]) \mapsto (\text{class represented by } [a])\big)\\ : \big(\text{bidegree } (0,0) \text{ component of } K(r)/MK(r)\big) \to U_r/MU_r\end{gathered}$$

induces an isomorphism

$$H^0\big(K(r)/MK(r), d+\delta\big) \xrightarrow{\sim} H^0(G_r, U_r/MU_r) = H^0(G, U_r/MU_r).$$

Then, passing to the limit over r, we find that the G-equivariant homomorphism

$$\begin{gathered}\big((\text{class represented by } [a,1,1]) \mapsto (\text{class represented by } [a])\big)\\ : (\text{bidegree } (0,0) \text{ component of } K/MK) \to U/MU\end{gathered}$$

induces an isomorphism

$$H^0(K/MK, d+\delta) \xrightarrow{\sim} H^0(G, U/MU).$$

The latter fact can be also be verified directly by a straightforward spectral sequence argument, the key observation being that the subcomplexes of K with fixed ordinate are direct sums of copies of the complex (L, d) discussed in Section 3.5.

5.5 The Canonical Basis For $H^0(G_r, U_r/MU_r)$

Fix a positive integer r dividing $\mathbf{r}$. Let $S(r)$ be the bigraded G-, d- and δ-stable subgroup of $K(r)$ generated by all symbols $[a,g,h]$ of the canonical basis of $K(r)$ of the form

$$[a,g,h](\text{if } a=0, \text{ then } g \text{ does not divide } h).$$

By Proposition 5.4 on p. 20 of Ouyang's paper [5], which is the main technical result of that paper, the quotient map

$$\big(K(r), d+\delta\big) \to \big(K(r)/S(r), d+\delta\big)$$

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

is a quasi-isomorphism of complexes. Ouyang's result is proved by verifying that the induced map of spectral sequences is an isomorphism at E_2. Clearly the family of symbols of the form

$$[0, g, gh] \left(\begin{array}{c} g\text{: positive integer dividing } r \\ h\text{: positive integer dividing some power of } r \end{array}\right)$$

forms a graded basis for $K(r)/S(r)$; moreover, it is easy to check that

$$dK(r) + \delta K(r) \subset S(r) + MK(r).$$

The upshot is that there exists a unique $\mathbb{Z}/M\mathbb{Z}$-basis

$$\{\bar{c}_g \in H^0(G, U_r/MU_r)\}_{g|r}$$

indexed by the positive integers g dividing r such that the corresponding class $\bar{c}_g$ is represented by a 0-cocycle of the complex $\bigl(K(r)/MK(r), d + \delta\bigr)$ congruent modulo $S(r) + MK(r)$ to the symbol $[0, g, g]$. Up to signs determined by the automorphism ϵ defined in Section 5.3, the canonical basis constructed here coincides with the canonical basis provided by Theorem 5.5 on p. 22 of Ouyang's paper [5].

5.6 The Canonical Basis For $H^0(G, U/MU)$

Let S be the bigraded G-, d- and δ-stable subgroup of K generated by all symbols $[a, g, h]$ of the canonical basis of K of the form

$$[a, g, h] (\text{if } a = 0, \text{ then } g \text{ does not divide } h).$$

We have

$$K = \bigcup_{r|\mathbf{r}} K(r), \quad S = \bigcup_{r|\mathbf{r}} S(r)$$

where in both unions r ranges over the positive integers dividing $\mathbf{r}$. Passing to the limit over r in the obvious way, we find that there exists a unique $\mathbb{Z}/M\mathbb{Z}$-basis

$$\{\bar{c}_r \in H^0(G_r, U_r/MU_r)\}_{r|\mathbf{r}}$$

for $H^0(G, U/MU)$ indexed by the positive integers r dividing $\mathbf{r}$ such that the corresponding class $\bar{c}_r$ admits representation by a 0-cocycle of the complex $\bigl(K(r)/MK(r), d + \delta\bigr)$ congruent modulo $S(r) + MK(r)$ to the symbol $[0, r, r]$. We call the family $\{\bar{c}_r\}$ the *canonical basis* for $H^0(G, U/MU)$.

5.7 The Diagonal Shift Operator Δ_ℓ

For each prime number ℓ dividing $\mathbf{r}$, we define the corresponding *diagonal shift* operator Δ_ℓ on K of bidegree $(1, -1)$ by the rule

$$\Delta_\ell[a, g, h] := \begin{cases} [a, g/\ell, h/\ell] & \text{if } \ell|g \text{ and } \ell|h, \\ 0 & \text{otherwise.} \end{cases}$$

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

One has

$$\Delta_\ell d_p = d_p \Delta_\ell, \quad \Delta_\ell \delta_p = \delta_p \Delta_\ell$$

for all prime numbers p distinct from ℓ. One has

$$\Delta_\ell d_\ell = d_\ell \Delta_\ell = 0, \quad (\delta_\ell \Delta_\ell - \Delta_\ell \delta_\ell) K \subset MK.$$

For every positive integer r dividing $\mathbf{r}$ one has

$$\Delta_\ell K(r) \subset \begin{cases} K(r/\ell) & \text{if } \ell \text{ divides } r, \\ \{0\} & \text{otherwise.} \end{cases}$$

The action of Δ_ℓ therefore passes to

$$H^0\big(K(r)/MK(r), d+\delta\big) = H^0\big(G_r, U(r)/MU(r)\big)$$

and in the limit to

$$H^0(K/MK, d+\delta) = H^0(G, U/MU).$$

Our definition of the diagonal shift operation Δ_ℓ is inspired by a very similar diagonal shift operation defined on p. 3564 of the paper of Das [2] and exploited there to great advantage.

Proposition 5.8 *For each prime number ℓ dividing $\mathbf{r}$ the endomorphism of $H^0(G, U/MU)$ induced by the diagonal shift operation Δ_ℓ coincides with D_ℓ.*

Proof Fix a positive integer r dividing $\mathbf{r}$ and divisible by ℓ. Fix a class

$$c \in H^0(G_r, U_r/MU_r).$$

It suffices to show that D_ℓ and the endomorphism of $H^0(G, U/MU)$ induced by Δ_ℓ applied to c give the same result. Let $\mathbf{c}$ be a 0-chain in $K(r)$ reducing modulo $MK(r)$ to a 0-cycle representing c. Write

$$0 = (d+\delta)\mathbf{c} + M\mathbf{b}$$

where $\mathbf{b}$ is a 1-chain of $K(r)$. For any positive integer g dividing r and positive integer h dividing some power of r let

$$(\mathbf{a} \mapsto \mathbf{a} \otimes [g,h]) \colon \mathcal{A}(r/g) \to K(r)$$

be the unique homomorphism such that

$$[a] \otimes [g,h] := [a,g,h]$$

for all $a \in \frac{g}{r}\mathbb{Z}/\mathbb{Z}$. Write

$$\mathbf{c} = \sum \mathbf{c}_{g,h} \otimes [g,h], \quad \Delta_\ell \mathbf{c} = \sum \mathbf{c}_{g\ell,h\ell} \otimes [g,h] \big(\mathbf{c}_{g,h} \in \mathcal{A}(r/g)\big)$$

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press

and

$$\mathbf{b} = \sum \mathbf{b}_{g,h} \otimes [g,h]\big(\mathbf{b}_{g,h} \in \mathcal{A}(r/g)\big)$$

where all the sums are extended over pairs (g,h) consisting of a positive integer g dividing r and a positive integer h dividing a power of r. Let $\rho_\ell \colon \mathcal{A}(r) \to \mathcal{A}(r/\ell)$ and $\gamma_p \colon \mathcal{A}(r/p) \to \mathcal{A}(r)$ be as in the proof of Proposition/Definition 3.7. By hypothesis one has an identity

$$0 = \Big(\sum_{\substack{p|r\\ p<\ell}} \gamma_p \mathbf{c}_{p,\ell}\Big) + \gamma_\ell \mathbf{c}_{\ell,\ell} - \Big(\sum_{\substack{p|r\\ p>\ell}} \gamma_p \mathbf{c}_{p,\ell}\Big) + (1-\sigma_\ell)\mathbf{c}_{1,1} + M\mathbf{b}_{1,\ell}$$

and hence also an identity

$$0 = \Big(\sum_{\substack{p|r\\ p<\ell}} \gamma_p \rho_\ell \mathbf{c}_{p,\ell}\Big) - (\ell - \mathrm{Frob}_\ell)(\mathrm{Frob}_\ell^{-1}\, \mathbf{c}_{\ell,\ell}) - \Big(\sum_{\substack{p|r\\ p>\ell}} \gamma_p \rho_\ell \mathbf{c}_{p,\ell}\Big) + M\rho_\ell \mathbf{b}_{1,\ell}.$$

Let $x \in U_r$ be the element represented by $\mathbf{c}_{1,1}$ and let $y \in U_{r/\ell}$ be the element represented by $\mathbf{c}_{\ell,\ell}$. One the one hand, the class of $H^0(G_r, U_r/MU_r)$ represented by the 0-cocycle $\mathbf{c}$ mod M of the complex $\big(K(r)/MK(r), d+\delta\big)$ is x mod MU_r and the class of $H^0(G_{r/\ell}, U_{r/\ell}/MU_{r/\ell})$ represented by the 0-cocycle $\Delta_\ell \mathbf{c}$ mod M of the complex $\big(K(r/\ell)/MK(r/\ell), d+\delta\big)$ is y mod $MU_{r/\ell}$. But on the other hand, one has

$$\frac{(\sigma_\ell - 1)x}{M} \equiv \frac{(\ell - \mathrm{Frob}_\ell)y}{M} \bmod I_\ell$$

and hence

$$D_\ell(x \bmod MU) \equiv y \bmod MU_{\mathbf{r}/\ell}$$

by Proposition/Definition 3.7. Therefore the results of applying D_ℓ and the endomorphism of $H^0(G, U/MU)$ induced by Δ_ℓ to the class x mod MU indeed coincide. ■

Corollary 5.9 *The canonical basis $\{\bar{c}_r\}$ satisfies the universal Kolyvagin recursion.*

Proof Clear. ■

Corollary 5.10 *Any system of classes $\{b_r\}$ satisfying the universal Kolyvagin recursion and the normalization $b_1 = \bar{c}_1$ is a $\mathbb{Z}/M\mathbb{Z}$-basis of $H^0(G, U/MU)$.*

Proof Fix a positive integer r dividing $\mathbf{r}$ and arbitrarily and let

$$r = \ell_1 \cdots \ell_n$$

be the prime factorization of r. One then has

$$D_{\ell_1} \cdots D_{\ell_n} b_r = b_1 = \bar{c}_1 = D_{\ell_1} \cdots D_{\ell_n} \bar{c}_r$$

and hence

$$b_r - \bar{c}_r \in \ker\Big(H^0(G_r, U_r/MU_r) \xrightarrow{D_{\ell_1}\cdots D_{\ell_n}} H^0(G_r, U_r/MU_r)\Big) = \bigoplus_{\substack{r'|r\\ r'\neq r}} \mathbb{Z}/M\mathbb{Z} \cdot \bar{c}_{r'},$$

whence the result. ■

5.11 Remark

From Corollary 5.10 it follows in particular that the system $\{c_r\}$ of universal Kolyvagin classes defined in Section 4.3 is a $\mathbb{Z}/M\mathbb{Z}$-basis for $H^0(G, U/MU)$. More precisely, it follows that for every positive integer r dividing $\mathbf{r}$, the family $\{c_g\}_{g|r}$ is a $\mathbb{Z}/M\mathbb{Z}$-basis for $H^0(G_r, U_r/MU_r)$. The latter fact is none other than Theorem B on p. 2 of Ouyang's paper [5]; our way of proving Theorem B here is simpler than Ouyang's original method.

References

[1] G. W. Anderson, *A double complex for computing the sign-cohomology of the universal ordinary distribution*. Contemp. Math. **224**(1999), 1–27.

[2] P. Das, *Algebraic Gamma monomials and double coverings of cyclotomic fields*. Trans. Amer. Math. Soc. **352**(2000), 3557–3594.

[3] D. S. Kubert, *The universal ordinary distribution*. Bull. Soc. Math. France **107**(1979), 179–202.

[4] S. Lang, *Cyclotomic Fields I and II, combined 2^{nd} edition*. Grad. Texts in Math. **121**, Springer Verlag, 1990.

[5] Y. Ouyang, *Group cohomology of the universal ordinary distribution*. J. Reine Angew. Math. **537**(2001), 1–32.

[6] K. Rubin, *Euler systems*. Ann. of Math. Stud. **147**, Princeton University Press, 2000.

School of Mathematics
University of Minnesota
Minneapolis, Minnesota 55455
USA
e-mail: gwanders@math.umn.edu

Department of Mathematics
University of Toronto
100 St. George Street
Toronto, Ontario
M5S 3G3
e-mail: youyang@math.toronto.edu

https://doi.org/10.4153/CJM-2003-028-5 Published online by Cambridge University Press