Generalized Bockstein maps and Massey products

Yeuk Hay Joshua Lam, Yuan Liu, Romyar Sharifi, Preston Wake, Jiuya Wang

Abstract

Given a profinite group G of finite p-cohomological dimension and a pro-p quotient H of G by a closed normal subgroup N, we study the filtration on the Iwasawa cohomology of N by powers of the augmentation ideal in the group algebra of H. We show that the graded pieces are related to the cohomology of G via analogues of Bockstein maps for the powers of the augmentation ideal. For certain groups H, we relate the values of these generalized Bockstein maps to Massey products relative to a restricted class of defining systems depending on H. We apply our study to prove lower bounds on the p-ranks of class groups of certain nonabelian extensions of $\mathbb{Q}$ and to give a new proof of the vanishing of triple Massey products in Galois cohomology.

1 Introduction

At its essence, this paper revolves around the fundamental question of how the continuous cohomology of a profinite group G with compact coefficients compares with the cohomology of an open normal subgroup N. As a starting point, if G has cohomological dimension d, then the corestriction map from N to G induces an isomorphism from on G/N-coinvariants in degree d. In this paper, we introduce a sequence of generalized Bockstein maps $\Psi^{(n)}$ for $n \geq 0$ as a tool for refining this result and, more generally, allow N to be closed by considering Iwasawa cohomology. The powers of the augmentation ideal I of a completed group ring of G/N yield a natural filtration on the domain of corestriction. We show that the nth graded piece of this augmentation filtration is isomorphic to the cokernel of $\Psi^{(n)}$. We demonstrate how, in many cases, the image of $\Psi^{(n)}$ is described by n-fold Massey products.

Keywords: Bockstein maps, Massey products, augmentation ideal, continuous cohomology, profinite groups, absolute Galois groups, Iwasawa theory

MSC2020: 20J05, 20J06, 12G05 (Primary), 11R23, 11R34 (Secondary)

Our initial motivation for studying this problem came from Iwasawa theory. Indeed, Galois groups G with restricted ramification above a prime p have p-cohomological dimension is 2, and their second cohomology groups with coefficients in p-power roots of unity are closely related to ideal class groups. In such a setting, the fundamental question above translates to comparing ideal class groups as one goes up a tower of fields, the original question of Iwasawa theory. The idea that Massey products should be related to Iwasawa theory originates in [Sh2]. This paper distillates the purely algebraic results of that paper from the number theory. The distinct perspective using generalized Bockstein maps that we introduce here allows us to go beyond the procyclic setting of [Sh2]. We demonstrate how our methods can be used to derive concrete arithmetic results by proving lower bounds on the p-ranks of class groups of finite p-ramified bicyclic and Heisenberg extensions of $\mathbb{Q}(\mu_p)$. Though we eschew Iwasawa-theoretic applications in this paper to ground our study, a description of the augmentation filtrations of inverse limits of p-parts of class groups in $\mathbb{Z}_p$-extensions that is derived using our methods may be found in [Sh4].

We also consider applications of generalized Bockstein maps to the study of absolute Galois groups of fields, especially to the consideration of the Massey vanishing conjecture of Mináč and Tân [MT4]. Many algebraic properties of absolute Galois groups are encoded cohomologically as properties of the norm residue symbol. We show that these properties are naturally expressed in terms of generalized Bockstein maps. As an application, we give a new proof for odd primes of the triple Massey vanishing theorem of Efrat–Matzri [EfMa] and Mináč–Tân [MT3]. In fact, we show that it follows given one straightforward axiom on the profinite group that in the case of absolute Galois groups follows from properties of the norm residue symbol.

Mináč and Tân originally formulated the Massey vanishing conjecture, in part, as a way to help cohomologically characterize which profinite groups are isomorphic to absolute Galois groups of fields. We suspect that generalized Bockstein maps have an important role to play in formulating and understanding such cohomological characterizations.

1.1 Generalized Bockstein maps

Let G be a profinite group of p-cohomological dimension 2, and let H be a finitely generated pro-p quotient of G by a closed normal subgroup N. Let $\Omega = \mathbb{Z}_p[\![H]\!]$ denote the completed $\mathbb{Z}_p$-group ring of H, the inverse limit of the $\mathbb{Z}_p$-group rings of the finite quotients of H. Let T be a finitely generated $\mathbb{Z}_p$-module with a continuous action of G. This paper is concerned with the study of connecting maps in the G-cohomology of the augmentation filtration of the tensor product $T \otimes_{\mathbb{Z}_p} \Omega$. That is, if $I = \ker(\Omega \to \mathbb{Z}_p)$ denotes the augmentation ideal of Ω, then we have exact sequences

$$0 \to T \otimes_{\mathbb{Z}_p} I^n/I^{n+1} \to T \otimes_{\mathbb{Z}_p} \Omega/I^{n+1} \to T \otimes_{\mathbb{Z}_p} \Omega/I^n \to 0 \tag{1.1}$$

for each $n \geq 1$ such that Ω/I^n is $\mathbb{Z}_p$-flat. We study the connecting homomorphisms

$$\Psi^{(n)} \colon H^1(G, T \otimes_{\mathbb{Z}_p} \Omega/I^n) \to H^2(G,T) \otimes_{\mathbb{Z}_p} I^n/I^{n+1}$$

attached to these sequences, which we refer to as *generalized Bockstein maps*, due to their similarlity to usual Bockstein maps for exact sequences of p-power order cyclic groups.

We can use the Bockstein maps to partially describe the second *Iwasawa cohomology group* $H^2_{\mathrm{Iw}}(N,T)$ of N with T-coefficients. This cohomology group is the inverse limit of the groups $H^2(U,T)$ under corestriction maps, where U runs over the open normal subgroups of G containing N. It is naturally endowed, through the $\mathbb{Z}_p[G/U]$-actions on each $H^2(U,T)$, with the structure of an Ω-module. We prove that the cokernels of the generalized Bockstein maps describe the graded quotients in the augmentation filtration of $H^2_{\mathrm{Iw}}(N,T)$ (see Theorem 2.2.4).

Theorem A. *There are canonical isomorphisms*

$$\frac{I^n H^2_{\mathrm{Iw}}(N,T)}{I^{n+1} H^2_{\mathrm{Iw}}(N,T)} \cong \frac{H^2(G,T) \otimes_{\mathbb{Z}_p} I^n/I^{n+1}}{\operatorname{im} \Psi^{(n)}}.$$

The proof rests on an Iwasawa-cohomological version [LiSh, FuKa] of a descent spectral sequence of Tate, applied to the terms of our exact sequences for the augmentation filtration of Ω. We verify the compatibility of these spectral sequences with generalized Bockstein maps and a connecting map in the H-homology of the $\mathbb{Z}_p$-tensor product of $H^2_{\mathrm{Iw}}(N,T)$ with (1.1).

1.2 The image of $\Psi^{(n)}$ and Massey products

The case $H \cong \mathbb{Z}_p$ of Theorem A was first studied in [Sh2] from a different perspective and applied in an Iwasawa-theoretic context. Its main result has a similar form to Theorem A, but in place of the image of $\Psi^{(n)}$, it has a group of values of certain $(n+1)$-fold *Massey products*, which are higher operations in Galois cohomology generalizing cup products. We describe threefold Massey products after the statement of Theorem B below.

Here, we show that in the case that $H \cong \mathbb{Z}_p$, the values of generalized Bockstein maps are in fact values of certain Massey products relative to the *proper defining systems* introduced in [Sh2]. These systems reduce the indeterminacy inherent in the definition of a Massey product, which is only defined if certain lower Massey products vanish, and if defined still depends on the choice of a *defining system*, a homomorphism from G to a group of unipotent matrices modulo upper right-hand corners.

This raises the question of whether one can relate the values of generalized Bockstein maps and Massey products for more general groups H, especially, beyond the procyclic setting of [Sh2]. We shall discuss three classes of groups for which the answer is yes, the torsion-free groups in these being $\mathbb{Z}_p$, $\mathbb{Z}_p^2$ and the Heisenberg group over $\mathbb{Z}_p$.

The most difficult step in making the comparison is to obtain notions of proper defining systems of Massey products with values relating to projections of the values of the generalized Bockstein maps corresponding to elements of a $\mathbb{Z}_p$-basis of I^n/I^{n+1}, which is $\mathbb{Z}_p$-free. For this, we start with a *partial defining system*, which consists of a pair of homomorphisms from H to upper-triangular unipotent matrices of dimensions $a+1$ and $b+1$, where $a+b=n$. Our proper defining systems are extensions of these pairs viewed as maps on G to a defining system, with the two maps giving the two diagonal blocks in the defining system: see Definition 3.3.2.

For example, we prove the following result for $H \cong \mathbb{Z}_p^2$ in Theorem 4.4.3.

Theorem B. *Suppose that $\nu = (\chi, \psi)\colon H \to \mathbb{Z}_p^2$ is an isomorphism. Let $x, y \in I$ be such that $x+1$ and $y+1$ are group elements mapping under ν to the standard ordered basis of $\mathbb{Z}_p^2$. For $n \geq 2$, the cosets of $x^a y^{n-a}$ with $0 \leq a \leq n$ then form a $\mathbb{Z}_p$-basis for I^n/I^{n+1}.*

a. To a 1-cocycle $f\colon G \to T \otimes_{\mathbb{Z}_p} \Omega/I^n$ and $0 \leq a \leq n$, we can associate a proper defining system for an $(n+1)$-fold Massey product

$$(\chi^{(a)}, \lambda, \psi^{(n-a)}) := (\underbrace{\chi, \ldots, \chi}_{a \text{ times}}, \lambda, \underbrace{\psi, \ldots, \psi}_{n-a \text{ times}}) \in H^2(G, T),$$

where $\lambda\colon G \to T$ is the composition of f with the quotient map $T \otimes_{\mathbb{Z}_p} \Omega/I^n \to T \otimes_{\mathbb{Z}_p} \Omega/I \cong T$.

b. With the notation of part a, let $[f]$ denote the class of f in $H^1(G, T \otimes_{\mathbb{Z}_p} \Omega/I^n)$. Then

$$\Psi^{(n)}([f]) = \sum_{a=0}^{n} (\chi^{(a)}, \lambda, \psi^{(n-a)}) \otimes x^a y^{n-a}.$$

Let us illustrate Theorem B in some detail in the case that $n=2$ and $a=1$. In this case,

$$\Omega/I^2 = \mathbb{Z}_p[x, y]/(x^2, xy, y^2)$$

in the notation of the theorem. We can therefore write the 1-cocycle $f\colon G \to T \otimes_{\mathbb{Z}_p} \Omega/I^2$ as

$$f = \lambda + \lambda_x x + \lambda_y y,$$

with $\lambda_x, \lambda_y \colon G \to T$, abbreviating the tensor product as formal multiplication. Part a of Theorem B says that f gives rise to a defining system

$$\rho = \left(\begin{array}{cc|cc} 1 & \chi & \lambda_x & * \\ & 1 & \lambda & \lambda_y \\ \cline{3-4} \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & 1 & \psi \\ \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & & 1 \end{array}\right) : G \to U/Z$$

for the Massey triple product (χ, λ, ψ). Here, the values of ρ lie in the quotient of a group U of *generalized* upper-triangular unipotent 4-by-4 matrices by its subgroup Z of matrices with zero above-diagonal entries outside of the upper right-hand corner. The entries in the upper-right hand block are T-valued (and in particular $Z \cong T$), whereas they are $\mathbb{Z}_p$-valued outside of it. Matrix mulitplication proceeds using the $\mathbb{Z}_p$-module structure on T. That ρ is a defining system means that $\rho \colon G \to U/Z$ is a nonabelian 1-cocycle, where G acts on U coordinate-wise. The Massey product $(\chi, \lambda, \psi)_\rho$ relative to the defining system ρ is an element of $H^2(G, T)$ providing the obstruction to lifting ρ to a nonabelian 1-cocycle $G \to U$.

In general, even for such a cocycle ρ and therefore a Massey product (χ, λ, ψ) to exist, the cup products $\chi \cup \lambda$ and $\lambda \cup \psi$ must vanish in $H^2(G, T)$ so that cochains λ_x and λ_y can be chosen with $d\lambda_x = -\chi \cup \lambda$ and $d\lambda_y = -\lambda \cup \psi$. Even then, the class (χ, λ, ψ) depends on these choices. In our description, this vanishing is encapsulated in the fact that f is a 1-cocycle, and the indeterminacy is removed by fixing f.

The content of part b of Theorem B is that the coefficients of $\Psi^{(2)}([f])$ in $H^2(G, T)$ for the $\mathbb{Z}_p$-basis x^2, xy, and y^2 of I^2/I^3 are triple Massey products: in particular, the coefficient of xy is the Massey product $(\chi, \lambda, \psi)_\rho$ for the defining system ρ. More precisely, $(\chi, \lambda, \psi)_\rho$ is defined as class of the 2-cocycle $F \colon G^2 \to T$ given by

$$F \colon (g, h) \mapsto \chi(g) g\lambda_x(h) + \psi(h)\lambda_y(g).$$

This cocycle F arises as the upper-right hand corner of $(g, h) \mapsto \tilde{\rho}(g) \cdot g\tilde{\rho}(h)$ for the naive lift of ρ to a cochain $\tilde{\rho} \colon G \to U$ with zero upper-right hand corner. The theorem boils down to the fact that $F \cdot xy$ is also exactly the coboundary of the naive lift of f to a cochain $G \to \mathbb{Z}_p[x, y]/(x^2, y^2)$ with zero xy-coefficient.

From our perspective, the generalized Bockstein maps are more flexible than Massey products, being connecting homomorphisms more directly amenable to basic applications of homological algebra. For instance, the argument proving Theorem A for arbitrary H amounts to a diagram chase for maps of Grothendieck spectral sequences. Moreover, Theorem B allows us to study defining systems using abelian, rather than nonabelian, cocycles.

1.3 Galois groups with restricted ramification and class groups

At its core, our work is motivated by the potential arithmetic applications. One has at least something of an understanding of class groups of cyclotomic fields through Bernoulli numbers and thereby L-functions, and most notably via tfhe Iwasawa main conjecture (theorem of Mazur-Wiles). However, little is known about p-adic analytic invariants describing aspects of class groups of non-CM extensions of $\mathbb{Q}$.

One does have at least a partial understanding of the structure of p-parts of class groups of p-ramified $\mathbb{F}_p$-extensions of $\mathbb{Q}(\mu_p)$ through known values of cup products of cyclotomic p-units, and in certain instances one can give lower bounds on p-ranks of these groups (see [Sh2, Section 7]). In Section 5, we consider more complex extensions, deriving lower bounds on the p-ranks of class groups of p-ramified bicyclic and Heisenberg extensions of $\mathbb{Q}(\mu_p)$ in cases where standard genus theory does not produce any unramified extensions. The key tools in this work are Theorem A, our descriptions of the generalized Bockstein maps $\Psi^{(n)}$ for $n \in \{1, 2\}$, and computations of cup products of cyclotomic units from [McS].

We consider the case that the class group of $\mathbb{Q}(\mu_p)$ has p-rank 1. Suppose we have an $\mathbb{F}_p^2$-extension K of $\mathbb{Q}(\mu_p)$ that is Galois over $\mathbb{Q}$ for which the cup product pairing with the Kummer cocycle of the Kummer generators of the $\mathbb{F}_p^2$-extension vanish. Under certain assumptions on the action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ on these Kummer generators, we can show that the p-rank of the class group of K is at least 6 (see Proposition 5.2.1). This $\mathbb{F}_p^2$-extension K is then further contained in a Heisenberg extension L of $\mathbb{Q}(\mu_p)$ of degree p^3 that is Galois over $\mathbb{Q}$, and the p-rank of its class group is at least 7 (see Proposition 5.2.3). The smallest irregular prime p for which there exist $\mathbb{F}_p^2$-extensions for which these lower bounds are shown to hold by our methods is 101.

In the preprint [Sh4], the results of this paper are applied in the setting of Iwasawa theory to study inverse limits of class groups. There, G is the Galois group of the maximal extension of a number field unramified outside a finite set of primes containing those above p, and H is the Galois group of a $\mathbb{Z}_p$-extension. The group $H^2_{\mathrm{Iw}}(N, \mathbb{Z}_p(1))$ is closely related to but not always isomorphic to the usual inverse limit X of class groups up the tower defined by H. The isomorphisms of Theorem A are then used to derive exact sequences describing the graded pieces in the augmentation filtration of X.

1.4 Absolute Galois groups and the Massey vanishing conjecture

Let G be a profinite group and let p be a prime number. Let $\chi \in H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p)$. Consider the sequence

$$H^1(\ker \chi, \mathbb{F}_p) \xrightarrow{\mathrm{cor}} H^1(G, \mathbb{F}_p) \xrightarrow{\chi \cup} H^2(G, \mathbb{F}_p) \xrightarrow{\mathrm{res}} H^2(\ker \chi, \mathbb{F}_p). \tag{1.2}$$

If $G = G_F$ is the absolute Galois group of a field F that contains a primitive pth root of unity, then this sequence is exact, as can be seen using the properties of the norm residue symbol. This exactness is an important property of absolute Galois groups – for example, it is used heavily in the proof of the norm residue isomorphism theorem (Milnor-Bloch-Kato conjecture) by Voevodsky and Rost (see [Vo]).

Using Theorem B, we show that:

(i) The sequence (1.2) is exact at $H^1(G, \mathbb{F}_p)$ if and only if all p-fold Massey products of the form $(\chi^{(p-1)}, \lambda)$ with $\chi \cup \lambda = 0$ vanish for some proper defining system.

(ii) If (1.2) is exact at $H^2(G, \mathbb{F}_p)$, then it is exact.

In light of (i), we say that a group G has the *p-cyclic Massey vanishing property* if the sequence (1.2) is exact at $H^1(G, \mathbb{F}_p)$ for every $\chi \in H^1(G, \mathbb{F}_p)$. We prove the following in Theorem 6.2.1.

Theorem C. *Let G be a profinite group with the p-cyclic Massey vanishing property for an odd prime p. Then every triple Massey product on $H^1(G, \mathbb{F}_p)$ which is defined contains zero.*

If F is a field containing a primitive pth root of unity, then its absolute Galois group G_F has the p-cyclic Massey vanishing property. Hence Theorem C implies that every triple Massey product on $H^1(G_F, \mathbb{F}_p)$ which is defined contains zero. This is the *triple Massey vanishing* theorem of Efrat–Matzri [EfMa] and Mináč–Tân [MT3] for odd p (which implies the vanishing for arbitrary fields as in the latter paper). For more discussion about absolute Galois groups and the general Massey vanishing conjecture of [MT4], see the introduction to Section 6.

In our proof of Theorem C, to show that a defined Massey product (χ, λ, ψ) vanishes, we consider the coimage H of the map $(\chi, \psi)\colon G \to \mathbb{F}_p^2$, let $\Omega = \mathbb{F}_p[H]$, and let $I \subset \Omega$ be the augmentation ideal. We then apply a variant of Theorem B to this H to see that the Massey product (χ, λ, ψ) relative to a certain defining system is the obstruction to lifting λ to a class in $H^1(G, \Omega/J)$ for a particular ideal J between I^2 and I^3. Via an involved diagram chase, we see that the p-cyclic Massey vanishing property for the quotients of H that are the coimages of χ, ψ, and $\chi + \psi$ implies that this obstruction equals $\nu \cup (\chi + \psi)$ for some $\nu \in H^1(G, \mathbb{F}_p)$. This is enough to show that the Massey product contains zero.

Theorem C raises several interesting questions that we do not attempt to address here, including whether or not the vanishing of Massey products $(\chi^{(n)}, \psi)$ for arbitrary n is sufficient to imply Massey vanishing.

Acknowledgments. This paper arose out of a project of the first, second, and fifth authors at the 2018 Arizona Winter School on Iwasawa theory that was proposed by the third and led by the third and fourth authors. We would like to thank the AWS for the stimulating environment that enabled our collaboration. We would also like to thank Nguyễn Duy Tân for helpful comments on a earlier draft of this article. The third author's research was supported in part by the National Science Foundation under Grant No. DMS-1801963. The fourth author's research was supported in part by the National Science Foundation under Grant No. DMS-1901867. The fifth author was partially supported by a Foerster-Berstein Fellowship at Duke University.

2 Generalized Bockstein maps

In this section, we define generalized Bockstein maps and employ them in the study of the structure of inverse limits of cohomology groups. Throughout, we use the following objects:

- a profinite group G,
- a topologically finitely generated pro-p quotient H of G by a closed normal subgroup N,
- a compact Noetherian $\mathbb{Z}_p$-algebra R (usually taken to be a quotient of $\mathbb{Z}_p$),
- the completed group ring $\Omega = R[\![H]\!]$,
- the augmentation ideal I of Ω, i.e., the kernel of the continuous R-algebra homomorphism $\Omega \to R$ that sends every group element in H to 1,
- a positive integer n such that Ω/I^n and I^n/I^{n+1} are R-flat, and
- a compact $R[\![G]\!]$-module T that is R-finitely generated.

Note that a compact $R[\![G]\!]$-module is the same as a compact R-module with a continuous R-linear action of G. We will frequently take tensor products $M \otimes_R M'$ of compact $R[\![G]\!]$-modules M and M', at least one of which is finitely generated over R. These compact R-modules (with the topology of the isomorphic completed tensor product) have the diagonal action of G.

2.1 Augmentation sequences

Since we have assumed that Ω/I^n is R-flat, the right exact sequence of compact $R[\![G]\!]$-modules

$$0 \to T \otimes_R I^n/I^{n+1} \to T \otimes_R \Omega/I^{n+1} \to T \otimes_R \Omega/I^n \to 0 \tag{2.1}$$

is exact. For any $d \geq 1$, we have the resulting connecting homomorphisms

$$H^{d-1}(G, T \otimes_R \Omega/I^n) \to H^d(G, T \otimes_R I^n/I^{n+1})$$

on continuous G-cohomology.

Since G acts trivially on the finitely generated R-module I^n/I^{n+1}, we have a homomorphism

$$H^d(G,T) \otimes_R I^n/I^{n+1} \to H^d(G, T \otimes_R I^n/I^{n+1}) \tag{2.2}$$

that is an isomorphism as I^n/I^{n+1} is R-flat, so long as we assume either that G has finite p-cohomological dimension or that I^n/I^{n+1} has a finite resolution by projective R-modules (see [LiSh, Proposition 3.1.3], the proof of which does not use the assumption on R in that section). The latter condition is automatic, given that I^n/I^{n+1} is flat, if R is a quotient of $\mathbb{Z}_p$. We let

$$\Psi^{(n)} \colon H^{d-1}(G, T \otimes_R \Omega/I^n) \to H^d(G,T) \otimes_R I^n/I^{n+1}. \tag{2.3}$$

denote the resulting composite map, and we refer to it as a *generalized Bockstein map*.

Remark 2.1.1. We may replace the assumption that Ω/I^n is R-flat with the assumption that T is R-flat in order that (2.1) still hold. We may also replace the assumption that I^n/I^{n+1} is R-flat with the assumption that G has p-cohomological dimension d and still have an isomorphism as in (2.2). (To see this, choose a presentation of I^n/I^{n+1} by finitely generated free R-modules and use the right exactness of the dth cohomology functor and the tensor product, noting that $H^d(G, T^r) \cong H^d(G,T) \otimes_R R^r$ for any r.) With either replacement, $\Psi^{(n)}$ is still a map as in (2.3).

2.2 Graded quotients of Iwasawa cohomology groups

Recall that N denotes the kernel of the surjection $G \to H$. Our interest in this section is in the *Iwasawa cohomology groups*

$$H^i_{\mathrm{Iw}}(N,T) = \varprojlim_{N \leq U \trianglelefteq^o G} H^i(U,T)$$

for $i \geq 1$, where the inverse limit is taken with respect to corestriction maps over open normal subgroups U of G containing N. Note that the Iwasawa cohomology groups are relative to the larger group G, though this is omitted from our notation. Since each $H^i(U,T)$ is a $R[G/U]$-module and the actions are compatible with corestriction, the group $H^i_{\mathrm{Iw}}(N,T)$ is endowed with the structure of an Ω-module.

Remark 2.2.1. If H is finite, then $H^i_{\mathrm{Iw}}(N,T) = H^i(N,T)$.

Let us define two notions that we need. First, a profinite group $\mathcal{G}$ is *p-cohomologically finite* if $\mathcal{G}$ has finite p-cohomological dimension and $H^i(\mathcal{G},M)$ is finite for every finite $\mathbb{Z}_p[\mathcal{G}]$-module M and $i \geq 0$. Second, a *compact p-adic Lie group* is a profinite group that has an open pro-p subgroup any closed subgroup of which can be topologically generated by r elements for some fixed r. Equivalently, a compact p-adic Lie group is any profinite group continuously isomorphic to a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ for some $n \geq 1$.

We make the following assumptions for the rest of this section:

- G is p-cohomologically finite of p-cohomological dimension d,
- R is a complete commutative local Noetherian $\mathbb{Z}_p$-algebra with finite residue field, and
- either
  - (i) H is a compact p-adic Lie group or
  - (ii) T has a finite resolution by a complex of $R[\![G]\!]$-modules free of finite rank over R.

Recall that the zeroth H-homology group of a compact Ω-module M is its coinvariant module $M_H \cong M/IM$. In our setting, corestriction provides an isomorphism on coinvariants in degree d (see [NSW, Proposition 3.3.11]), which is to say that we have a natural isomorphism

$$\frac{H^d_{\mathrm{Iw}}(N,T)}{IH^d_{\mathrm{Iw}}(N,T)} \cong H^d(G,T). \tag{2.4}$$

This gives rise to a Grothendieck spectral sequence for the implicit composition of right exact functors, which is a version of Tate's descent spectral sequence for Iwasawa cohomology

Proposition 2.2.2 (Fukaya-Kato, Lim-Sharifi)**.** *The Ω-modules $H^i_{\mathrm{Iw}}(N,T)$ are finitely generated for all $i \geq 0$. Moreover, we have a first quadrant homological spectral sequence of R-modules*

$$E^2_{i,j}(T) = H_i(H, H^{d-j}_{\mathrm{Iw}}(N,T)) \Rightarrow E_{i+j}(T) = H^{d-i-j}(G,T),$$

where d is the p-cohomological dimension of G.

This result is proven in [Ta, Theorem 1] if H is finite, and it follows from [FuKa, Proposition 1.6.5] if (ii) holds and from [LiSh, Propositions 3.1.3 and 3.2.4] if (i) holds.

The isomorphism (2.4) and the other edge maps on coinvariant groups in this spectral sequence are given by the inverse limits of corestriction maps. This isomorphism forces the nth graded quotient $I^nA/I^{n+1}A$ in the augmentation filtration of $A = H^d_{\mathrm{Iw}}(N,T)$ to be a quotient of $H^d(G,T) \otimes_R I^n/I^{n+1}$ using the surjective map

$$A/IA \otimes_R I^n/I^{n+1} \to I^nA/I^{n+1}A$$

induced by the map $A \times I^n \to I^nA$ given by the multiplication $(a,x) \mapsto xa$. As we shall see, this quotient is in fact $\operatorname{coker} \Psi^{(n)}$.

Recall that we have assumed that Ω/I^n is R-flat. Moreover, the fact that H is topologically finitely generated implies that Ω/I^n is finitely generated over R.

Lemma 2.2.3. *Let A be an Ω-module, and consider the exact sequence*

$$0 \to A \otimes_R I^n/I^{n+1} \to A \otimes_R \Omega/I^{n+1} \to A \otimes_R \Omega/I^n \to 0. \tag{2.5}$$

The connecting homomorphism

$$\partial_n \colon H_1(H, A \otimes_R \Omega/I^n) \to A_H \otimes_R I^n/I^{n+1}$$

in the H-homology of (2.5) *has cokernel isomorphic to $I^nA/I^{n+1}A$.*

Proof. We have compatible, natural isomorphisms of R-modules

$$(A \otimes_R \Omega/I^m)_H \cong \Omega/I^m \otimes_\Omega A \cong A/I^mA$$

for $m \geq 1$ given on $a \in A$ and $\omega \in \Omega$ (or its quotient by I^m) by

$$a \otimes \omega \mapsto \iota(\omega) \otimes a \mapsto \iota(\omega)a,$$

where $\iota\colon \Omega \to \Omega$ is the unique continuous R-linear map given by inversion of group elements on H. Note that the switch of terms in the tensor product in the first isomorphism is necessitated by the fact that A is a left Ω-module. (In fact, these become isomorphisms of Ω-modules since $a \otimes \omega h^{-1} \mapsto h \cdot \iota(\omega) \otimes a$ for $h \in H$ under the first map.)

By the long exact sequence in H-homology and the above isomorphisms, the cokernel of interest is identified with the kernel of the quotient map $A/I^{n+1}A \to A/I^nA$, hence the result. □

We now come to our theorem.

Theorem 2.2.4. *For each $n \geq 1$, there is a canonical isomorphism*

$$\frac{I^n H^d_{\mathrm{Iw}}(N,T)}{I^{n+1} H^d_{\mathrm{Iw}}(N,T)} \cong \frac{H^d(G,T) \otimes_R I^n/I^{n+1}}{\operatorname{im} \Psi^{(n)}}$$

of R-modules, where d is the p-cohomological dimension of G.

Proof. There are isomorphisms

$$H^d_{\mathrm{Iw}}(N, T \otimes_R M) \cong H^d_{\mathrm{Iw}}(N,T) \otimes_R M$$

for any compact $R[\![G]\!]$-module M finitely generated over R, since G has p-cohomological dimension d. In particular, the following sequence is exact:

$$0 \to H^d_{\mathrm{Iw}}(N, T \otimes_R I^n/I^{n+1}) \to H^d_{\mathrm{Iw}}(N, T \otimes_R \Omega/I^{n+1}) \to H^d_{\mathrm{Iw}}(N, T \otimes_R \Omega/I^n) \to 0.$$

We consider the connecting homomorphism in H-homology:

$$\partial^{(n)} \colon H_1(H, H^d_{\mathrm{Iw}}(N,T) \otimes_R \Omega/I^n) \to H^d_{\mathrm{Iw}}(N,T)_H \otimes_R I^n/I^{n+1}. \tag{2.6}$$

We next apply Lemma A.0.1 of the appendix, which says that edge maps to total terms in homological Grothendieck spectral sequences are compatible with connecting maps. Here, the spectral sequence is that of Proposition 2.2.2, which is associated to the composition of functors $F = H_0(H, \cdot\,)$ and $F' = H^d_{\mathrm{Iw}}(N, \cdot\,)$, noting that $F \circ F' \cong H^d(G, \cdot\,)$ via corestriction. The connecting homomorphisms are from degrees 1 to 0 and are associated to the short exact sequence of (2.1).

In this setting, the lemma provides a commutative square related to the diagram

$$\begin{tikzcd} H^{d-1}(G, T \otimes_R \Omega/I^n) \arrow[r, "\Psi^{(n)}"] \arrow[d, two heads] & H^d(G,T) \otimes_R I^n/I^{n+1} \arrow[d, "\wr"] \\ H_1(H, H^d_{\mathrm{Iw}}(N,T) \otimes_R \Omega/I^n) \arrow[r, "\partial^{(n)}"] & H^d_{\mathrm{Iw}}(N,T)_H \otimes_R I^n/I^{n+1}, \end{tikzcd} \tag{2.7}$$

but with $L_1(F \circ F')(T \otimes_R \Omega/I^n)$ in place of $H^{d-1}(G, T \otimes_R \Omega/I^n)$. By Lemma A.0.2, which is a simple consequence of the universality of left derived functors, we have a surjection from the latter object to the former compatible with their connecting homomorphisms to $H^d(G,T) \otimes_R I^n/I^{n+1}$. This allows us to make the replacement while maintaining the surjectivity of the left vertical map, so we indeed have the commutative square (2.7).

By Lemma 2.2.3, the isomorphism in the statement of the theorem is the map on cokernels of the horizontal maps in (2.7). $\square$

Although not used in this paper, for the purposes of Iwasawa-theoretic applications, it is useful to have a slightly stronger version of Theorem 2.2.4. So, we remark that it has the following generalization, with virtually no additional complications (given that the results of [LiSh, FuKa] hold in this generality).

Remark 2.2.5. Let $\mathcal{G}$ be a profinite group, and let Γ be a quotient of $\mathcal{G}$ by a closed normal subgroup G. Let $\mathcal{H}$ be a quotient of $\mathcal{G}$ by a closed normal subgroup N that is contained in G, and let $H = G/N$ as before. We then have $\Gamma \cong \mathcal{H}/H$. That is, we have a commutative diagram of exact sequences

$$\begin{tikzcd}
N \arrow[r, equal] \arrow[d, hook] & N \arrow[d, hook] & \\
G \arrow[r, hook] \arrow[d, two heads] & \mathcal{G} \arrow[r, two heads] \arrow[d, two heads] & \Gamma \arrow[d, equal] \\
H \arrow[r, hook] & \mathcal{H} \arrow[r, two heads] & \Gamma.
\end{tikzcd}$$

Take T to be a compact $R[\![\mathcal{G}]\!]$-module finitely generated over R, and replace the assumptions on G and H from the beginning of this subsection with the identical assumptions on $\mathcal{G}$ and $\mathcal{H}$, respectively. We have Iwasawa cohomology groups $H^i_{\mathrm{Iw}}(N,T)$ and $H^i_{\mathrm{Iw}}(G,T)$, which are now taken relative to the larger group $\mathcal{G}$. These are finitely generated as modules over $R[\![\mathcal{H}]\!]$ and $\Lambda = R[\![\Gamma]\!]$, respectively, and we have as before a spectral sequence

$$E^2_{i,j}(T) = H_i(H, H^{d-j}_{\mathrm{Iw}}(N,T)) \Rightarrow E_{i+j}(T) = H^{d-i-j}_{\mathrm{Iw}}(G,T),$$

but now of Λ-modules. In exactly the same manner as before, this gives rise to isomorphisms

$$\frac{I^n H^d_{\mathrm{Iw}}(N,T)}{I^{n+1} H^d_{\mathrm{Iw}}(N,T)} \cong \frac{H^d_{\mathrm{Iw}}(G,T) \otimes_R I^n/I^{n+1}}{\operatorname{im} \Psi^{(n)}},$$

again of Λ-modules.

2.3 The abelian case

We turn to the direct computation of generalized Bockstein maps on 1-cocycles for abelian H. That is, let us now take H to be a finitely generated, abelian pro-p group, and let us take R to be a quotient of $\mathbb{Z}_p$. We give an explicit formula for $\Psi^{(n)}$ under a hypothesis on the size of R that ensures our flatness hypothesis is satisfied. If H has no nonzero p-torsion, no hypothesis is needed.

We begin with the following simple lemma.

Lemma 2.3.1. *Let s and t be positive integers with $n < p^{t-s+1}$. Then $(1+x)^{p^t} - 1$ is in the ideal (x^{n+1}, p^s) of $\mathbb{Z}[x]$.*

Proof. Recall that p^s divides $\binom{p^t}{i}$ for $0 < i < p^{t-s+1}$. Therefore

$$(1+x)^{p^t} = \sum_{i=0}^{p^t} \binom{p^t}{i} x^i \equiv 1 \bmod (x^{n+1}, p^s)$$

so long as $n < p^{t-s+1}$. $\square$

Let $h_1, \ldots, h_r$ be a minimal set of generators for H, labeled such that $h_1, \ldots, h_c$ have finite orders $p^{t_1} \leq \cdots \leq p^{t_c}$ and $h_{c+1}, \ldots, h_r$ have infinite order, for some $0 \leq c \leq r$. Define $x_i = [h_i] - 1 \in \Omega$ for $1 \leq i \leq r$, where $[h_i]$ denotes the group element of h_i, so that $I = (x_1, \ldots, x_r)$. We then have

$$\Omega \cong \frac{R[\![x_1, \ldots, x_r]\!]}{((x_1+1)^{p^{t_1}} - 1, \ldots, (x_c+1)^{p^{t_c}} - 1)}.$$

We have $c > 0$ if and only if H is not $\mathbb{Z}_p$-free, in which case we suppose that $R = \mathbb{Z}/p^s\mathbb{Z}$ with $n < p^{t_1-s+1}$. By Lemma 2.3.1, we have

$$\Omega/I^j \cong \frac{R[x_1, \ldots, x_r]}{(x_1, \ldots, x_r)^j}$$

for $j \leq n+1$. Moreover, I^n/I^{n+1} is a free R-module with basis the monomials in the variables x_i of degree n. In particular, the generalized Bockstein map $\Psi^{(n)}$ is defined.

We may view any element of $q \in T \otimes_R \Omega/I^n$ as having the form

$$q = \sum_{k_1+\cdots+k_r<n} \alpha_{k_1,\ldots,k_r} x_1^{k_1} \cdots x_r^{k_r},$$

where the sum is taken over r-tuples $(k_1, \ldots, k_r)$ of nonnegative integers with sum less than n and with $\alpha_{k_1,\ldots,k_r} \in T$, omitting the notation for the tensor product in such an expression. Setting $\|k\| = k_1 + \cdots + k_r$ for an r-tuple $(k_1, \ldots, k_r)$, let's simplify this notation as

$$q = \sum_{\|k\|<n} \alpha_k x^k, \tag{2.8}$$

where $x^k = x_1^{k_1} \cdots x_r^{k_r}$.

Let $\pi \colon G \to H$ denote the quotient map. For each i, let

$$A_i = \begin{cases} \mathbb{Z}/p^{t_i}\mathbb{Z} & \text{if } 1 \leq i \leq c, \\ \mathbb{Z}_p & \text{if } c < i \leq r. \end{cases}$$

For $1 \leq i \leq r$, let $\chi_i \colon G \to A_i$ be the homomorphisms determined by

$$\pi(g) = \prod_{i=1}^{r} h_i^{\chi_i(g)}$$

for $g \in G$. The action of $g \in G$ on q as in (2.8) is given by multiplication by $\prod_{i=1}^{r}(1+x_i)^{\chi_i(g)}$. That is, we have the formula

$$g \cdot q = \sum_{\|k\|<n} \left(\sum_{0 \leq k' \leq k} \binom{\chi(g)}{k'} g\alpha_{k-k'} \right) x^k, \tag{2.9}$$

where the second sum is over r-tuples k' of nonnegative integers with $k'_i \leq k_i$ for each i, and where we have set $\binom{\chi(g)}{k'} = \binom{\chi_1(g)}{k'_1} \cdots \binom{\chi_r(g)}{k'_r}$.

Note that our assumption on the cardinality of R can be rephrased as saying that either $c = 0$ or R is a quotient of A_1 such that $|R| < \frac{p}{n}|A_1|$. With our notation and this assumption established, we can give an explicit formula for $\Psi^{(n)}$.

Proposition 2.3.2. *Let $f \colon G \to T \otimes_R \Omega/I^n$ be a 1-cocycle, and write*

$$f = \sum_{\|k\|<n} \lambda_k x^k$$

with $\lambda_k \colon G \to T$. Then $\Psi^{(n)}$ takes the class of f to the class of the 2-cocycle

$$(g,h) \mapsto \sum_{\|k\|=n} \left(\sum_{0 < k' \leq k} \binom{\chi(g)}{k'} g\lambda_{k-k'}(h) \right) x^k,$$

where the first sum is taken over r-tuples $k = (k_1, \ldots, k_r)$ of nonegative integers summing to n, and the second sum is taken over nonzero r-tuples k' of nonnegative integers with $k'_i \leq k_i$ for all i.

Proof. Consider the set-theoretic section

$$s_n \colon T \otimes_R \Omega/I^n \to T \otimes_R \Omega/I^{n+1} \tag{2.10}$$

that takes a sum as in (2.8) to the same expression in the larger module. Let $\tilde{f} = s_n \circ f$. By definition $\Psi^{(n)}(f)$ is the class of $d\tilde{f}$, where

$$d\tilde{f}(g,h) = \tilde{f}(g) + g\tilde{f}(h) - \tilde{f}(gh)$$

for $g, h \in G$. Since f is a cocycle, the right-hand side of this expression is equal to the degree n part of $g\tilde{f}(h)$, which by (2.9) is exactly as in the statement of the proposition. $\square$

For general H, pro-p but not necessarily abelian, we can use this computation to see that $\Psi^{(1)}$ is given by cup products. We consider the case that H is a quotient of G such that the abelianization H^{ab} of H is finitely generated and pro-p. As before, but now for H^{ab} in place of H, there are nonnegative integers $r \geq c$ and positive integers $t_1 \leq \cdots \leq t_c$ such that

$$H^{\mathrm{ab}} \cong \bigoplus_{i=1}^{r} A_i, \tag{2.11}$$

where $A_i = \mathbb{Z}/p^{t_i}\mathbb{Z}$ for $i = 1, \ldots, c$ and $A_i = \mathbb{Z}_p$ for $i = c+1, \ldots, r$. For $i = 1, \ldots, r$, we let $\chi_i \colon G \to A_i$ denote the quotient map $G \to A_i$. We take $n = 1$, and our condition on the cardinality of R becomes $s \leq t_1$ when $c \geq 1$.

Fix generators $h_1, \ldots, h_r$ of H such that each h_i maps to $1 \in A_i$ under the composition of the quotient map and the isomorphism in (2.11). There is an isomorphism $I/I^2 \cong H^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} R$ taking the image of $x_i = [h_i] - 1$ to $h_i \otimes 1$.

Proposition 2.3.3. *Let H be a finitely generated pro-p group with H^{ab} as in* (2.11)*, let I be the augmentation ideal in $\Omega = R[\![H]\!]$, and let χ_i and x_i for $1 \leq i \leq r$ be as in the previous paragraph. For any* 1*-cocycle $f \colon G \to T$, we have*

$$\Psi^{(1)}(f) = \sum_{i=1}^{r} (\chi_i \cup f)x_i \in H^2(G, T) \otimes_R I/I^2.$$

Proof. Let $\Omega' = R[\![H^{\mathrm{ab}}]\!]$ with augmentation ideal $I' \subset \Omega'$. Both Ω/I and Ω'/I' are identified with R via the augmentation maps, and there are also compatible isomorphisms between the graded quotients I/I^2 and $I'/(I')^2$ and the R-module $H^{\mathrm{ab}} \otimes_{\mathbb{Z}_p} R$. It follows that the canonical map $\Omega \to \Omega'$ induces an isomorphism $\Omega/I^2 \cong \Omega'/(I')^2$. Thus $\Psi^{(1)}$ equals the first generalized Bockstein map for H^{ab}, and the proposition follows from the case $n = 1$ of Proposition 2.3.2. $\square$

This result was previously studied by the third author in the context of Iwasawa theory, where these maps are referred to as reciprocity maps with restricted ramification: see for instance [Sh3, Lemma 4.1] for its introduction. In the following section, we study analogous results for $\Psi^{(n)}$ with $n > 1$ in terms of higher Massey products.

3 Massey products

The notion of Massey products that we will use is conveniently stated using the theory of generalized matrix algebras, as found in [BeCh]. We require only a simple upper-triangular version of these algebras.

3.1 Upper-triangular generalized matrix algebras

Let n be a positive integer, and let R be a commutative ring.

Definition 3.1.1. An n-dimensional *upper-triangular generalized matrix algebra* $\mathcal{A}$ over R (or, R-*UGMA*) is an R-algebra formed out of the data of

- finitely generated R-modules $A_{i,j}$ for $1 \le i \le j \le n$ with $A_{i,j} = R$ if $i = j$, and
- R-module homomorphisms $\varphi_{i,j,k} \colon A_{i,j} \otimes_R A_{j,k} \to A_{i,k}$ for all $1 \le i \le j \le k \le n$ which are induced by the given R-actions if $i = j$ or $j = k$

such that the two resulting maps

$$A_{i,j} \otimes_R A_{j,k} \otimes_R A_{k,l} \to A_{i,l}$$

coincide for all $1 \le i < j < k < l \le n$. The tuple $(A_{i,j}, \varphi_{i,j,k})$ defines an R-algebra $\mathcal{A}$ with underlying R-module

$$\mathcal{A} = \bigoplus_{1 \le i \le j \le n} A_{i,j},$$

and multiplication given by matrix multiplication: that is, for $a = (a_{i,j})$ and $b = (b_{i,j})$ in $\mathcal{A}$, the (i,j)-entry $(ab)_{i,j}$ of ab is

$$(ab)_{i,j} = \sum_{k=i}^{j} \varphi_{i,k,j}(a_{i,k} \otimes b_{k,j}).$$

Our interest is in the multiplicative group $\mathcal{U} = \mathcal{U}(\mathcal{A})$ of *unipotent* matrices in a UGMA $\mathcal{A}$, i.e., those $a = (a_{i,j})$ with $a_{i,i} = 1$ for all i. We shall often take the quotient $\mathcal{U}' = \mathcal{U}'(\mathcal{A})$ of this $\mathcal{U}$ by its central subgroup $\mathcal{Z} = \mathcal{Z}(\mathcal{A})$ of *unipotent central* elements, i.e., those $a \in \mathcal{U}$ with $a_{i,j} = 0$ for all $(i,j) \neq (1,n)$.

The following is the key example for our purposes.

Example 3.1.2. Let M be a finitely generated R-module, and let m be a positive integer less than n. We define an n-dimensional R-UGMA $\mathcal{A}_n(M,m)$ as follows. Set

$$A_{i,j} = \begin{cases} M & \text{if } i \le m < j, \\ R & \text{otherwise} \end{cases}$$

and take the maps $\varphi_{i,j,k}$ to be the R-module structure maps. This makes sense since, given $i \le j \le k$, at least one of $A_{i,j}$ and $A_{j,k}$ must be R, as m cannot satisfy both $m < j$ and $j \le m$.

Let us write $\mathcal{U}_n(M,m)$ for $\mathcal{U}(\mathcal{A}_n(M,m))$ and $\mathcal{U}'_n(M,m)$ for $\mathcal{U}'(\mathcal{A}_n(M,m))$. To make this easier to visualize, note that we can write $\mathcal{U}_n(M,m)$ in "block matrix" form as

$$\mathcal{U}_n(M,m) = \begin{pmatrix} \mathrm{U}_m(R) & \mathrm{M}_{m,n-m}(M) \\ 0 & \mathrm{U}_{n-m}(R) \end{pmatrix},$$

where $\mathrm{U}_k(R) \leqslant \mathrm{GL}_k(R)$ denotes the group of upper-triangular unipotent matrices and $\mathrm{M}_{k,l}(M)$ denotes the additive group of k-by-l matrices with entries in M for positive integers k and l. The latter group is endowed with a left $\mathrm{U}_k(R)$-action and a commuting right $\mathrm{U}_l(R)$-action. Put differently, $\mathcal{A}_n(M,m)$ itself is a sort of 2-by-2 generalized matrix algebra, allowing noncommutative rings on the diagonal and bimodules in the non-diagonal entries.

We actually need to use *profinite UGMAs* defined just as in Definition 3.1.1 using profinite rings R and compact R-modules $A_{i,j}$, but now assuming that the induced multiplication maps $A_{i,j} \times A_{j,k} \to A_{i,k}$ are continuous. Alternatively, the maps $\varphi_{i,j,k}$ can be replaced by maps of completed tensor products over R in the definition.

Though unnecessary, to keep things simple, let us suppose that the compact R-modules $A_{i,j}$ in a profinite R-UGMA are R-finitely generated. This forces them to have the adic topology for any directed system of ideals that are open neighborhoods of zero. Moreover, their tensor products and completed tensor products are then abstractly isomorphic, and so we may in particular view the tensor products $A_{i,j} \otimes_R A_{j,k}$ themselves as compact R-modules. (For a slightly longer discussion of this, see [LiSh, Section 2.3].)

Note that any profinite R-UGMA $\mathcal{A}$ has a topology as a finite direct product of the compact R-modules $A_{i,j}$, and $\mathcal{U}$ inherits the subspace topology.

We also want to make a second modification, allowing a continuous action of G.

Definition 3.1.3. For a profinite ring R and a profinite group G, a *profinite (R,G)-UGMA* is the data of a profinite R-UGMA $\mathcal{A}$ together with a continuous G-action on each $A_{i,j}$ such that

- the action on $A_{i,i} = R$ is trivial for all i, and
- the maps $\varphi_{i,j,k}$ are maps of $R[\![G]\!]$-modules, where $A_{i,j} \otimes_R A_{j,k}$ is given the diagonal action of G.

We remark that, aside from issues of finite generation, the difference between a profinite $R[\![G]\!]$-UGMA and a profinite (R,G)-UGMA is that in the former, each $A_{i,i} = R[\![G]\!]$, whereas in the latter, each $A_{i,i}$ is R with the trivial G-action. We are interested in the latter structure.

Example 3.1.4. If R is a profinite ring and T is a compact $R[\![G]\!]$-module (that is R-finitely generated), then the R-UGMA $\mathcal{A}_n(T,m)$ of Example 3.1.2 has a natural structure of a profinite (R,G)-UGMA by letting G act on $A_{i,j}$ via its action on T if $i \le m < j$ and trivially otherwise.

3.2 Defining systems and Massey products

Let R be a profinite ring, let G be a profinite group, and let $n \geq 2$. Let $T_1, \ldots, T_n$ be compact $R[\![G]\!]$-modules that are R-finitely generated for simplicity, and let $\chi_i \colon G \to T_i$ be continuous 1-cocycles for $1 \leq i \leq n$. In this section, we define *Massey products* of these cocycles, which will be 2-cocycles that depend on a number of choices constituting a *defining system*.

Definition 3.2.1. A *defining system* for the Massey product of $\chi_1, \ldots, \chi_n$ is the data of

- an $(n+1)$-dimensional profinite (R, G)-UGMA $\mathcal{A}$ and
- a (nonabelian) continuous 1-cocycle $\rho \colon G \to \mathcal{U}'$

such that $A_{i,i+1} = T_i$ for $1 \leq i \leq n$, and the composition of ρ with projection to $A_{i,i+1}$ is χ_i.

Given a defining system $\rho \colon G \to \mathcal{U}'$, there is a unique function $\tilde{\rho} \colon G \to \mathcal{U}$ lifting ρ and having zero as the $(1, n+1)$-entry of $\tilde{\rho}(g)$ for all $g \in G$. We let $\rho_{i,j} \colon G \to A_{i,j}$ be the map given by taking the (i, j)-entry of $\tilde{\rho}$.

Definition 3.2.2. Given a defining system ρ, the *n-fold Massey product* $(\chi_1, \ldots, \chi_n)_\rho \in H^2(G, A_{1,n+1})$ is the class of the 2-cocycle

$$(g, h) \mapsto \sum_{i=2}^{n} \varphi_{1,i,n+1}(\rho_{1,i}(g) \otimes g\rho_{i,n+1}(h))$$

that sends (g, h) to the $(1, n+1)$-entry of $\tilde{\rho}(g) \cdot g\tilde{\rho}(h)$.

In the remainder of the paper, we will restrict our attention to the setting of the $(n+1)$-dimensional profinite (R, G)-UGMAs of the form $\mathcal{A}_{n+1}(T, m)$ defined in Examples 3.1.2 and 3.1.4. This means in particular that we only consider n-fold Massey products for which there is an m with $1 \leq m \leq n$ such that $T_m = T$ and $T_i = R$ for $i \neq m$. In particular, we will always have $(\chi_1, \ldots, \chi_n)_\rho \in H^2(G, T)$.

In [Sh2], the third author considered the case in which $m = n$ and $\chi_1 = \cdots = \chi_{n-1}$ in a Galois-cohomological setting. In that case, the key idea for relating Massey products to graded pieces of Iwasawa cohomology groups was to consider only a restricted set of defining systems referred to as *proper defining systems*. We will consider a more general notion of proper defining system that depends on extra data we call a *partial defining system*. In [Sh2], the partial defining system comes from unipotent binomial matrices, which we review in Section 4.2 below.

3.3 Massey products relative to proper defining systems

Fix an integer $n \geq 2$ and two integers $a, b \geq 0$ with $a + b = n$. Let $Z^i(G, M)$ for a profinite $R[\![G]\!]$-module M denote the group of continuous i-cocycles on G valued in M. Choose tuples

$$\alpha = (\alpha_1, \dots, \alpha_a) \in Z^1(G, R)^a \quad \text{and} \quad \beta = (\beta_1, \dots, \beta_b) \in Z^1(G, R)^b$$

and a compact $R[\![G]\!]$-module T that is finitely generated as an R-module.

We next consider a pair of homomorphisms that constitute a part of the defining systems for $(n+1)$-fold Massey products $(\alpha_1, \dots, \alpha_a, \lambda, \beta_1, \dots, \beta_b)$, where $\lambda \in Z^1(G, T)$ is allowed to vary. We write the collection of such Massey products as $(\alpha, \cdot, \beta)$ for short.

Definition 3.3.1. A *partial defining system* for $(n+1)$-fold Massey products $(\alpha, \cdot, \beta)$ is a pair of homomorphisms

$$\phi\colon G \to \mathrm{U}_{a+1}(R) \quad \text{and} \quad \theta\colon G \to \mathrm{U}_{b+1}(R)$$

such that α is the off-diagonal of ϕ and β is the off-diagonal of θ, i.e., $\phi_{i,i+1} = \alpha_i$ for $1 \leq i \leq a$ and $\theta_{i,i+1} = \beta_i$ for $1 \leq i \leq b$.

More specifically, an (a, b)*-partial defining system* is a partial defining system restricting to some pair $(\alpha, \beta) \in Z^1(G, R)^a \times Z^1(G, R)^b$.

Recall that

$$\mathcal{U}_{n+2}(T, a+1) = \begin{pmatrix} \mathrm{U}_{a+1}(R) & M_{a+1,b+1}(T) \\ & \mathrm{U}_{b+1}(R) \end{pmatrix}.$$

We may then write the quotient by the unipotent central matrices as

$$\mathcal{U}'_{n+2}(T, a+1) = \begin{pmatrix} \mathrm{U}_{a+1}(R) & M'_{a+1,b+1}(T) \\ & \mathrm{U}_{b+1}(R) \end{pmatrix}$$

for $M'_{a+1,b+1}(T) = M_{a+1,b+1}(T)/T$, where T is identified with the matrices that are zero outside the $(1, b+1)$-entry.

Definition 3.3.2. Given a 1-cocycle $\lambda\colon G \to T$, a *proper defining system* for an $(n+1)$-fold Massey product (α, λ, β) *relative to a partial defining system* (ϕ, θ) is a continuous 1-cocycle

$$\rho\colon G \to \mathcal{U}'_{n+2}(T, a+1)$$

of the form

$$\rho = \begin{pmatrix} \phi & \kappa \\ 0 & \theta \end{pmatrix}$$

for some $\kappa\colon G \to M'_{a+1,b+1}(T)$ with $\kappa_{a+1,1} = \lambda$.

The advantage of proper defining systems is that they are parameterized by abelian, rather than nonabelian, cocycles. To show this, we introduce a compact $R[\![G]\!]$-module $\mathfrak{U}_{\phi,\theta}(T)$ such that proper defining systems in T relative to (ϕ,θ) correspond to 1-cocycles with values in $\mathfrak{U}_{\phi,\theta}(T)$.

Consider the compact R-module $\mathfrak{U}_{n+2}(R)$ that is the R-module of strictly upper-triangular $(n+2)$-dimensional square matrices. The group $\mathrm{U}_{n+2}(R)$ acts continuously on $\mathfrak{U}_{n+2}(R)$ by conjugation. We consider a $R[\![\mathrm{U}_{n+2}(R)]\!]$-submodule $\mathfrak{U}_{a,b}(R)$ of $\mathfrak{U}_{n+2}(R)$ given by

$$\{x=(x_{ij})\in M_{n+2}(R)\mid x_{ij}=0 \text{ if } j\le a+1 \text{ or } i\ge a+2\}.$$

In other words, breaking $M_{n+2}(R)$ into blocks using the partition $n+2=(a+1)+(b+1)$ and using block-matrix notation, we have

$$\mathfrak{U}_{a,b}(R)=\begin{pmatrix}0 & M_{a+1,b+1}(R)\\ 0 & 0\end{pmatrix}.$$

Given a partial defining system (ϕ,θ), we consider $\mathfrak{U}_{a,b}(R)$ as a G-module via the continuous homomorphism

$$G\to \mathrm{U}_{n+2}(R),\quad g\mapsto \begin{pmatrix}\phi(g) & 0\\ 0 & \theta(g)\end{pmatrix}.$$

We define an $R[\![G]\!]$-module $\mathfrak{U}_{\phi,\theta}(T)$ as $\mathfrak{U}_{a,b}(R)\otimes_R T$ with the diagonal G-action. We also have the following equivalent definition, which has the benefit of being more explicit:

- $\mathfrak{U}_{\phi,\theta}(T)=M_{a+1,b+1}(T)$ as an R-module,
- the action map $G\to \mathrm{End}(M_{a+1,b+1}(T))$ is given, for $g\in G$ and $x\in M_{a+1,b+1}(T)$, by

  $$g\star x=\phi(g)\cdot gx\cdot\theta(g)^{-1}.$$

  where gx means apply the g action on T to each matrix entry, and the multiplication denoted by "$\cdot$" is of matrices.

Going forward, we use the latter description of $\mathfrak{U}_{\phi,\theta}(T)$, so consider it as consisting of $(a+1)$-by-$(b+1)$ matrices, rather than as a subgroup of $M_{n+2}(R)$. Note that $\mathfrak{U}_{\phi,\theta}(T)$ contains a copy of T as an $R[\![G]\!]$-submodule by inclusion in the $(1,b+1)$-entry. Let

$$\mathfrak{U}'_{\phi,\theta}(T)=\mathfrak{U}_{\phi,\theta}(T)/T.$$

Let $x\mapsto\tilde{x}$ denote the R-module section $\mathfrak{U}'_{\phi,\theta}(T)\to\mathfrak{U}_{\phi,\theta}(T)$ given by filling in the $(1,b+1)$-entry as 0.

Lemma 3.3.3. *Let (ϕ, θ) be a partial defining system for Massey products $(\alpha, \cdot, \beta)$. Then the map that takes a continuous 1-cocycle $\kappa' \colon G \to \mathfrak{U}'_{\phi,\theta}(T)$ to a map $\rho \colon G \to \mathcal{U}'_{n+2}(T, a)$ given by*

$$\rho = \begin{pmatrix} \phi & \kappa'\theta \\ 0 & \theta \end{pmatrix}.$$

is a bijection between $Z^1(G, \mathfrak{U}'_{\phi,\theta}(T))$ and the set of proper defining systems in T relative to (ϕ, θ).

Proof. Given a cochain $\kappa' \colon G \to \mathfrak{U}'_{\phi,\theta}(T)$, set $\kappa = \kappa'\theta \colon G \to \mathfrak{U}'_{\phi,\theta}(T)$. We have to check that

$$\rho = \begin{pmatrix} \phi & \kappa \\ 0 & \theta \end{pmatrix}$$

is a cocycle if and only if κ' is a cocycle. Matrix multiplication tells us that ρ is a cocycle if and only if

$$\kappa(gh) = \phi(g)g\kappa(h) + \kappa(g)\theta(h). \tag{3.1}$$

The cochain κ' is a cocycle if and only if the second equality holds in the following string of equalities

$$\begin{aligned}
\kappa(gh) &= \kappa'(gh)\theta(gh) \\
&= (g \star \kappa'(h) + \kappa'(g))\theta(gh) \\
&= (\phi(g)g\kappa'(h)\theta(g)^{-1} + \kappa'(g))\theta(g)\theta(h) \\
&= \phi(g)g\kappa'(h)\theta(h) + \kappa'(g)\theta(g)\theta(h) \\
&= \phi(g)g\kappa(h) + \kappa(g)\theta(h),
\end{aligned}$$

hence the result. □

The value of the Massey product associated to a proper defining system is also a value of a connecting homomorphism for an exact sequence attached to the underlying partial defining system.

Theorem 3.3.4. *Let (ϕ, θ) be a partial defining system for $(\alpha, \cdot, \beta)$. Let $\kappa' \in Z^1(G, \mathfrak{U}'_{\phi,\theta}(T))$, and let $\rho = \left(\begin{smallmatrix} \phi & \kappa'\theta \\ & \theta \end{smallmatrix}\right)$ be the associated proper defining system as in Lemma 3.3.3. Consider the short exact sequence*

$$0 \to T \to \mathfrak{U}_{\phi,\theta}(T) \to \mathfrak{U}'_{\phi,\theta}(T) \to 0.$$

Then the image of the class of κ' under the connecting map

$$\partial \colon H^1(G, \mathfrak{U}'_{\phi,\theta}(T)) \to H^2(G, T)$$

is the $(n+1)$-fold Massey product $(\alpha_1, \ldots, \alpha_a, \kappa'_{a+1,1}, \beta_1, \ldots, \beta_b)_\rho$.

Proof. Let $\kappa = \kappa'\theta \colon G \to \mathfrak{U}'_{\phi,\theta}(T)$, and let $\tilde{\kappa}$ be its unique lift to $\mathfrak{U}_{\phi,\theta}(T)$ with $\tilde{\kappa}(g)$ having zero $(1, b+1)$-entry for all $g \in G$. The map $\tilde{\kappa}' = \tilde{\kappa}\theta^{-1} \colon G \to \mathfrak{U}_{\phi,\theta}(T)$ is then a lift of κ'. By definition, the image of κ is represented by the 2-cocycle that is given by taking the $(1, b+1)$-entry of $d\tilde{\kappa}'$. We have

$$\begin{aligned} d\tilde{\kappa}'(g,h) &= \tilde{\kappa}'(g) + g \star \tilde{\kappa}'(h) - \tilde{\kappa}'(gh) \\ &= \tilde{\kappa}(g)\theta(g)^{-1} + \phi(g)g\tilde{\kappa}(h)\theta(h)^{-1}\theta(g)^{-1} - \tilde{\kappa}(gh)\theta(gh)^{-1} \\ &= (\tilde{\kappa}(g)\theta(h) + \phi(g)g\tilde{\kappa}(h) - \tilde{\kappa}(gh))\theta(gh)^{-1}. \end{aligned}$$

Since κ satisfies (3.1), we have $\tilde{\kappa}(g)\theta(h) + \phi(g)g\tilde{\kappa}(h) - \tilde{\kappa}(gh) \in T$, and T is fixed under the action of right multiplication by an element of $\mathrm{U}_{b+1}(R)$. Since $\tilde{\kappa}(gh)$ has zero $(1, b+1)$-entry, the $(1, b+1)$-entries of $d\tilde{\kappa}'(g,h)$ and $\tilde{\kappa}(g)\theta(h) + \phi(g)g\tilde{\kappa}(h)$ are equal.

The Massey product $(\alpha_1, \ldots, \alpha_a, \kappa_{a+1,1}, \beta_1, \ldots, \beta_b)_\rho$ (and note that $\kappa_{a+1,1} = \kappa'_{a+1,1}$) is the $(1, n+2)$-entry of $\tilde{\rho}(g) \cdot g\tilde{\rho}(h)$, where

$$\tilde{\rho} = \begin{pmatrix} \phi & \tilde{\kappa} \\ 0 & \theta \end{pmatrix}.$$

The result then follows from the fact that

$$\tilde{\rho}(g) \cdot g\tilde{\rho}(h) = \begin{pmatrix} \phi(g) & \tilde{\kappa}(g) \\ 0 & \theta(g) \end{pmatrix} \begin{pmatrix} \phi(h) & g\tilde{\kappa}(h) \\ 0 & \theta(h) \end{pmatrix} = \begin{pmatrix} \phi(gh) & \phi(g)g\tilde{\kappa}(h) + \tilde{\kappa}(g)\theta(h) \\ 0 & \theta(gh) \end{pmatrix}.$$

□

In fact, the proof of Theorem 3.3.4 gives an explicit map $Z^1(G, \mathfrak{U}'_{\phi,\theta}(T)) \to Z^2(G,T)$, taking a 1-cocycle κ' to the $(1, b+1)$-entry of $d\tilde{\kappa}'$, for the specific lift $\tilde{\kappa}'$ of κ' defined therein.

4 Massey products as values of Bockstein maps

We return to the setting and notation of Section 2. We first discuss a general result that gives partial information about the generalized Bockstein map $\Psi^{(n)}$ in terms of Massey products. Then we discuss specific examples where this information completely determines $\Psi^{(n)}$.

4.1 Partial defining systems and Bockstein maps

Fix integers $a, b \geq 0$ such that $a + b = n$ and group homomorphisms

$$\phi \colon H \to \mathrm{U}_{a+1}(R) \quad \text{and} \quad \theta \colon H \to \mathrm{U}_{b+1}(R),$$

so viewing ϕ and θ as maps from G via precomposition with the quotient map, the pair (ϕ, θ) is an (a, b)-partial defining system. We let $\alpha = (\phi_{i,i+1})_i$ and $\beta = (\theta_{i,i+1})_i$, so this partial defining system is of Massey products $(\alpha, \cdot, \beta)$. If $b = 0$, we often refer to the pair (ϕ, θ) simply as ϕ.

Lemma 4.1.1. *Let $e \in \mathfrak{U}_{a,b}(R)$ be the matrix with $(a+1, 1)$-entry equal to 1 and all other entries 0. There is a continuous $R[\![G]\!]$-module homomorphism $p_{\phi,\theta} \colon \Omega/I^{n+1} \to \mathfrak{U}_{a,b}(R)$ given on the images of group elements by*

$$p_{\phi,\theta}([h]) = \phi(h) \cdot e \cdot \theta(h)^{-1}.$$

The image of I^n is contained in the submodule of matrices that are zero outside of their $(1, b+1)$-entries.

Proof. The map $\tilde{p}_{\phi,\theta} \colon \Omega \to \mathfrak{U}_{a,b}(R)$ inducing $p_{\phi,\theta}$ is given by the action of H on $e \in \mathfrak{U}_{a,b}(R)$ via the composite homomorphism

$$H \xrightarrow{\rho_{\phi,\theta}} \mathrm{U}_{n+2}(R) \xrightarrow{\mathrm{ad}} \mathrm{Aut}(\mathfrak{U}_{a,b}(R)),$$

where $\rho_{\phi,\theta} \colon H \to \mathrm{U}_{n+2}(R)$ is given by

$$\rho_{\phi,\theta}(h) = \begin{pmatrix} \phi(h) & 0 \\ 0 & \theta(h) \end{pmatrix}$$

and ad denotes the conjugation action. The action of G on Ω is given by the homomorphism $G \to H$, and the action of G on $\mathfrak{U}_{a,b}(R)$ is given by the composite of this map with $H \to \mathrm{Aut}(\mathfrak{U}_{a,b}(R))$, so $\tilde{p}_{\phi,\theta}$ is G-equivariant. We must show it factors through Ω/I^{n+1}.

Let $J \subset R[\![\mathrm{U}_{n+2}(R)]\!]$ be the augmentation ideal. Since the H-action factors through $U_{n+2}(R)$, we have $I^k\mathfrak{U}_{a,b}(R) \subseteq J^k\mathfrak{U}_{a,b}(R)$ for all k. It is easy to see inductively that

$$J^k\mathfrak{U}_{n+2}(R) = \{(a_{ij}) \in M_{n+2}(R) \mid a_{ij} = 0 \text{ if } j - i \leq k\}.$$

In particular, $J^{n+1}\mathfrak{U}_{n+2}(R) = 0$ and

$$J^n\mathfrak{U}_{n+2}(R) = \{(a_{ij}) \in M_{n+2}(R) \mid a_{ij} = 0 \text{ if } (i,j) \neq (1, n+2)\}.$$

Still viewing $\mathfrak{U}_{a,b}(R)$ as a subgroup of $\mathfrak{U}_{n+2}(R)$, the containments

$$I^k\mathfrak{U}_{a,b}(R) \subseteq J^k\mathfrak{U}_{a,b}(R) \subseteq J^k\mathfrak{U}_{n+2}(R)$$

imply the result. □

Lemma 4.1.1 implies that there is a map of short exact sequences of $R[\![G]\!]$-modules

$$\begin{tikzcd} 0 \arrow[r] & T \otimes_R I^n/I^{n+1} \arrow[r] \arrow[d, "p_{\phi,\theta}"] & T \otimes_R \Omega/I^{n+1} \arrow[r] \arrow[d, "p_{\phi,\theta}"] & T \otimes_R \Omega/I^n \arrow[r] \arrow[d, "p_{\phi,\theta}"] & 0 \\ 0 \arrow[r] & T \arrow[r] & \mathfrak{U}_{\phi,\theta}(T) \arrow[r] & \mathfrak{U}'_{\phi,\theta}(T) \arrow[r] & 0, \end{tikzcd} \tag{4.1}$$

where $p_{\phi,\theta}$ is the tensor product with T of the map in Lemma 4.1.1 coming from $\rho_{\phi,\theta}$. As a direct consequence of this commutativity and Theorem 3.3.4, we have the following.

Theorem 4.1.2. *Let $\phi\colon G \to \mathrm{U}_{a+1}(R)$ and $\theta\colon G \to \mathrm{U}_{b+1}(R)$ restrict to $\alpha \in Z^1(G,R)^a$ and $\beta \in Z^1(G,R)^b$ as above. Let $f \in Z^1(G, T \otimes_R \Omega/I^n)$, and let ρ denote the proper defining system relative to (ϕ,θ) associated to $p_{\phi,\theta} \circ f$ by Lemma 3.3.3. Then we have*

$$p_{\phi,\theta}(\Psi^{(n)}([f])) = (\alpha, (p_{\phi,\theta} \circ f)_{a+1,1}, \beta)_\rho$$

in $H^2(G,T)$. Here, the maps $p_{\phi,\theta}$ on the left and right are those induced on cohomology by the the left and right vertical maps in (4.1).

We will give examples of groups H and integers n such that there is a set X of choices of (ϕ,θ) for which the map

$$H^2(G,T) \otimes_R I^n/I^{n+1} \xrightarrow{\prod_{(\phi,\theta)\in X} p_{\phi,\theta}} \prod_{(\phi,\theta)\in X} H^2(G,T)$$

is injective. In such cases, Theorem 4.1.2 shows that the generalized Bockstein map $\Psi^{(n)}$ is determined by Massey products. In the rest of this section, we consider some specific examples in detail.

4.2 Unipotent binomial matrices

We introduce the *unipotent binomial matrices*, which are a source of many partial defining systems. Let n denote a positive integer, and let p be a prime number.

Let u_n denote the $(n+1)$-dimensional nilpotent upper triangular matrix

$$u_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ & 0 & 1 & \ddots & \vdots \\ & & 0 & \ddots & 0 \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix}.$$

For any $k \geq 1$, the matrix u_n^k has (i,j)-entry 1 if $j - i = k$ and 0 otherwise. In particular, we have $u_n^{n+1} = 0$.

Let $\left[\begin{smallmatrix} \cdot \\ n \end{smallmatrix}\right] \colon \mathbb{Z}_p \to \mathrm{U}_{n+1}(\mathbb{Z}_p)$ denote the unique continuous homomorphism to $(n+1)$-dimensional unipotent matrices with $\mathbb{Z}_p$-entries such that $\left[\begin{smallmatrix} 1 \\ n \end{smallmatrix}\right] = 1 + u_n$. By the binomial theorem, for $a \in \mathbb{Z}$ we have

$$\begin{bmatrix} a \\ n \end{bmatrix} = (1+u_n)^a = \sum_{k=0}^{n} \binom{a}{k} u_n^k = \begin{pmatrix} 1 & a & \binom{a}{2} & \cdots & \binom{a}{n} \\ & 1 & a & \ddots & \vdots \\ & & 1 & \ddots & \binom{a}{2} \\ & & & \ddots & a \\ & & & & 1 \end{pmatrix}.$$

If $t \geq s$ and $n < p^{t-s+1}$, then the composite map

$$\mathbb{Z} \xrightarrow{\left[\begin{smallmatrix} \cdot \\ n \end{smallmatrix}\right]} \mathrm{U}_{n+1}(\mathbb{Z}_p) \to \mathrm{U}_{n+1}(\mathbb{Z}/p^s\mathbb{Z})$$

that sends a to $(1+u_n)^a$ modulo p^s factors through $\mathbb{Z}/p^t\mathbb{Z}$ by Lemma 2.3.1 applied with $x = u_n$. By abuse of notation, we again denote the resulting map $\mathbb{Z}/p^t\mathbb{Z} \to \mathrm{U}_{n+1}(\mathbb{Z}/p^s\mathbb{Z})$ by $\left[\begin{smallmatrix} \cdot \\ n \end{smallmatrix}\right]$. In particular, the map $\binom{\cdot}{n} \colon \mathbb{Z} \to \mathbb{Z}/p^s\mathbb{Z}$ given by $a \mapsto \binom{a}{n} \pmod{p^s}$ factors through $\mathbb{Z}/p^t\mathbb{Z}$, and we abuse notation to also denote the resulting map $\mathbb{Z}/p^t\mathbb{Z} \to \mathbb{Z}/p^s\mathbb{Z}$ by $\binom{\cdot}{n}$.

The following lemma, phrased conveniently for our purposes, summarizes the above discussion.

Lemma 4.2.1. *Let A be a quotient of the ring $\mathbb{Z}_p$ and R be a quotient of A. Let H be a profinite group and $\chi \colon H \to A$ be a continuous homomorphism. Suppose that either $A = \mathbb{Z}_p$ or $|R| < \frac{p}{n}|A|$. Then there is a homomorphism*

$$\begin{bmatrix} \chi \\ n \end{bmatrix} \colon H \to \mathrm{U}_{n+1}(R),$$

defined by $\left[\begin{smallmatrix} \chi \\ n \end{smallmatrix}\right](h) = \left[\begin{smallmatrix} \chi(h) \\ n \end{smallmatrix}\right]$ for all $h \in H$.

Proof. If $|R| = p^s$ and $|A| = p^t$, then $|R| < \frac{p}{n}|A|$ if and only if $n < p^{t-s+1}$. ☐

4.3 Procyclic case

In this subsection, we fix a surjective homomorphism $\chi \colon G \to A$, where A is a nonzero quotient of $\mathbb{Z}_p$. We suppose that our ring R is a nonzero quotient of A with $A = \mathbb{Z}_p$ or $n|R| < p|A|$. We define H to be the coimage of χ, so $H \cong A$. We fix $h \in H$ to be the preimage of $1 \in A$ and let $x = [h] - 1 \in \Omega$, which is a generator of the augmentation ideal I. Our assumption on the size of R implies that $\Omega/I^j \cong R[x]/(x^j)$ for all $j \le n+1$ by the discussion of Section 2.3. In particular, we have $I^n/I^{n+1} = Rx^n$.

The $(n,0)$-proper defining systems relative to $\phi = \left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]$ and the trivial map θ to $\mathrm{U}_1(R) = \{1\}$ agree with the proper defining systems considered in [Sh2] for Galois groups. We give an interpretation of the resulting Massey products in terms of generalized Bockstein maps. That is, let us apply the discussion of Section 4.1 to this situation. We have $\alpha = (\chi, \dots, \chi) \in Z^1(G,R)^n$, which we denote by $\chi^{(n)}$. We denote $\mathfrak{U}_{\phi,\theta}(T)$ by $\mathfrak{U}_{\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]}(T)$.

Set $p_n = p_{\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right],0}$ for brevity. Then the diagram (4.1) becomes

$$\begin{tikzcd}
0 \arrow[r] & T \cdot x^n \arrow[r] \arrow[d] & T \otimes_R \Omega/I^{n+1} \arrow[r] \arrow[d, "p_n"] & T \otimes_R \Omega/I^n \arrow[r] \arrow[d, "p_n"] & 0 \\
0 \arrow[r] & T \arrow[r] & \mathfrak{U}_{\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]}(T) \arrow[r] & \mathfrak{U}'_{\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]}(T) \arrow[r] & 0,
\end{tikzcd}$$

where p_n is the map attached to $(\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right], 0)$ by Lemma 4.1.1. Explicitly, the vector $p_n(\sum_{k=0}^n a_k x^k)$ in $M_{n+1,1}(T)$ has ith entry a_{n+1-i}. (See the more general case proven in Lemma 4.4.1 of the next subsection.)

By Lemma 3.3.3, it follows that the proper defining system ρ_{x^n} relative to $\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]$ that is attached to $p_n \circ f$, where

$$f = \sum_{k=0}^{n-1} \lambda_k x^k \in Z^1(G, T \otimes_R \Omega/I^n),$$

satisfies $(\rho_{x^n})_{n+1-k,n+2} = \lambda_k$ for $0 \le k \le n-1$. In particular, the element $\lambda = \lambda_0 = (\rho_{x^n})_{n+1,n+2}$ is the image of f under the map

$$Z^1(G, T \otimes_R \Omega/I^n) \to Z^1(G,T)$$

induced by the augmentation $\Omega/I^n \mapsto \Omega/I = R$.

Theorem 4.1.2 then gives us an explicit description of the values of the generalized Bockstein homomorphism on classes in $H^1(G, T \otimes_R \Omega/I^n)$ as Massey products $(\chi^{(n)}, \cdot\,)$ relative to $\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]$, as follows.

Theorem 4.3.1. *For $f \in Z^1(G, T \otimes_R \Omega/I^n)$, we have*

$$\Psi^{(n)}([f]) = (\chi^{(n)}, \lambda)_{\rho_{x^n}} \cdot x^n,$$

where ρ_{x^n} is the proper defining system relative to $\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]$ attached to f, and λ is the image of f in $Z^1(G,T)$.

In particular, we have the following description of the image of $\Psi^{(n)}$.

Corollary 4.3.2. *The image of the generalized Bockstein map $\Psi^{(n)}$ is the set of all $(\chi^{(n)}, \lambda)_\rho \cdot x^n$ for Massey products of n copies of χ with 1-cocycles $\lambda \in Z^1(G,T)$ for proper defining systems ρ relative to $\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]$ with $\rho_{n+1,n+2} = \lambda$.*

Theorem 2.2.4 provides the following application to the graded quotients of Iwasawa cohomology groups of $N = \ker(\chi\colon G \to H)$.

Corollary 4.3.3. *Suppose that G is p-cohomologically finite of p-cohomological dimension 2. Let $P_n(H)$ denote the subgroup of $H^2(G,T) \otimes_R I^n/I^{n+1}$ generated by all $(\chi^{(n)}, \lambda)_\rho \cdot x^n$ for proper defining systems ρ relative to $\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right]$ and $\lambda = \rho_{n+1,n+2}$. We have a canonical isomorphism of R-modules*

$$\frac{I^n H^2_{\mathrm{Iw}}(N,T)}{I^{n+1} H^2_{\mathrm{Iw}}(N,T)} \cong \frac{H^2(G,T) \otimes_R I^n/I^{n+1}}{P_n(H)}.$$

4.4 Pro-bicyclic case

In this subsection, we

- fix a surjective homomorphism $(\chi, \psi)\colon G \twoheadrightarrow A \times B$, where A and B are nonzero quotients of $\mathbb{Z}_p$,
- let $a, b \geq 0$ denote integers such that $a + b = n$, and
- suppose that R is a nonzero quotient of both A and B with $a|R| < p|A|$ if A is finite and $b|R| < p|B|$ if B is finite.

Let H be the coimage of (χ, ψ) so that $H \cong A \times B$. Let $h_A, h_B \in H$ be the preimages of $(1,0), (0,1) \in A \times B$, respectively, and let $x = [h_A] - 1$ and $y = [h_B] - 1$ so that (x, y) is the augmentation ideal I of $\Omega = R[\![H]\!]$. We have $\Omega/I^j = R[x,y]/(x,y)^j$ for all $j \leq n$. In particular, we have

$$I^n/I^{n+1} = \bigoplus_{i+j=n} R x^i y^j.$$

We apply the discussion of Section 4.1 to this situation. We take $\phi = \left[\begin{smallmatrix}\chi\\ a\end{smallmatrix}\right]\colon H \to \mathrm{U}_a(R)$ and $\theta = \left[\begin{smallmatrix}\psi\\ b\end{smallmatrix}\right]\colon H \to \mathrm{U}_b(R)$. We have $\alpha = \chi^{(a)} \in Z^1(G,R)^a$ and $\beta = \psi^{(b)} \in Z^1(G,R)^b$.

Set $p_{a,b} = p_{\left[\begin{smallmatrix}\chi\\ a\end{smallmatrix}\right],\left[\begin{smallmatrix}\psi\\ b\end{smallmatrix}\right]}$ for brevity. In this setting, the diagram (4.1) becomes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigoplus_{i+j=n} T \cdot x^i y^j & \longrightarrow & T \otimes_R \Omega/I^{n+1} & \longrightarrow & T \otimes_R \Omega/I^n & \longrightarrow & 0 \\ & & \big\downarrow & & \big\downarrow{\scriptstyle p_{a,b}} & & \big\downarrow{\scriptstyle p_{a,b}} & & \\ 0 & \longrightarrow & T & \longrightarrow & \mathfrak{U}_{\left[\begin{smallmatrix}\chi\\ a\end{smallmatrix}\right],\left[\begin{smallmatrix}\psi\\ b\end{smallmatrix}\right]}(T) & \longrightarrow & \mathfrak{U}'_{\left[\begin{smallmatrix}\chi\\ a\end{smallmatrix}\right],\left[\begin{smallmatrix}\psi\\ b\end{smallmatrix}\right]}(T) & \longrightarrow & 0. \end{array} \tag{4.2}$$

Lemma 4.4.1. *The $R[\![G]\!]$-module map $p_{a,b}\colon T \otimes_R \Omega/I^{n+1} \to \mathfrak{U}_{\left[\begin{smallmatrix}\chi\\a\end{smallmatrix}\right],\left[\begin{smallmatrix}\psi\\b\end{smallmatrix}\right]}(T)$ is an isomorphism satisfying*

$$p_{a,b}\left(\sum_{k_1+k_2\le n} c_{k_1,k_2}x^{k_1}y^{k_2}\right) = (c_{a+1-i,j-1})_{i,j},$$

In particular, the lefthand vertical map in (4.2) *is given by projection onto the factor $T\cdot x^a y^b \cong T$.*

Proof. This reduces immediately to the case that $T = R$, since we can obtain the case of arbitrary T by R-tensor product with the identity of T. Let e be as in Lemma 4.1.1, the matrix with a single nonzero entry of 1 in the $(a+1,1)$-coordinate of $M_{a+1,b+1}(R)$. The (i,j)-entry of $g \star e = \left[\begin{smallmatrix}\chi(g)\\a\end{smallmatrix}\right] e \left[\begin{smallmatrix}\psi(g)\\b\end{smallmatrix}\right]$ is

$$\binom{\chi(g)}{a+1-i}\binom{\psi(g)}{j-1}.$$

which agrees with the coefficient of $x^{a+1-i}y^{j-1}$ in $g\cdot 1$ by (2.9). $\square$

Corollary 4.4.2. *For*

$$f = \sum_{k_1+k_2<n} \lambda_{k_1,k_2}x^{k_1}y^{k_2} \in Z^1(G,\Omega/I^n \otimes_R T)$$

and $\rho_{x^ay^b}$ the proper defining system relative to $(\left[\begin{smallmatrix}\chi\\a\end{smallmatrix}\right], \left[\begin{smallmatrix}\psi\\b\end{smallmatrix}\right])$ attached to $p_{a,b}\circ f$ by Lemma 3.3.3, we have

$$(\rho_{x^ay^b})_{a+1-k_1,a+2+k_2} = \lambda_{k_1,k_2}$$

for all $0 \le (k_1,k_2) < (a,b)$. In particular, we have $(\rho_{x^ay^b})_{a+1,a+2} = \lambda_{0,0}$, which is the image of f in $Z^1(G,T)$ under the map induced by the quotient $\Omega/I^n \to \Omega/I = R$.

The following is then a direct consequence of Theorem 4.1.2.

Theorem 4.4.3. *For $f \in Z^1(G,\Omega/I^n \otimes_R T)$, the image of $\Psi^{(n)}([f])$ in*

$$H^2(G,T)\otimes_R I^n/I^{n+1} \cong \bigoplus_{a+b=n} H^2(G,T)\cdot x^ay^b$$

is

$$\sum_{a+b=n} (\chi^{(a)},\lambda,\psi^{(b)})_{\rho_{x^ay^b}}\cdot x^ay^b,$$

where $\rho_{x^ay^b}$ is the proper defining system relative to $(\left[\begin{smallmatrix}\chi\\a\end{smallmatrix}\right], \left[\begin{smallmatrix}\psi\\b\end{smallmatrix}\right])$ attached to $p_{a,b}\circ f$, and λ is the image of f in $Z^1(G,T)$.

Applying Theorem 2.2.4, we obtain the following description of graded quotients of Iwasawa cohomology.

Corollary 4.4.4. *Suppose that G is p-cohomologically finite of p-cohomological dimension 2. Let $P_n(H)$ denote the subgroup of $H^2(G,T) \otimes_R I^n/I^{n+1}$ consisting of all sums $\sum_{a+b=n} (\chi^{(a)}, \lambda, \psi^{(b)})_{\rho_{x^a y^b}} \cdot x^a y^b$, where the $\rho_{x^a y^b}$ and λ are associated to a cocycle in $Z^1(G, \Omega/I^n \otimes_R T)$ as in Proposition 4.4.3. We then have a canonical isomorphism of R-modules*

$$\frac{I^n H^2_{\mathrm{Iw}}(N,T)}{I^{n+1} H^2_{\mathrm{Iw}}(N,T)} \cong \frac{H^2(G,T) \otimes_R I^n/I^{n+1}}{P_n(H)}.$$

4.5 Elementary abelian p-groups

The pattern seen in the cyclic and bicyclic cases does not continue for all finitely generated abelian pro-p groups. To see why, consider the case that $H \cong \mathbb{F}_p^3$ with basis $(\gamma_1, \gamma_2, \gamma_3)$ and dual basis (χ_1, χ_2, χ_3). For $x_i = [\gamma_i] - 1$, we have a basis of I^n/I^{n+1} consisting of monomials $x_1^{i_1} x_2^{i_2} x_3^{i_3}$ with $i_1 + i_2 + i_3 = n$. Following the pattern of the cyclic and bicyclic cases, one might guess that the coefficient of $x_1^{i_1} x_2^{i_2} x_3^{i_3}$ in $\Psi^{(n)}(f)$ is an $(n+1)$-fold Massey product involving i_j copies of each χ_j and another cocycle λ determined by f. However, this pattern fails already for $n = 3$ and the coefficient of $x_1 x_2 x_3$: any 4-fold Massey product involving the χ_i must have two of these characters beside each other, and thus, to be defined, the cup product of those two characters must vanish. Since these cup products will not vanish in general, we cannot hope for such a general statement to hold.

Nevertheless, at least in some cases, one can still describe the generalized Bockstein maps $\Psi^{(n)}$ in terms of Massey products, at the expense of taking a non-standard basis for I^n/I^{n+1}. In this subsection, we assume that $H \cong \mathbb{F}_p^r$ for some $r \geq 1$. Correspondingly, we take $n < p$ and $R = \mathbb{F}_p$.

We let $V^\vee = \mathrm{Hom}(V, \mathbb{F}_p)$ for an abelian group V. For any element $\chi \in H^\vee$, we have a homomorphism

$$\begin{bmatrix} \chi \\ n \end{bmatrix} \colon H \to \mathrm{U}_{n+1}(\mathbb{F}_p).$$

Precomposing with $G \to H$, we may view χ as a character of G. This gives an $(n,0)$-partial defining system, and we set $p_{\chi,n} = p_{\left[\begin{smallmatrix}\chi\\ n\end{smallmatrix}\right],0}$ for brevity. By (4.1), the map $p_{\chi,n}$ induces a map $p_{\chi,n} \colon I^n/I^{n+1} \to \mathbb{F}_p$, so $p_{\chi,n} \in (I^n/I^{n+1})^\vee$. This defines a function $p_{-,n} \colon H^\vee \to (I^n/I^{n+1})^\vee$.

Let us fix an isomorphism $H \xrightarrow{\sim} \mathbb{F}_p^r$, which in turn fixes an ordered dual basis $(\gamma_i)_{i=1}^r$ of H. Setting $x_i = [\gamma_i] - 1 \in \Omega$, this provides an identification

$$\Omega/I^{n+1} = \mathbb{F}_p[x_1, \ldots, x_n]/(x_1, \ldots, x_r)^{n+1}. \tag{4.3}$$

Then I^n/I^{n+1} has a basis given by $x_1^{d_1} \cdots x_r^{d_r}$ with $(d_1, \ldots, d_r)$ ranging over r-tuples of nonnegative integers with $d_1 + \cdots + d_r = n$. We compute $p_{\chi,n}$ on this basis.

Lemma 4.5.1. *Let $\chi \in H^\vee$. For any nonnegative integers $d_1, \dots, d_r$ with sum n, we have*

$$p_{\chi,n}(x_1^{d_1} \cdots x_r^{d_r}) = \prod_{i=1}^r \chi(\gamma_i)^{d_i}.$$

Proof. We have

$$p_{\chi,n}(x_i) = \left(\begin{bmatrix} \chi(\gamma_i) \\ n \end{bmatrix} - 1 \right) e = ((1+u_n)^{\chi(\gamma_i)} - 1)e \in \mathfrak{U}_{\left[\substack{\chi \\ n}\right]},$$

where u_n is as in Section 4.2 and e is as in Lemma 4.1.1. Note that u_n^n has a 1 in its $(1, n+1)$ entry and all other entries 0, and $u_n^{n+1} = 0$. For $d_1 + \cdots + d_r = n$, the value $p_{\chi,n}(x_1^{d_1} \cdots x_r^{d_r})$ is the $(1, n+1)$-entry of the matrix

$$\prod_{i=1}^r ((1+u_n)^{\chi(\gamma_i)} - 1)^{d_i} = \prod_{i=1}^r (\chi(\gamma_i) u_n)^{d_i} = \left(\prod_{i=1}^r \chi(\gamma_i)^{d_i} \right) u_n^n,$$

proving the lemma. □

The key lemma is then the following.

Lemma 4.5.2. *The image of $p_{-,n} \colon H^\vee \to (I^n/I^{n+1})^\vee$ generates $(I^n/I^{n+1})^\vee$.*

Proof. Using our identification (4.3), any non-zero $F \in I^n/I^{n+1}$ has a unique representative also denoted F in $\mathbb{F}_p[x_1, \dots, x_r]$ that is homogeneous of degree n and Lemma 4.5.1 implies that

$$p_{\chi,n}(F) = F(\chi(\gamma_1), \dots, \chi(\gamma_r)).$$

Writing $\Gamma \colon H^\vee \to \mathbb{F}_p^r$ for the isomorphism given by $\Gamma(\chi) = (\chi(\gamma_1), \dots, \chi(\gamma_r))$, this can be succinctly written as $p_{\chi,n}(F) = F(\Gamma(\chi))$.

For a finite set S and an $s \in S$, we denote by $\mathbb{F}_p^S$ the vector space of functions $S \to \mathbb{F}_p$ and by $1_s \in \mathbb{F}_p^S$ the indicator function of s. The lemma may then be rephrased as the statement that the linearization $\tilde{p}_{-,n}$ of $p_{-,n}$, given by

$$\tilde{p}_{-,n} \colon \mathbb{F}_p^{H^\vee} \to (I^n/I^{n+1})^\vee, \quad 1_\chi \mapsto p_{\chi,n}$$

is surjective, or equivalently that the dual map

$$\tilde{p}_{-,n}^\vee \colon I^n/I^{n+1} \to (\mathbb{F}_p^{H^\vee})^\vee$$

is injective. For any non-zero $F \in I^n/I^{n+1}$, since $n < p$, the finite field Nullstellensatz provides the existence of $v \in \mathbb{F}_p^r$ for which $F(v) \neq 0$. Then

$$\tilde{p}_{-,n}^\vee(F)(1_{\Gamma^{-1}(v)}) = p_{\Gamma^{-1}(v),n}(F) = F(v) \neq 0,$$

so $\tilde{p}_{-,n}^\vee(F) \neq 0$. □

Remark 4.5.3. This lemma is the reason for our assumption that $n < p$ in this section rather than the assumption $n|R| < p|A|$ used in other sections. To see that this argument cannot work for torsion-free abelian groups H and arbitrary n, take $R = \mathbb{F}_p$ and $H \cong \mathbb{Z}_p^2$. Then we know that I^n/I^{n+1} has dimension $n+1$ for any n, and the proof of Lemma 4.5.2 shows that $p_{-,n}\colon \operatorname{Hom}(H, \mathbb{F}_p) \to (I^n/I^{n+1})^\vee$ is homogeneous of degree n in the sense that $p_{a\varphi,n} = a^n p_{\varphi,n}$ for $\varphi \in \operatorname{Hom}(H, \mathbb{F}_p)$ and $a \in \mathbb{F}_p$, so the span of its image has dimension at most the cardinality of $\operatorname{Hom}(H, \mathbb{F}_p)/\mathbb{F}_p^\times$, which is $p+1$.

We now come to our result expressing values of the generalized Bockstein maps as sums of "cyclic" Massey products. If $\chi \in H^\vee$ and $f \in Z^1(G, T \otimes_R \Omega/I^n)$, then we say that a proper defining system relative to $\begin{bmatrix}\chi\\ n\end{bmatrix}$ is attached to f if it is attached to the image of f in $Z^1(G, T \otimes_R \Omega_\chi/I_\chi^n)$, where $\Omega_\chi = R[H/\ker\chi]$ and I_χ is its augmentation ideal.

Theorem 4.5.4. *There exist $N \geq 1$ and $\chi_1, \ldots, \chi_N \in H^\vee$ such that $(p_{\chi_i,n})_{i=1}^N$ is an ordered $\mathbb{F}_p$-basis of $(I^n/I^{n+1})^\vee$. For any such $(\chi_i)_{i=1}^N$, let $(y_i)_{i=1}^N$ be the basis of I^n/I^{n+1} dual to $(p_{\chi_i,n})_{i=1}^N$. Then for any $f \in Z^1(G, T \otimes_R \Omega/I^n)$, we have*

$$\Psi^{(n)}(f) = \sum_{i=1}^N (\chi_i^{(n)}, \lambda)_{\rho_i} \cdot y_i,$$

where ρ_i is the proper defining system relative to $\begin{bmatrix}\chi_i\\ n\end{bmatrix}$ attached to f and λ is the image of f in $Z^1(G, T)$.

Proof. The first statement is clear from Lemma 4.5.2. For the second statement, let

$$\Psi^{(n)}(f) = \sum_{i=1}^N c_i \cdot y_i.$$

for some $c_i \in H^2(G, T)$. Since $p_{\chi_1,n}, \ldots, p_{\chi_N,n}$ is the dual basis to $y_1, \ldots, y_N$, we have $c_i = p_{\chi_i,n}(\Psi^{(n)}(f))$ for $1 \leq i \leq N$. But by Theorem 4.1.2, we have

$$p_{\chi_i,n}(\Psi^{(n)}(f)) = (\chi_i^{(n)}, \lambda)_{\rho_i}.$$

□

4.6 Heisenberg case

In this section, assume that $H = \mathrm{U}_3(A)$ for a nonzero quotient A of $\mathbb{Z}_p$, and that R is a quotient of A such that either $R = \mathbb{Z}_p$ or $n|R| < p|A|$. We study the generalized Bockstein maps $\Psi^{(n)}$ in the cases $n = 2$ and $n = 3$.

Let

$$x = \left[\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right] - 1, \quad y = \left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right] - 1, \quad z = \left[\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right] - 1 \in \Omega. \tag{4.4}$$

Then I is the two-sided ideal generated by x and y, and $I/I^2 \cong Rx \oplus Ry$. Let $\chi, \psi \colon G \to A$ be the unique characters factoring through H and such that

$$\chi\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) = 1, \quad \chi\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) = 0, \quad \psi\left(\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) = 0, \quad \text{and} \quad \psi\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}\right) = 1.$$

Then $(\chi, \psi) \colon G \to A \times A$ defines a homomorphism.

Lemma 4.6.1. *The R-module I^2/I^3 is freely generated by the image of the set*

$$S_2 = \{x^2, y^2, yx, z\},$$

and I^3/I^4 is R-freely generated by the image of

$$S_3 = \{x^3, xz, yx^2, y^2x, y^3, yz\}.$$

Proof. For any n, Lemma 2.3.1 and the condition that $n|R| < p|A|$ in the case that A is finite are enough to guarantee that the quotient Ω/I^{n+1} is isomorphic to the analogous quotient with A replaced by $\mathbb{Z}_p$, so we may suppose in this proof that $H = U_3(\mathbb{Z}_p)$.

Let Σ be the noncommutative $R[\![z]\!]$-power series ring Σ in variables x and y. It follows from the standard presentation of $U_3(\mathbb{Z}_p)$ as a finitely generated pro-p group that $\Omega = R[\![U_3(\mathbb{Z}_p)]\!]$ is the quotient of Σ by the ideal generated by

$$w = (1+y)(1+x)z - (xy - yx). \tag{4.5}$$

The augmentation ideal I of Ω is (x, y), so I^n is generated by the monomials in x and y of degree at least n. Using (4.5), we can reduce this to

$$I^n = (y^j x^i z^k \mid i + j + 2k \geq n).$$

It is therefore enough to check that the image of the set S_n is R-linearly independent in I^n/I^{n+1} for $n \in \{2, 3\}$.

Consider Σ as a graded R-algebra with x, y, and z in degrees 1, 1, and 2, respectively. Let J_n denote the ideal of elements of Σ of degree at least n. Suppose that $f \in \Sigma$ lies in the intersection of the R-span of the elements of S_n with $(w) + J_{n+1}$. When $n = 2$, one can easily see that $f = 0$. When $n = 3$, there are $a, b, c, d \in R$ such that

$$f + J_4 = (ax + by)w + w(cx + dy) + J_4.$$

By the hypothesis on f, the degree 3 terms above are in the R-span of S_3, which forces $a = b = c = d = 0$, and hence $f = 0$. $\square$

Let us first consider the case $n = 2$. By Lemma 4.6.1, we see that I^2/I^3 is a free R-module on the set $S_2 = \{x^2, y^2, yx, z\}$. We consider the three partial defining systems

$$\phi_{x^2} = \begin{bmatrix} \chi \\ 2 \end{bmatrix}, \quad \phi_{y^2} = \begin{bmatrix} \psi \\ 2 \end{bmatrix}, \quad \phi_z \colon H \to \mathrm{U}_3(R) \times \mathrm{U}_1(R) = \mathrm{U}_3(R),$$

with $a = 2$ and $b = 0$, where ϕ_z is the quotient map on coefficients, and the partial defining system

$$\phi_{yx} = (\chi, \psi) \colon H \to \mathrm{U}_2(R) \times \mathrm{U}_2(R) = R \times R$$

for $a = b = 1$. By Theorem 3.3.4, the partial defining systems ϕ_{x^2}, ϕ_{y^2}, ϕ_z, and ϕ_{yx} correspond to Massey products $(\chi, \chi, \cdot\,)$, $(\psi, \psi, \cdot\,)$, $(\chi, \psi, \cdot\,)$, and $(\chi, \cdot\,, \psi)$, respectively.

As for $n = 3$, the graded quotient I^3/I^4 is a free R-module on S_3 of Lemma 4.6.1. For each $s \in S_3$, we define a partial defining system ϕ_s (viewed as a pair of homoorphisms) as follows:

$$\begin{aligned}
\phi_{x^3} \colon H &\xrightarrow{\left[\begin{smallmatrix}\chi\\3\end{smallmatrix}\right],0} \mathrm{U}_4(R) \times \mathrm{U}_1(R), \\
\phi_{xz} \colon H &\xrightarrow{\mathrm{id},\chi} \mathrm{U}_3(R) \times \mathrm{U}_2(R), \\
\phi_{yx^2} \colon H &\xrightarrow{\psi,\left[\begin{smallmatrix}\chi\\2\end{smallmatrix}\right]} \mathrm{U}_2(R) \times \mathrm{U}_3(R), \\
\phi_{y^2x} \colon H &\xrightarrow{\left[\begin{smallmatrix}\psi\\2\end{smallmatrix}\right],\chi} \mathrm{U}_3(R) \times \mathrm{U}_2(R), \\
\phi_{y^3} \colon H &\xrightarrow{\left[\begin{smallmatrix}\psi\\3\end{smallmatrix}\right],0} \mathrm{U}_4(R) \times \mathrm{U}_1(R), \\
\phi_{yz} \colon H &\xrightarrow{\psi,\mathrm{id}} \mathrm{U}_2(R) \times \mathrm{U}_3(R).
\end{aligned}$$

By Theorem 3.3.4, each partial defining system corresponds to a collection of Massey products as follows:

$$\begin{aligned}
\phi_{x^3} &\longleftrightarrow (\chi, \chi, \chi, \cdot\,), \\
\phi_{xz} &\longleftrightarrow (\chi, \psi, \cdot\,, \chi), \\
\phi_{yx^2} &\longleftrightarrow (\psi, \cdot\,, \chi, \chi), \\
\phi_{y^2x} &\longleftrightarrow (\psi, \psi, \cdot\,, \chi), \\
\phi_{y^3} &\longleftrightarrow (\psi, \psi, \psi, \cdot\,), \\
\phi_{yz} &\longleftrightarrow (\psi, \cdot\,, \chi, \psi).
\end{aligned}$$

For each $s \in S_n$ with $n \in \{2, 3\}$, the diagram (4.1) becomes

$$\begin{tikzcd}
0 \arrow[r] & T \otimes_R I^n/I^{n+1} \arrow[r] \arrow[d, "p_s"] & T \otimes_R \Omega/I^{n+1} \arrow[r] \arrow[d, "p_s"] & T \otimes_R \Omega/I^n \arrow[r] \arrow[d, "p_s"] & 0 \\
0 \arrow[r] & T \arrow[r] & \mathfrak{U}_s(T) \arrow[r] & \mathfrak{U}'_s(T) \arrow[r] & 0,
\end{tikzcd}$$

where the maps p_s are induced by the map ϕ_s and we have used the shorthand $\mathfrak{U}_s(T)$ for $\mathfrak{U}_{\phi_s}(T)$ (and similarly for the quotients). Note that $p_s\colon T \otimes_R I^n/I^{n+1} \to T$ is just the R-tensor product of the likewise-defined $p_s\colon I^n/I^{n+1} \to R$ with the identity on T. The maps $p_s\colon I^n/I^{n+1} \to R$ for $s \in S_n$ form the dual basis to the R-basis S_n of I^n/I^{n+1}. This can be seen by an omitted direct computation, proceeding as in the following example.

Example 4.6.2. Suppose that $n = 2$, and take $s = z \in S_2$. Recall that $\phi_z\colon H \to U_3(R)$ is given by the canonical surjection $A \to R$ on coefficients. By definition of $p_z\colon \Omega/I^3 \to \mathfrak{U}_{\phi_z}(R) = M_{3,1}(R)$ in Lemma 4.1.1, we have

$$p_z([h]) = \phi_z(h) \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) \in M_{3,1}(R)$$

for all $h \in H$. Recalling that $x+1$, $y+1$, and $z+1$ are the group elements of matrices as in (4.4), we compute

$$\begin{aligned}
p_z(x^2) &= \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) - 2\left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) = 0, \\
p_z(y^2) &= \left(\begin{smallmatrix} 0 \\ 2 \\ 1 \end{smallmatrix}\right) - 2\left(\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) = 0, \\
p_z(yx) &= \left(\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) = 0, \\
p_z(z) &= \left(\begin{smallmatrix} 1 \\ 0 \\ 1 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right),
\end{aligned} \tag{4.6}$$

and note that $\left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right)$ gives the identity of $R \subset \mathfrak{U}_{\phi_z}(R)$.

By Theorem 4.1.2, we then have the following.

Theorem 4.6.3. *For $n \in \{2,3\}$ and $f \in Z^1(G, T \otimes_R \Omega/I^n)$, the element $\Psi^{(n)}(f)$ of*

$$H^2(G,T) \otimes_R I^n/I^{n+1} \cong \bigoplus_{s \in S_n} H^2(G,T)s$$

is the sum

$$(\chi,\chi,\lambda)_{\rho_{x^2}} x^2 + (\chi,\lambda,\psi)_{\rho_{yx}} yx + (\psi,\psi,\lambda)_{\rho_{y^2}} y^2 + (\chi,\psi,\lambda)_{\rho_z} z \tag{4.7}$$

for $n = 2$ and the sum

$$\begin{aligned}
&(\chi,\chi,\chi,\lambda)_{\rho_{x^3}} x^3 + (\chi,\psi,\lambda,\chi)_{\rho_{xz}} xz + (\psi,\lambda,\chi,\chi)_{\rho_{yx^2}} yx^2 \\
&\quad + (\psi,\psi,\lambda,\chi)_{\rho_{y^2x}} y^2x + (\psi,\psi,\psi,\lambda)_{\rho_{y^3}} y^3 + (\psi,\lambda,\chi,\psi)_{\rho_{yz}} yz
\end{aligned} \tag{4.8}$$

for $n = 3$, where each ρ_s for $s \in S_n$ is the proper defining system relative to ϕ_s attached to $p_s \circ f$ by Lemma 3.3.3, and λ is the image of f in $Z^1(G,T)$.

As before, Theorem 2.2.4 then provides the following isomorphisms.

Corollary 4.6.4. *Suppose that G is p-cohomologically finite of p-cohomological dimension 2. For $n \in \{2,3\}$, let $P_n(H)$ denote the subgroup of $H^2(G,T) \otimes_R I^n/I^{n+1}$ consisting of all sums in* (4.7) *for $n = 2$ and in* (4.8) *for $n = 3$. We then have a canonical isomorphism of R-modules*

$$\frac{I^n H^2_{\mathrm{Iw}}(N,T)}{I^{n+1} H^2_{\mathrm{Iw}}(N,T)} \cong \frac{H^2(G,T) \otimes_R I^n/I^{n+1}}{P_n(H)}.$$

5 Applications to cyclotomic fields

In this section, we apply our general results to study class groups of finite extensions of a cyclotomic field $\mathbb{Q}(\mu_p)$ with p an irregular prime. That is, under assumptions that include vanishing of certain cup products, we are able to bound the sizes of the p-parts of the class groups from below. This is a particularly simple setting where the p-parts of class groups can be directly identified with second cohomology groups. Even in this setting, we are satisfied to demonstrate the method in a special case. Rather general results in an Iwasawa-theoretic context may be obtained as in [Sh4, Section 4].

5.1 Notation and preliminaries

In this subsection, we recall some standard facts regarding the mod p unramified outside p cohomology of the pth cyclotomic field, for an odd prime p. Most of these may be found, for instance, in [McS]. Let Cl_K denote the ideal class group of a number field K. Let S denote the set of primes over p in any number field. Let $\mathrm{Cl}_{K,S}$ denote the S-class group of K, which is to say the class group of the ring $\mathcal{O}_{K,S}$ of S-integers of K. Let $G_{K,S}$ denote the Galois group of the maximal unramified outside S, or *p-ramified*, extension of K.

For any number field K and prime p, Kummer theory provides an exact sequence

$$0 \to \mathcal{O}_{K,S}^{\times} \otimes_{\mathbb{Z}} \mathbb{F}_p \to H^1(G_{K,S}, \mu_p) \to \mathrm{Cl}_{K,S}[p] \to 0$$

and a canonical injection

$$\mathrm{Cl}_{K,S} \otimes_{\mathbb{Z}} \mathbb{F}_p \hookrightarrow H^2(G_{K,S}, \mu_p)$$

of $\mathbb{F}_p[\Delta]$-modules. The latter injection is an isomorphism if K is a p-ramified, purely imaginary extension of $\mathbb{Q}$ with a unique prime over p. We shall write Massey products of elements of $H^1(G_{F,S}, \mu_p)$ as products of elements of $F^{\times}/F^{\times p}$ whose Kummer cocycles (in this case characters) give classes in $H^1(G_{F,S}, \mu_p)$, as opposed to the cocycles themselves.

Now let $F = \mathbb{Q}(\zeta_p)$ for an odd prime p and a primitive pth root of unity ζ_p. Note that $\mathcal{O}_{F,S} = \mathbb{Z}[\zeta_p, \frac{1}{p}]$ and $\mathrm{Cl}_{F,S} = \mathrm{Cl}_F$, since the prime $(1 - \zeta_p)$ over p is principal. Let

$\Delta = \mathrm{Gal}(F/\mathbb{Q})$, and let $\omega\colon \Delta \to \mathbb{Z}_p^\times$ be unique lift of the mod p cyclotomic character. For $j \in \mathbb{Z}$, the ω^j-isotypical component, or *eigenspace*, of a $\mathbb{Z}_p[\Delta]$-module M is

$$M^{(j)} = \{m \in M \mid \delta m = \omega(\delta)^j m \text{ for all } \delta \in \Delta\}.$$

We say that a positive even integer $k < p$ is an *irregular index* for p if $\mathrm{Cl}_F[p]^{(1-k)} \neq 0$, or equivalently, p divides the numerator of the kth Bernoulli number B_k. As p divides the denominator of B_{p-1}, every irregular index k for p satisfies $k \leq p-3$.

We suppose that p satisfies Vandiver's conjecture that $\mathrm{Cl}_{\mathbb{Q}(\zeta_p+\zeta_p^{-1})}[p] = 0$. By Leopoldt's reflection principle, this implies that for each irregular index k, the eigenspace $\mathrm{Cl}_F[p]^{(1-k)}$ is cyclic, so we fix a generator and let $\alpha_k \in H^1(G_{F,S}, \mu_p)^{(1-k)}$ be its unique lift. This also allows us to identify $H^2(G_{F,S}, \mu_p)^{(1-k)}$ with $\mathbb{F}_p$ via the isomorphisms

$$\mathbb{F}_p \xrightarrow{1\mapsto\alpha_k} H^1(G_{F,S}, \mu_p)^{(1-k)} \xrightarrow{\sim} \mathrm{Cl}_F[p]^{(1-k)} \xrightarrow{\sim} (\mathrm{Cl}_F \otimes_{\mathbb{Z}} \mathbb{F}_p)^{(1-k)} \xrightarrow{\sim} H^2(G_{F,S}, \mu_p)^{(1-k)},$$

where the isomorphism $(\mathrm{Cl}_F \otimes_{\mathbb{Z}} \mathbb{F}_p)^{(1-k)} \xrightarrow{\sim} \mathrm{Cl}_F[p]^{(1-k)}$ is multiplication by a power of p.

For an odd integer i, we define

$$\eta_i \in (\mathcal{O}_{F,S}^\times \otimes_{\mathbb{Z}} \mathbb{F}_p)^{(1-i)}$$

to be the projection of $1-\zeta_p$ into that eigenspace. We often refer to the index i as taking values in $\mathbb{Z}/(p-1)\mathbb{Z}$. Via Kummer theory, we identify η_i with an element of

$$H^1(G_{F,S}, \mu_p)^{(1-i)} \cong (H^1(G_{F,S}, \mu_p) \otimes_{\mathbb{Z}} \mu_p^{\otimes(i-1)})^\Delta \cong H^1(G_{F,S}, \mu_p^{\otimes i})^\Delta$$

and ζ_p with an element of $H^1(G_{F,S}, \mu_p)^{(1)}$. Vandiver's conjecture for p is equivalent to the statement that every η_i is nontrivial. We codify all this and a bit more in the following remark.

Remark 5.1.1. For any positive integer $j < p$, the eigenspace $H^1(G_{F,S}, \mu_p)^{(1-j)}$ is cyclic, generated by the element

- η_j if j is odd,
- ζ_p if $j = p-1$,
- α_j if j is an irregular index,

and is trivial for all other j. If i is odd, then cup product with η_i vanishes on $H^1(G_{F,S}, \mu_p)$ if and only if $\eta_i \cup \eta_{k-i} = 0$ for all irregular indices k for p.

Given a p-extension L/F that unramified outside p and for which $L/\mathbb{Q}$ is Galois, we can consider its Galois group $H = \mathrm{Gal}(L/F)$, which is of course normal inside $\mathrm{Gal}(L/\mathbb{Q})$. Set $\Omega = \mathbb{F}_p[H]$ as before. We have an action of $G_{\mathbb{Q},S}$ on Ω such that $g \in G_{\mathbb{Q},S}$ sends the image $[h]$ of $h \in H$ to $[\bar{g}h\bar{g}^{-1}]$, where $\bar{g}$ is the image of g in G.

Since $G_{F,S}$ is normal in $G_{\mathbb{Q},S}$, this $G_{\mathbb{Q},S}$-action (together with right conjugation on $G_{F,S}$ in the usual fashion) induces a $\mathrm{Gal}(L/\mathbb{Q})$-action on $H^*(G_{F,S}, \mu_p \otimes_{\mathbb{F}_p} I^n/I^m)$ for every $0 \leq n < m$. For $m = n+1$, this action factors through Δ. We fix a lift of Δ to a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ so that we may speak of the Δ-action on these cohomology groups for all $n < m$, though in general this action depends upon the choice of lift. The generalized Bockstein maps $\Psi^{(n)}$ are then Δ-equivariant.

5.2 Class groups of bicyclic and Heisenberg extensions

In this subsection, we let $i, j < p$ be distinct odd positive integers and set $K = F(\eta_i^{1/p}, \eta_j^{1/p})$, with the slight abuse of notation that we are in fact taking pth roots of any lifts of η_i and η_j. Note that $K/\mathbb{Q}$ is Galois. We assume throughout this subsection that

- $\mathrm{Cl}_F[p]$ is cyclic, and
- the cup products $\eta_i \cup \eta_{k-i}$ and $\eta_j \cup \eta_{k-j}$ vanish.

By the first assumption, p has a unique irregular index k and Vandiver's conjecture holds for p. In particular, K is an $\mathbb{F}_p^2$-extension of F. The interested reader might calculate how the bounds we give are worsened as one weakens these assumptions.

For $h \in \mathbb{Z}/(p-1)\mathbb{Z}$, let

$$\delta_h = \begin{cases} 1 & \text{if } h \in \{0, k\}, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 5.2.1. *We have*

$$\dim_{\mathbb{F}_p} H^2(G_{K,S}, \mu_p) \geq 6 - \delta_{2i} - \delta_{i+j} - \delta_{2j}.$$

Proof. We will apply the results of Section 4.4 in the case that $G = G_{F,S}$ and $H = \mathrm{Gal}(K/F)$. To construct our lower bound, we will use the fact that $\dim_{\mathbb{F}_p} H^2(G_{K,S}, \mu_p) \geq \sum_{n=0}^{2} d_n$, where

$$d_n = \dim_{\mathbb{F}_p} \frac{I^n H^2(G_{K,S}, \mu_p)}{I^{n+1} H^2(G_{K,S}, \mu_p)}.$$

So, first note that

$$\frac{H^2(G_{K,S}, \mu_p)}{I H^2(G_{K,S}, \mu_p)} \cong H^2(G_{F,S}, \mu_p) \cong (\mathrm{Cl}_F \otimes_{\mathbb{Z}} \mathbb{F}_p)^{(1-k)},$$

and the latter group has $\mathbb{F}_p$-dimension 1 by our assumption of Vandiver's conjecture, so $d_0 = 1$.

Let x and y be the ordered basis of $I/I^2 \cong H$ that is Kummer dual to η_i and η_j. The quantity $(\eta_i \cup \lambda)x + (\eta_j \cup \lambda)y$ is zero for λ one of the generators of $H^1(G_{F,S}, \mu_p)$ listed in Remark 5.1.1 unless (perhaps) if λ is one of η_{k-i} or η_{k-j}, in which cases it equals $(\eta_i \cup \eta_{k-i})x$ and $(\eta_j \cup \eta_{k-j})y$, respectively. Thus, by Proposition 2.3.3 and Theorem 2.2.4 for $n = 1$, we have

$$\frac{IH^2(G_{K,S}, \mu_p)}{I^2H^2(G_{K,S}, \mu_p)} \cong \frac{H^2(G_{F,S}, \mu_p) \otimes_{\mathbb{F}_p} I/I^2}{\langle (\eta_i \cup \eta_{k-i})x, (\eta_j \cup \eta_{k-j})y \rangle},$$

and given the vanishing of the cup products on the right, we see that $d_1 = 2$.

Theorem 2.2.4 tells us that $d_2 = \dim_{\mathbb{F}_p} \operatorname{coker} \Psi^{(2)}$. For $\tilde{\lambda} \in H^1(G_{F,S}, \Omega/I^2 \otimes_{\mathbb{F}_p} \mu_p)$ with image $\lambda \in H^1(G_{F,S}, \mu_p)$, Corollary 4.4.4 provides the explicit formula

$$\Psi^{(2)}(\tilde{\lambda}) = (\eta_i, \eta_i, \lambda)_{\rho_{x^2}} x^2 + (\eta_i, \lambda, \eta_j)_{\rho_{xy}} xy + (\lambda, \eta_j, \eta_j)_{\rho_{y^2}} y^2. \tag{5.1}$$

Since cup products with η_i and η_j are trivial by assumption and Remark 5.1.1, we see that the expression on the right of (5.1) is independent of the proper defining systems, and therefore $\Psi^{(2)}$ factors through $H^1(G_{F,S}, \mu_p)$.

Now suppose that for some h we have $\lambda \in H^1(G_{F,S}, \mu_p)^{(1-h)}$, a space of dimension at most 1. Note that Δ acts on x^2 through ω^{2i}, on xy through ω^{i+j}, and on y^2 through ω^{2j}. We then see by Remark 5.1.1 that the Massey products in (5.1) can be nontrivial if and only if $h - 2i$, $h - i - j$, or $h - 2j$ (in that order) is congruent to 0 or k modulo $p - 1$, which is to say if and only if $\delta_{2i} = 1$, $\delta_{i+j} = 1$, or $\delta_{2j} = 1$. Since $\dim_{\mathbb{F}_p} H^2(G_{F,S}, \mu_p) \otimes_{\mathbb{F}_p} I^2/I^3 = \dim_{\mathbb{F}_p} I^2/I^3 = 3$, we have $d_2 \geq 3 - \delta_{2i} - \delta_{i+j} - \delta_{2j}$, as required. □

Note that $\eta_i \cup \eta_j = 0$, since we must have $j \equiv k - i \bmod p - 1$ for this cup product not to vanish, and we have assumed that $\eta_i \cup \eta_{k-i} = 0$. Thus, there exists a degree p extension L of K, Galois over F and unramified outside p, such that $\operatorname{Gal}(L/F) \cong U_3(\mathbb{F}_p)$. We can and do choose L to be Galois over $\mathbb{Q}$: in fact, [Sh1, Proposition 2.7] provides the following description of Kummer generators of such fields L, viewed as extensions of K.

Remark 5.2.2. Set $E = F(\eta_i^{1/p})$, and let σ be a generator of $\operatorname{Gal}(E/F)$. Write $\eta_j = \prod_{i=0}^{p-1} \sigma^i \beta'$ for some $\beta' \in E^\times/E^{\times p}$. Pick a lift of Δ to a subgroup of $\operatorname{Gal}(E/\mathbb{Q})$. Let β be the projection of β' to the ω^j-eigenspace of $E^\times/E^{\times p}$ for the action of this lift. The fact that $\eta_j \in (F^\times/F^{\times p})^{(j)}$ implies that $\eta_j = \prod_{i=0}^{p-1} \sigma^i \beta$ as well. We then have $L = K((c\gamma)^{1/p})$ for $\gamma = \prod_{i=1}^{p-1} \sigma^i \beta^i$ and any $c \in H^1(G_{F,S}, \mu_p)^{(1-i-j)}$. The latter group is zero if $\delta_{i+j} = 0$ (see Remark 5.1.1), in which case L is unique.

The group Δ acts on $\mathrm{Gal}(L/K)$ by conjugation through ω^{i+j}. It may be helpful for the reader to view $\mathrm{Gal}(L/\mathbb{Q})$ as the group of matrices

$$\begin{pmatrix} \omega(\delta)^i & * & * \\ 0 & 1 & * \\ 0 & 0 & \omega(\delta)^{-j} \end{pmatrix}$$

for some $\delta \in \Delta$.

Proposition 5.2.3. *We have*

$$\dim_{\mathbb{F}_p} H^2(G_{L,S}, \mu_p) \geq 7 - \delta_{2i} - \delta_{2j} - \delta_{i+j}.$$

Proof. We will apply the results of Section 4.6 in the case that $G = G_{F,S}$ and $H = \mathrm{Gal}(L/F)$. Set

$$d_n = \dim_{\mathbb{F}_p} \frac{I^n H^2(G_{L,S}, \mu_p)}{I^{n+1} H^2(G_{L,S}, \mu_p)}.$$

We have $d_0 = 1$ and $d_1 = 2$ by the same arguments as for K/F (noting that in the Heisenberg case, we still have $I/I^2 \cong H^{\mathrm{ab}} \cong \mathbb{F}_p^2$). As in the proof of Proposition 5.2.1, we must give a lower bound on $d_2 = \dim_{\mathbb{F}_p} \operatorname{coker} \Psi^{(2)}$.

Corollary 4.6.4 tells us that for $\tilde{\lambda} \in H^1(G_{F,S}, \Omega/I^2 \otimes_{\mathbb{F}_p} \mu_p)$ with image $\lambda \in H^1(G_{F,S}, \mu_p)$, we have

$$\Psi^{(2)}(\tilde{\lambda}) = (\eta_i, \eta_i, \lambda)_{\rho_{x^2}} x^2 + (\eta_i, \lambda, \eta_j)_{\rho_{yx}} yx + (\eta_j, \eta_j, \lambda)_{\rho_{y^2}} y^2 + (\eta_i, \eta_j, \lambda)_{\rho_z} z.$$

Again, the vanishing of $\eta_i \cup \eta_{k-i}$ and $\eta_j \cup \eta_{k-j}$ ensures that $\Psi^{(2)}(\tilde{\lambda})$ depends only on λ. As before, but now noting also that Δ acts on $z \in I^2/I^3$ by ω^{i+j}, we see that these Massey products must vanish unless $\delta_{2i} = 1$, $\delta_{i+j} = 1$, $\delta_{2j} = 1$, and $\delta_{i+j} = 1$, respectively. Moreover, if $\delta_{i+j} = 1$, then the image of $\Psi^{(2)}$ on $H^1(G_{F,S}, I/I^2 \otimes_{\mathbb{F}_p} \mu_p)^{(k-i-j)}$ is at most one-dimensional, generated by $(\eta_i, \lambda, \eta_j)yx + (\eta_i, \eta_j, \lambda)z$ for $\lambda = \zeta_p$ or $\lambda = \alpha_k$, by Remark 5.1.1 (and similarly for the other cases). Thus, we have $d_2 \geq 4 - \delta_{2i} - \delta_{2j} - \delta_{i+j}$. $\square$

Remark 5.2.4.

1. If $2i \equiv k \bmod p-1$, so in particular $\delta_{2i} = 1$, then the condition that $\eta_i \cup \eta_i = 0$ is automatic by antisymmetry of the cup product.

2. It occurs that δ_{2i}, δ_{2j}, and δ_{i+j} are all 1 if and only if p is 1 modulo 4 but not 8 and $k = \frac{p-1}{2}$, so that we have $\{i, j\} = \{\frac{p-1}{4}, \frac{3(p-1)}{4}\}$.

   We can have $2i \equiv 0 \bmod p-1$ only if $p \equiv 3 \bmod 4$, in which case $i = \frac{p-1}{2}$. We can then also choose j such that $2j \equiv k \bmod p-1$ (see Example 5.2.5), but then $i+j$ is either $\frac{k}{2}$ or $\frac{k}{2} + \frac{p-1}{2}$ modulo $p-1$, which cannot be 0 or k, so $\delta_{i+j} = 0$.

3. The pth root of η_{p-k} generates the unique degree p unramified extension of F, and it satisfies $\eta_{p-k} \cup \eta_{2k-1} = 0$. In such a setting, $\dim_{\mathbb{F}_p} H^2(G_{F(\eta_{p-k}^{1/p}),S}, \mu_p) = p-1$, coming entirely from the Brauer part of this second cohomology group.

   On the other hand, suppose that i and j are not $p-k$ modulo $p-1$. (By what we have just said, we can take one of them to be $2k-1$, so long as $2k-1$ is not $p-k$ modulo $p-1$, i.e., $3k \not\equiv 2 \bmod p-1$.) Then $K/\mathbb{Q}$ is totally ramified at p, which forces $L/\mathbb{Q}$ to be as well. This implies that

$$H^2(G_{K,S}, \mu_p) \cong \mathrm{Cl}_{K,S} \otimes \mathbb{F}_p \quad \text{and} \quad H^2(G_{L,S}, \mu_p) \cong \mathrm{Cl}_{L,S} \otimes \mathbb{F}_p.$$

   In particular, our lower bounds on the $\mathbb{F}_p$-dimensions of these S-class groups give lower bounds on the dimensions of the class groups $\mathrm{Cl}_K \otimes \mathbb{F}_p$ and $\mathrm{Cl}_L \otimes \mathbb{F}_p$.

We conclude with some numerical examples. Many more are available using the tables referenced in [McS], which compute the cup product pairings up to scalar for primes less than 25,000.

Example 5.2.5. Let $p = 59$, for which $k = 44$ is the unique irregular index. For $i = 29$ and $j = 51$, we have $2i \equiv 0 \bmod p-1$ and $2j \equiv k \bmod p-1$, so $\delta_{2i} = \delta_{2j} = 1$, while $\delta_{i+j} = 0$. We then have $\eta_j \cup \eta_{k-j} = \eta_{51} \cup \eta_{51} = 0$ and $\eta_i \cup \eta_{k-i} = \eta_{29} \cup \eta_{15} = 0$ as in Remark 5.2.4, noting that $15 = p-k$. Given this, Propositions 5.2.1 and 5.2.3 provide the following lower bounds on the p-ranks of the class groups of K and L:

$$\dim_{\mathbb{F}_p} \mathrm{Cl}_K \otimes \mathbb{F}_p \geq 4 \quad \text{and} \quad \dim_{\mathbb{F}_p} \mathrm{Cl}_L \otimes \mathbb{F}_p \geq 5.$$

The relevant, potentially nonzero, Massey triple products in this example are $(\eta_{51}, \eta_{51}, \zeta_{59})$ and $(\eta_{29}, \eta_{29}, \alpha_{44})$.

Example 5.2.6. Let $p = 67$, for which $k = 58$ is the unique irregular index. For $i = 29$ and $j = 49$, we have $\delta_{2i} = 1$ and $\delta_{2j} = \delta_{i+j} = 0$. Since $p - k = 9 \notin \{29, 49\}$, we have

$$\dim_{\mathbb{F}_p} \mathrm{Cl}_K \otimes \mathbb{F}_p \geq 5 \quad \text{and} \quad \dim_{\mathbb{F}_p} \mathrm{Cl}_L \otimes \mathbb{F}_p \geq 6.$$

Here, the interesting Massey product is $(\eta_{29}, \eta_{29}, \zeta_{67})$.

It is not hard to find examples in which all the error terms vanish, so the maximal lower bounds are achieved.

Example 5.2.7. Let $p = 101$, which has unique irregular index $k = 68$. Take $i = 13$ and $j = 35$. The computations referenced in [McS] show that $\eta_{13} \cup \eta_{55} = 0$, and $\eta_{35} \cup \eta_{33} = 0$ holds since $p - k = 33$. Since $\delta_{i+j} = \delta_{2i} = \delta_{2j} = 0$, we have

$$\dim_{\mathbb{F}_p} \mathrm{Cl}_K \otimes \mathbb{F}_p \geq 6 \quad \text{and} \quad \dim_{\mathbb{F}_p} \mathrm{Cl}_L \otimes \mathbb{F}_p \geq 7.$$

The same lower bounds are achieved for $\{i, j\} = \{35, 55\}$. (Note that $\{i, j\} = \{13, 55\}$ has $\delta_{i+j} = 1$, so the bounds for this pair are one worse.)

Notice that genus theory has no contribution to the lower bounds (for S-class groups) in the above examples. Indeed, an unramified $\mathbb{F}_p$-extension of either K or L which descends to an abelian extension of F would contribute to the zeroth graded piece in the augmentation filtration, but in these examples this is entirely accounted for the class group of F (i.e., all such extensions are already unramified over F).

6 Massey vanishing for absolute Galois groups

In this final section of this paper, we apply our techniques to study absolute Galois groups of fields. The motivating problem is to determine which profinite groups can be isomorphic to the absolute Galois group G_F of a field F. Artin and Schreier showed in 1927 that any nontrivial finite group with this property is the cyclic group has order two. Other restrictions are reflected in the cohomological properties of G_F. The norm residue isomorphism theorem, or Milnor-Bloch-Kato conjecture, proven by Voevodsky and Rost (see [Vo]), tells us that the algebra $H^*(G_F, \mathbb{F}_p)$ under cup product is isomorphic to the mod-p Milnor K-theory of F (for F containing a primitive pth root of 1). In particular, this implies that the $\mathbb{F}_p$-cohomology algebra is generated in degree 1 with all relations generated in degree 2.

Going beyond cup products to higher cohomological operations, Mináč and Tân formulated a remarkable conjecture, known as the *Massey vanishing conjecture*, for Massey products of $\mathbb{F}_p$-valued characters on the absolute Galois group G_F of a field F in [MT4]. For $n \geq 3$, it states that any n-fold Massey product of characters $G_F \to \mathbb{F}_p$ that has a defining system has some defining system for which the resulting Massey product is zero. The Massey product is said to *contain zero* if such a defining system exists.

Prior to the formulation of this conjecture, Hopkins and Wickelgren had already proved using splitting varieties in [HoWi] that for number fields, n-fold Massey products that are defined contain zero for $n = 3$ and $p = 2$. Their work was later generalized to arbitrary p and successively general n: to $n = 3$ in [MT2], to $n = 4$ in [GMT], and in a fairly recent preprint [HrWt] to arbitrary n, all over number fields.

For arbitrary fields F, Efrat–Matzri [EfMa] and Mináč–Tân [MT3] independently proved *triple Massey vanishing*, which is to say the conjecture for $n = 3$ and arbitrary p. Other results tend to require that several of the characters in the Massey products be the same. For instance, the third author had long ago proved in [Sh2] what we refer to here as the *p-cyclic Massey vanishing property* for absolute Galois groups: for $n \leq p-1$, all $(n+1)$-fold Massey products

$(\chi^{(n)}, \psi)$ for $\chi, \psi \in H^1(G_F, \mathbb{F}_p)$ with $\chi \cup \psi = 0$ vanish with respect to some proper defining system. More recently, Mináč and Tân [MT1] proved the vanishing of n-fold Massey products when all n characters are the same, for arbitrary n.

6.1 The cyclic Massey vanishing property

Definition 6.1.1. Let G be a profinite group, and let p be a prime number. We say that G has the *p-cyclic Massey vanishing property* if for all homomorphisms $\chi, \lambda \colon G \to \mathbb{F}_p$ with $\chi \cup \lambda = 0$, there exists a proper defining system such that $(\chi^{(p-1)}, \lambda)$ vanishes.

As a simple corollary of [Sh2, Theorem 4.3], the absolute Galois group of field F containing a primitive pth root of unity has the p-cyclic Massey vanishing property. (For this, consider the case that Ω is the separable closure of K and $m = 1$ in the notation of said theorem.) The proof uses only the fact that if the norm residue symbol $(a, b)_{p,F}$ vanishes, then b is a norm from $F(a^{1/p})$. We shall give a streamlined proof of this and more, using the following abstract characterization of a standard property of absolute Galois groups.

Definition 6.1.2. Let $m \geq 1$, and set $R = \mathbb{Z}/m\mathbb{Z}$. We say that a profinite group G is of *m-absolute Galois type* if it has the property that, for any $\chi \in H^1(G, R)$, the sequence

$$H^1(G, R[H_\chi]) \to H^1(G, R) \xrightarrow{\chi \cup} H^2(G, R) \to H^2(G, R[H_\chi]) \tag{6.1}$$

is exact, where $H_\chi = G/\ker(\chi)$ is the coimage of χ.

Under Shapiro's lemma, the first and last maps in (6.1) are identified with corestriction and restriction maps, respectively [NSW, Proposition 1.6.5]. It is well-known that an absolute Galois group G_F is of m-absolute Galois type if F contains a primitive mth root of unity (see for instance [Se, Propositions XIV.2 and XIV.4]). This condition on G_F generalized to arbitrary cohomological degree is heavily used in the proof of the norm residue isomorphism theorem: see [HsWe, Theorem 3.6]. We focus on the comparison of p-absolute Galois type with p-cyclic Massey vanishing. In fact, our results would allow us to prove a more general but analogous result for profinite groups with the property that characters on G of order p^s lift to characters of order p^t for some large enough t relative to s, under conditions as in Section 4.3.

Proposition 6.1.3. *Let G be a profinite group. Then G has the p-cyclic Massey vanishing property if and only if the sequence* (6.1) *is exact at $H^1(G, \mathbb{F}_p)$.*

Proof. Let $\chi, \lambda\colon G \to \mathbb{F}_p$ with $\chi \cup \lambda = 0$, and set $\Omega = \mathbb{F}_p[H_\chi]$. The pth power of the augmentation ideal in Ω is zero, and the kernel of the generalized Bockstein map $\Psi^{(p-1)}$ is the image of $H^1(G,\Omega) \to H^1(G,\Omega/I^{p-1})$. Theorem 4.3.1 tells us that the Massey product $(\chi^{(p-1)}, \lambda)$ is defined and vanishes for some choice of proper defining system in $H^1(G,\Omega/I^{p-1})$ if and only if λ lifts to $H^1(G,\Omega)$. From this, we have the proposition. □

Proposition 6.1.3 applies in particular to the absolute Galois group of any field F containing a primitive pth root of unity, i.e., G_F has the p-cyclic Massey vanishing property. We also have the following result, which may be of independent interest.

Proposition 6.1.4. *Let G be a profinite group. If* (6.1) *is exact at $H^2(G,\mathbb{F}_p)$ for a given $\chi \in H^1(G,\mathbb{F}_p)$, then it is exact at $H^1(G,\mathbb{F}_p)$, so G is of p-absolute Galois type.*

Proof. Let $\chi, \lambda\colon G \to \mathbb{F}_p$ with $\chi \cup \lambda = 0$, and suppose that (6.1) is exact at $H^2(G,\mathbb{F}_p)$. We have to show that there is a proper defining system ρ such that $(\chi^{(p-1)}, \lambda)_\rho$ vanishes. We may suppose that $\chi \neq 0$. Let $x = [h] - 1$ for $h \in H_\chi$ with $\chi(h) = 1$. By induction on n, we can assume that there is a proper defining system ρ_{x^n} for $(\chi^{(n)}, \lambda)$ with $n < p$ determined by some $f = \sum_{k=0}^{n-1} \lambda_k x^k \in Z^1(G,\Omega/I^n)$, with λ necessarily equal to λ_0. Writing $(\chi^{(n)}, \lambda)_f$ for the corresponding Massey product $(\chi^{(n)}, \lambda)_{\rho_{x^n}}$, we have

$$(\chi^{(n)}, \lambda)_f = \chi \cup \lambda_{n-1} + \binom{\chi}{2} \cup \lambda_{n-2} + \cdots + \binom{\chi}{n} \cup \lambda.$$

Clearly the restriction of $(\chi^{(n)}, \lambda)_f$ to $\ker(\chi)$ vanishes, so, by the exactness of (6.1) at $H^2(G,\mathbb{F}_p)$, we have $(\chi^{(n)}, \lambda)_f = \chi \cup \psi$ for some $\psi \in H^1(G,\mathbb{F}_p)$. Then we see that $f' = f - \psi x^{n-1}$ is a proper defining system such that the Massey product $(\chi^{(n)}, \lambda)_{f'}$ vanishes. By Theorem 4.3.1, this implies that the class of f' is in the kernel of $\Psi^{(n)}$, so it lifts to the class of some $\tilde{f} \in Z^1(G,\Omega/I^{n+1})$, which gives rise to a proper defining system $\rho_{x^{n+1}}$ for $(\chi^{(n+1)}, \lambda)$. If $n+1 = p$, then the class of $\tilde{f}$ is the desired lift to $H^1(G,\Omega)$. □

It is unclear that exactness of (6.1) at $H^1(G,\mathbb{F}_p)$ should imply exactness at $H^2(G,\mathbb{F}_p)$.

6.2 Triple Massey vanishing

In this subsection, let us suppose that p is an odd prime. The following theorem gives a new proof of the vanishing of triple Massey products for absolute Galois groups due to Efrat–Matzri [EfMa] and Mináč–Tân [MT3]. Both proofs used that the absolute Galois groups of a field containing a primitive pth root of unity is of p-absolute Galois type. We show that the potentially weaker condition of p-cyclic Massey vanishing suffices.

Theorem 6.2.1. *Let G be a profinite group with the p-cyclic Massey vanishing property for an odd prime p. Let $\chi, \psi, \lambda \in H^1(G, \mathbb{F}_p)$ be such that $\chi \cup \lambda = \lambda \cup \psi = 0$. Then there exists a defining system ρ for (χ, λ, ψ) such that the triple Massey product $(\chi, \lambda, \psi)_\rho$ vanishes.*

The case where χ and ψ are linearly dependent follows easily from the p-cyclic Massey vanishing property, so we can and do assume that $(\chi, \psi)\colon G \to \mathbb{F}_p^2$ is surjective, and we let H be the coimage. Let $\Omega = \mathbb{F}_p[H]$ and let $I \subset \Omega$ be the augmentation ideal. Let $h_\chi, h_\psi \in H$ be the dual basis to (χ, ψ), and let $x = [h_\chi] - 1$ and $y = [h_\psi] - 1$ so that $I = x\Omega + y\Omega$.

We want to make maximal use of the fact that G has the cyclic Massey vanishing property. For this, we let C_1, C_2, and C_3 be the coimages of $\alpha_1 = \chi$, $\alpha_2 = \psi$, and $\alpha_3 = \chi + \psi$, respectively. Let $\Omega_i = \mathbb{F}_p[C_i]$, and let $I_i \subset \Omega_i$ be its augmentation ideal. Let $\gamma_i \in C_i$ with $\alpha_i(\gamma_i) = 1$, and let $x_i = [\gamma_i] - 1 \in I_i$. Note that each α_i factors through H, so α_i induces a surjective ring homomorphism $\Omega \to \Omega_i$ that we also call α_i. Then note that

$$(\alpha_1(x), \alpha_1(y)) = (x_1, 0), \quad (\alpha_2(x), \alpha_2(y)) = (0, x_2), \quad (\alpha_3(x), \alpha_3(y)) = (x_3, x_3). \tag{6.2}$$

Now consider the ideal $J = I^3 + xy\Omega$, and let $J_i = \alpha_i(J)$. By (6.2), we have $J_1 = I_1^3$, $J_2 = I_2^3$, and $J_3 = I_3^2$. Hence we have a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & J/I^3 \arrow[r] \arrow[d, "\wr"] & I/I^3 \arrow[r] \arrow[d, hook] & I/J \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & I_3^2/I_3^3 \arrow[r] & \bigoplus_{i=1}^3 I_i/I_i^3 \arrow[r] & \bigoplus_{i=1}^3 I_i/J_i \arrow[r] & 0, \end{tikzcd} \tag{6.3}$$

where the vertical maps are induced by the maps α_i. Note that $J/I^3 = \mathbb{F}_p xy$, so the leftmost vertical arrow is an isomorphism, and $I/J = \mathbb{F}_p x \oplus \mathbb{F}_p x^2 \oplus \mathbb{F}_p y \oplus \mathbb{F}_p y^2$, and the map $I/J \to I_1/I_1^3 \oplus I_2/I_2^3$ is an isomorphism, so the rightmost vertical arrow is split injective.

Lemma 6.2.2. *There is a commutative diagram with exact rows*

$$\begin{tikzcd} H^1(G, I/J) \arrow[r] \arrow[d] & H^2(G, J/I^3) \arrow[r, "\iota"] \arrow[d, "f", "\wr"'] & H^2(G, I/I^3) \arrow[r] \arrow[d, "g"] & H^2(G, I/J) \arrow[d, hook] \\ H^1(G, \mathbb{F}_p) \arrow[r, "\alpha_3 \cup"] & H^2(G, \mathbb{F}_p) \arrow[r, "h"] & \bigoplus_{i=1}^3 H^2(G, I_i/I_i^3) \arrow[r] & \bigoplus_{i=1}^3 H^2(G, I_i/J_i), \end{tikzcd} \tag{6.4}$$

where f is the isomorphism $\xi \cdot xy \mapsto \xi$ and g is the map induced by the center vertical arrow in (6.3).

Proof. The lower sequence in (6.3) is a direct sum of three exact sequences for $i \in \{1, 2, 3\}$, where for $i \in \{1, 2\}$ the sequence has zero as its first term. Taking cohomology of (6.3), we obtain the commutative diagram with exact rows

$$\begin{tikzcd}
H^1(G, I/J) \arrow[r] \arrow[d] & H^2(G, J/I^3) \arrow[r, "\iota"] \arrow[d, "\wr"] & H^2(G, I/I^3) \arrow[r] \arrow[d, "g"'] & H^2(G, I/J) \arrow[d, hook] \\
\bigoplus_{i=1}^3 H^1(G, I_i/J_i) \arrow[r, "\partial_3"] & H^2(G, I_3^2/I_3^3) \arrow[r] & \bigoplus_{i=1}^3 H^2(G, I_i/I_i^3) \arrow[r] & \bigoplus_{i=1}^3 H^2(G, I_i/J_i),
\end{tikzcd} \tag{6.5}$$

where ∂_3 is zero on the first two terms of the summand and the connecting map on the third. Note that the rightmost vertical arrow is injective by the split injectivity of the underlying map on coefficients. To complete the proof, we have to show that $\partial_3(\beta) = \alpha_3 \cup \beta$ for $\beta \in H^1(G, I_3/J_3)$. But the lower sequence in (6.3) for $i = 3$ is isomorphic to

$$0 \to I_3/I_3^2 \to \Omega_3/I_3^2 \to \mathbb{F}_p \to 0$$

via the isomorphism $I_3/J_3 \xrightarrow{\sim} \mathbb{F}_p$ taking the image of x_3 to 1, so this follows from Proposition 2.3.3. □

Proof of Theorem 6.2.1. Consider the commutative diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & J/I^3 \arrow[r] \arrow[d] & \Omega/I^3 \arrow[r] \arrow[d, equal] & \Omega/J \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I/I^3 \arrow[r] & \Omega/I^3 \arrow[r] & \mathbb{F}_p \arrow[r] & 0
\end{tikzcd}$$

and the associated diagram in cohomology

$$\begin{tikzcd}
H^1(G, \Omega/I^3) \arrow[r] \arrow[d, equal] & H^1(G, \Omega/J) \arrow[r, "\partial'"] \arrow[d] & H^2(G, J/I^3) \arrow[r] \arrow[d, "\iota"] & H^2(G, \Omega/I^3) \arrow[d, equal] \\
H^1(G, \Omega/I^3) \arrow[r] & H^1(G, \mathbb{F}_p) \arrow[r, "\partial"] & H^2(G, I/I^3) \arrow[r] & H^2(G, \Omega/I^3),
\end{tikzcd} \tag{6.6}$$

where ι is as in (6.4).

Now let $\lambda \in H^1(G, \mathbb{F}_p)$ be as in the statement of the theorem and consider the element $\partial(\lambda) \in H^2(G, I/I^3)$. Then $g(\partial(\lambda)) \in \bigoplus_{i=1}^3 H^2(G, I_i/I_i^3)$ is the obstruction to lifting λ to $H^1(G, \Omega/I_i^3)$ for all $i \in \{1, 2, 3\}$, and this vanishes by the p-cyclic Massey vanishing property. Hence $g(\partial(\lambda)) = 0$.

By Lemma 6.2.2 and the injectivity of the rightmost vertical arrow in (6.4), this implies that $\partial(\lambda)$ is in the image of ι. By the commutativity of (6.6), there is then a lift $\tilde{\lambda} \in H^1(G, \Omega/J)$ of λ. Using Corollary 4.4.2, we see that $\tilde{\lambda}$ determines a proper defining system ρ_{xy} for (χ, λ, ψ) such that $\partial'(\tilde{\lambda}) = (\chi, \lambda, \psi)_{\rho_{xy}} \cdot xy$.

By Lemma 6.2.2, we have

$$hf(\partial'(\tilde{\lambda})) = g\iota(\partial'(\tilde{\lambda})) = g(\partial(\lambda)) = 0,$$

so $f(\partial'(\tilde{\lambda})) \in \ker(h) = \operatorname{im}(\alpha_3 \cup)$. Hence we have

$$f(\partial'(\tilde{\lambda})) = (\chi, \lambda, \psi)_{\rho_{xy}} = \alpha_3 \cup \nu = \chi \cup \nu - \nu \cup \psi \tag{6.7}$$

in $H^2(G, \mathbb{F}_p)$, for some $\nu \in H^1(G, \mathbb{F}_p)$. In particular, we have that

$$(\chi, \lambda, \psi)_{\rho_{xy}} \in \operatorname{im}(\chi \cup) + \operatorname{im}(\cup \psi),$$

which implies that there is a defining system ρ such that $(\chi, \lambda, \psi)_\rho = 0$. $\square$

The reader may note that in Theorem 6.2.1, we used something weaker than p-cyclic Massey vanishing. Namely, the actual condition employed is that for any character $\chi\colon G \to \mathbb{F}_p$, the sequence

$$H^1(G, \mathbb{F}_p[H_\chi]/I_\chi^3) \to H^1(G, \mathbb{F}_p) \xrightarrow{\chi \cup} H^2(G, \mathbb{F}_p) \tag{6.8}$$

is exact, where $H_\chi = G/\ker(\chi)$ and I_χ is the augmentation ideal in $\mathbb{F}_p[H_\chi]$. This is equivalent to the statement that if $\chi \cup \lambda = 0$ for some $\lambda \in H^1(G, \mathbb{F}_p)$, then (χ, χ, λ) is zero for some proper defining system.

Remark 6.2.3. In [Ma, Corollary 3.5], Matzri proved that Massey triple vanishing follows from defined Massey products of the form (χ, λ, χ) containing zero. The proof exploits the exactness of (6.1) at $H^2(G, \mathbb{F}_p)$ to obtain this vanishing. From our perspective, the vanishing of these Massey products follows directly from the exactness of (6.8).

Remark 6.2.4. The proof of Theorem 6.2.1 does not show that G has the "bicyclic Massey vanishing property" that any $\lambda \in H^1(G, \mathbb{F}_p)$ that lifts to $H^1(G, \Omega/I^2)$ lifts further to $H^1(G, \Omega/I^3)$. Equivalently, this condition can be formulated as saying that if $\chi \cup \lambda = \lambda \cup \psi = 0$, then $\partial(\lambda) = 0$. One can show that this is equivalent to showing that there exists $\nu \in H^1(G, \mathbb{F}_p)$ satisfying (6.7) that lies in the subgroup

$$\ker(\chi \cup) + \ker(\psi \cup) + \ker((\chi + \psi) \cup).$$

A Two lemmas from homological algebra

We provide a proof of the following simple lemma from homological algebra for the reader's convenience.

Lemma A.0.1. *Let $\mathcal{Q}$, $\mathcal{R}$, and $\mathcal{S}$ be abelian categories such that $\mathcal{Q}$ and $\mathcal{R}$ have enough projectives, and let $F\colon \mathcal{R} \to \mathcal{S}$ and $F'\colon \mathcal{Q} \to \mathcal{R}$ be right exact functors such that F' sends projective objects to F-acyclic objects. Let*

$$0 \to A \to B \to C \to 0$$

be an exact sequence in $\mathcal{Q}$ such that

$$0 \to F'(A) \to F'(B) \to F'(C) \to 0$$

is exact. For each $j \geq 0$, we have commutative diagrams

$$\begin{array}{ccc} L_{j+1}(F \circ F')(C) & \longrightarrow & L_j(F \circ F')(A) \\ \downarrow & & \downarrow \\ L_{j+1}F(F'(C)) & \longrightarrow & L_jF(F'(A)), \end{array}$$

in which the vertical arrows are edge maps in the Grothendieck spectral sequence attached to the composition $F \circ F'$ and the horizontal maps are connecting morphisms, where L_i denotes the ith left derived functor.

Proof. Let X denote any of A, B, and C. We may choose projection resolutions $P_\cdot^X$ of X with each term of

$$0 \to F'(P_\cdot^A) \to F'(P_\cdot^B) \to F'(P_\cdot^C) \to 0$$

split exact. Then we may choose first quadrant Cartan-Eilenberg resolutions $Q_{\cdot,\cdot}^X$ of the $F'(P_\cdot^X)$ fitting in split exact sequences

$$0 \to Q_{j,k}^A \to Q_{j,k}^B \to Q_{j,k}^C \to 0$$

so that, in particular, we have exact sequences

$$0 \to H_k(Q_{j,\cdot}^A) \to H_k(Q_{j,\cdot}^B) \to H_k(Q_{j,\cdot}^C) \to 0,$$

and the complexes $H_k(Q_{\cdot,\cdot}^X) \to H_k(F'(P_\cdot^X))$ are projective resolutions. Note that

$$H_j(F(H_k(Q_{\cdot,\cdot}^X))) = L_jF(L_kF'(X)),$$

and we have canonical isomorphisms

$$H_j(F(\operatorname{Tot} Q_{\cdot,\cdot}^X)) \xrightarrow{\sim} H_j(F \circ F'(P_\cdot^X)) = L_j(F \circ F')(X),$$

the first isomorphism as the terms of $F'(P_\cdot^X)$ are F-acyclic. The diagram in question is then simply

$$\begin{tikzcd}
H_{j+1}(F(\operatorname{Tot} Q^C_{\cdot,\cdot})) \arrow[r] \arrow[d] & H_j(F(\operatorname{Tot} Q^A_{\cdot,\cdot})) \arrow[d] \\
H_{j+1}(F(H_0(Q^C_{\cdot,\cdot}))) \arrow[r] & H_j(F(H_0(Q^A_{\cdot,\cdot}))),
\end{tikzcd}$$

the horizontal arrows being the connecting homomorphisms and the vertical arising from the augmentation maps on the total complexes. □

The following lemma is rather elementary but also useful to us.

Lemma A.0.2. *Let $\mathcal{R}$ and $\mathcal{S}$ be abelian categories such that $\mathcal{R}$ has enough projectives. Let $F\colon \mathcal{R} \to \mathcal{S}$ be a left exact functor. Suppose that $G\colon \mathcal{R} \to \mathcal{S}$ is a functor such that the pair (F, G) extends to a functor from short exact sequences $0 \to A \to B \to C \to 0$ in $\mathcal{R}$ to exact sequences*

$$G(A) \to G(B) \to G(C) \xrightarrow{\delta} F(A) \to F(B) \to F(C) \to 0.$$

Then there is a natural transformation $G \rightsquigarrow L_1F$ such that the resulting diagrams

$$\begin{tikzcd}
G(C) \arrow[d] \arrow[dr, "\delta"] & \\
L_1F(C) \arrow[r, "\partial"] & F(A),
\end{tikzcd}$$

are commutative for the usual connecting homomorphisms ∂ and such that $G(A) \to L_1F(A)$ is an epimorphism for all objects A of $\mathcal{R}$.

Proof. Put any object A of $\mathcal{R}$ in an exact sequence

$$0 \to K \to P \to A \to 0$$

in $\mathcal{R}$, where P is a projective object. We then have a commutative diagram

$$\begin{tikzcd}
G(P) \arrow[r] & G(A) \arrow[r] \arrow[d] & F(K) \arrow[r] \arrow[d, equal] & F(P) \arrow[d, equal] \\
0 \arrow[r] & L_1F(A) \arrow[r] & F(K) \arrow[r] & F(P),
\end{tikzcd}$$

with exact rows, where the vertical morphism is unique making the diagram commute. That this gives a natural transformation is standard, and the fact that the morphisms are epimorphisms follows from the five lemma. □

References

[BeCh] J. Bellaïche and G. Chenevier, Families of Galois representations and Selmer groups, *Astérisque* **324**, Soc. Math. France, Paris, 2009.

[EfMa] I. Efrat and E. Matzri, Triple Massey products and absolute Galois groups, *J. Eur. Math. Soc.* **19** (2017), 3629–3640.

[FuKa] T. Fukaya and K. Kato, A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory, Proceedings of the St. Petersburg Mathematical Society, Vol. XII, 1–85, *Amer. Math. Soc. Transl. Ser. 2* **219**, Amer. Math. Soc., Providence, 2006.

[GMT] P. Guillot, J. Mináč and A. Topaz, Four-fold Massey products in Galois cohomology, *Compos. Math.* **154** (2018), 1921–1959.

[HrWt] Y. Harpaz and O. Wittenberg, The Massey vanishing conjecture for number fields, preprint, arXiv:1904.06512.

[HsWe] C. Haesemeyer and C. Weibel, The norm residue isomorphism in motivic cohomology, *Ann. of Math. Stud.* **200**, Princeton Univ. Press, Princeton, 2019.

[HoWi] M. Hopkins and K. Wickelgren, Splitting varieties for triple Massey products, *J. Pure Appl. Algebra* **219** (2015), 1304–1319.

[LiSh] M. F. Lim and R. Sharifi, Nekovář duality over p-adic Lie extensions of global fields, *Doc. Math.* **18** (2013), 621–678.

[Ma] E. Matzri, Triple Massey products of weight $(1, n, 1)$ in Galois cohomology, *J. Algebra* **499** (2018), 272–280.

[McS] W. McCallum and R. Sharifi, A cup product in the Galois cohomology of number fields, *Duke Math. J.* 120 (2003), no. 2, 269–310.

[MT1] J. Mináč and N. Tân, The kernel unipotent conjecture and the vanishing of Massey products for odd rigid fields, *Adv. Math.* **273** (2015), 242–270.

[MT2] J. Mináč and N. Tân, Triple Massey products over global fields, *Doc. Math.* **20** (2015), 1467–1480.

[MT3] J. Mináč and N. Tân, Triple Massey products vanish over all fields, *J. London Math. Soc.* **94** (2016), 909–932.

[MT4] J. Mináč and N. Tân, Triple Massey products and Galois theory, *J. Eur. Math. Soc.* **19** (2017), 76–112.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, Second Edition, *Grundlehren Math. Wiss.* **323**, Springer, 2008.

[Se] J-P. Serre, Local Fields, *Grad. Texts in Math.* **67**, Springer, New York, 1979.

[Sh1] R. Sharifi, Twisted Heisenberg extensions and local conductors, Ph.D. thesis, The University of Chicago, 1999.

[Sh2] R. Sharifi, Massey products and ideal class groups, *J. reine angew. Math.* **603** (2007), 1–33.

[Sh3] R. Sharifi, Iwasawa theory and the Eisenstein ideal, *Duke Math. J.* **137** (2007), 63–101.

[Sh4] R. Sharifi, Reciprocity maps with restricted ramification, preprint.

[Ta] J. Tate, Some duality theorems, Appendix I of J-P. Serre, Galois cohomology, Springer-Verlag, Berlin, 1997.

[Vo] V. Voevodsky, On motivic cohomology with $\mathbf{Z}/l$-coefficients, *Ann. of Math.* **174** (2001), 401–438.

Yeuk Hay Joshua Lam
Institut des Hautes Études Scientifiques
35 Route de Chartres
Bures-sur-Yvette 91440
France
ylam@ihes.fr

Preston Wake
Department of Mathematics
Michigan State University
619 Red Cedar Road
East Lansing, MI 48824
wakepres@msu.edu
https://sites.google.com/msu.edu/prestonwake

Yuan Liu
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109
yyyliu@umich.edu
https://sites.google.com/view/yuanliu-homepage

Jiuya Wang
Department of Mathematics
University of Georgia
Boyd Graduate Studies Research Center
Athens, GA 30602
jiuya.wang@uga.edu
https://wangjiuya.github.io/

Romyar Sharifi
Department of Mathematics
University of California, Los Angeles
520 Portola Plaza
Los Angeles, CA 90095
sharifi@math.ucla.edu
https://math.ucla.edu/~sharifi