IWASAWA λ INVARIANT AND MASSEY PRODUCT

PEIKAI QI

Abstract. We compute the Iwasawa λ-invariant in terms of Massey products in Galois cohomology with restricted ramification. Applied to imaginary quadratic fields and cyclotomic fields, this approach yields a new proof and a generalization of results by Gold [Gol74] and McCallum–Sharifi [MS03]. The main tool is the generalized Bockstein map introduced by Lam, Liu, Sharifi, Wake, and Wang [Lam+23].

1. Introduction

1.1. **Background.** Let K be a number field and $K \subset K_1 \subset K_2 \subset \cdots \subset K_l \subset \cdots \subset K_\infty$ be a $\mathbb{Z}_p$-extension of K. Define $X = \varprojlim \mathrm{Cl}(K_l)[p^\infty]$, where $\mathrm{Cl}(K_l)[p^\infty]$ denotes the p-primary part of the class group of K_l. Let μ and λ denote the Iwasawa invariants of X. Our goal is to relate the value of λ to the vanishing of Massey products, under the assumption that $\mu = 0$.

Massey products in Galois cohomology were introduced in number theory to study the structure of Galois groups. We will give their definition in Section 2.2. One may view Massey products as a generalization of cup products in cohomology; for instance, the cup product is a 2-fold Massey product.

The idea of using Massey products to study Iwasawa theory first appeared in Sharifi's work [Sha07]. McCallum and Sharifi proved that, under certain assumptions, Iwasawa invariant $\lambda \geq 2$ if and only if a specific cup product vanishes for cyclotomic fields [MS03, Proposition 4.2]. Similarly, Gold's criterion [Gol74] can be reinterpreted in terms of group cohomology: it also states that, under suitable assumptions, Iwasawa invariant $\lambda \geq 2$ if and only if a certain cup product vanishes for imaginary quadratic fields. Although these two results are proved by completely different methods, they share the same underlying form. Our goal is to uncover the deeper reason behind this phenomenon.

Our main theorem unifies these two results and, when specialized to these cases, provides their generalization. Roughly speaking, we prove that under suitable assumptions, if $\lambda \geq n-1$, then $\lambda \geq n$ if and only if a certain Massey product vanishes.

For readers familiar with Massey products, we highlight some differences that should be noted. In the Massey products vanishing conjecture of Ján Mináč and Nguyễn Duy Tân [MT17], the phrase "Massey products vanish" means that zero is in the set of the Massey products relative to *all* defining systems. In contrast,

Date: October 18, 2026.

Key words and phrases. Massey product, Iwasawa theory, Galois cohomology.

This work is part of the author's thesis. I would like to thank my advisor, Preston Wake, for his guidance in learning Iwasawa theory. He suggested this question and encouraged me to pursue the research. I am also grateful to the Department of Mathematics at Michigan State University for its support.

in this paper, "Massey products vanish" means that the Massey product vanishes relative to a particular defining system, which we call the *proper defining system*. Furthermore, Mináč and Tân work with Massey products in absolute Galois groups, whereas we study Massey products in Galois groups with restricted ramification.

1.2. **Strategy and Notation.** The strategy of this project is divided into four steps.

(1) *The Iwasawa invariants λ and λ_{cs}.*
Let S be the set of primes of K lying above p, and set

$$X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty],$$

where $\mathrm{Cl}_S(K_l)[p^\infty]$ denotes the p-primary part of the S-class group of K_l. Let μ_{cs} and λ_{cs} be the Iwasawa invariants associated with the Iwasawa module X_{cs}.

Define D_l to be the subgroup of $\mathrm{Cl}(K_l)[p^\infty]$ generated by the primes in S. Then we have the exact sequence

$$0 \longrightarrow \varprojlim D_l \longrightarrow X \longrightarrow X_{cs} \longrightarrow 0.$$

Thus, λ can be related to λ_{cs} once $\varprojlim D_l$ is understood.

(2) *The size of $H^2(G_{K_l,S}, \mu_p)$ and λ_{cs}.*
Let K_S be the maximal extension of K unramified outside S, and set $G_{K_l,S} = \mathrm{Gal}(K_S/K_l)$. By the Kummer theory, we have the exact sequence

$$0 \longrightarrow \mathrm{Cl}_S(K_l)/p \longrightarrow H^2(G_{K_l,S}, \mu_p) \longrightarrow \mathrm{Br}(\mathcal{O}_{K_l}[1/p])[p] \longrightarrow 0.$$

One can refer to the beginning of Section 4 for the definition of $Br(\mathcal{O}_K[1/p])$. To obtain information about λ_{cs}, it suffices to understand the size of $\mathrm{Cl}_S(K_l)[p^\infty]$. Hence, this requires information about the size of $H^2(G_{K_l,S}, \mu_p)$.

(3) *The generalized Bockstein map and the size of $H^2(G_{K_l,S}, \mu_p)$.*
By Lam, Liu, Sharifi, Wake, and Wang [Lam+23, Theorem 2.2.4], we have the following formula:

$$\frac{I^n H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p)}{I^{n+1} H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p)} \cong \frac{H^2(G_{K,S}, \mu_p)}{\mathrm{Im}\, \Psi^{(n)}},$$

where I is the augmentation ideal of $\mathbb{F}_p[[\mathrm{Gal}(K_l/K)]]$, and

$$\Psi^{(n)} : H^1(G_{K,S}, \mu_p \otimes I^n/I^{n+1}) \longrightarrow H^2(G_{K,S}, \mu_p)$$

is the generalized Bockstein map defined in [Lam+23].

This gives rise to a filtration

$$H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \supset I H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \supset I^2 H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \supset \cdots \supset I^n H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \supset \cdots.$$

Once the sizes of $H^2(G_{K,S}, \mu_p)$ and $\mathrm{Im}\, \Psi^{(n)}$ are known, this filtration determines the size of $H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p)$.

(4) *The generalized Bockstein map and Massey products.*
In Lam, Liu, Sharifi, Wake, and Wang [Lam+23], it is shown that, under certain circumstances, the image of the generalized Bockstein map, $\mathrm{Im}\, \Psi^{(n)}$, is spanned by specific n-fold Massey products.

1.3. **Main Theorem and Corollaries.** As noted above, our strategy does not rely on the Iwasawa Main Conjecture. The Iwasawa λ-invariant we compute is the algebraic Iwasawa λ-invariant. Following this strategy, one of our main theorems can be stated as follows:

Theorem 1. *Let $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$ be a $\mathbb{Z}_p$-extension of K, and let S be the set of primes of K lying above p. Assume that all primes in S are totally ramified in K_∞/K. Put $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty]$, and let μ_{cs} and λ_{cs} denote the Iwasawa invariants of X_{cs}. Assume that X_{cs} has no finite $\Lambda := \mathbb{Z}_p[[T]]$-submodule and that $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$.*

Then $\mu_{cs} = 0$ if and only if there exists an integer k such that $\Psi^{(k)} \neq 0$. Moreover, if $\mu_{cs} = 0$, then $\lambda_{cs} = \min\{n \mid \Psi^{(n)} \neq 0\} - \#S + 1$.

Remark 1. The paper is part of the author's thesis, and the results of the paper have been partially generalized by the preprint [RS25]. Here, we impose the condition $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$ to simplify the statement and make it easy for us to develop a numerical criterion. In [RS25], they do not require $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$. Hence, they also do not develop the numerical criterion. See the remark 15 for a detailed discussion on the condition $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$.

When a Galois group Δ acts on the Iwasawa module $X = \varprojlim \mathrm{Cl}(K_n)$, this action induces a decomposition $X = \bigoplus_i \varepsilon_i X$. The techniques used to prove Theorem 1 can be applied in the same way to compute the Iwasawa invariants λ_i of $\varepsilon_i X$ (see Theorem 16).

We apply Theorem 1 in several cases throughout the paper. In the introduction, we list two examples corresponding to the settings of the results of Gold [Gol74] and McCallum–Sharifi [MS03].

Theorem 2. *Let K be an imaginary quadratic field, and assume that p does not divide the class number h_K and that p splits in K as $p\mathcal{O}_K = \mathfrak{p}_0\tilde{\mathfrak{p}}_0$. In the cyclotomic $\mathbb{Z}_p$-extension of K, the λ-invariant can be determined in terms of Massey products as follows:*

Let $n \geq 2$, and suppose that $\lambda \geq n-1$. Then $\lambda \geq n$ if and only if the n-fold Massey product

$$(\underbrace{\chi, \chi, \ldots, \chi}_{n-1 \text{ copies}}, \alpha)$$

vanishes with respect to a proper defining system.

Here χ is the character $\chi : G_{K,S} \longrightarrow \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, and α is the generator of the principal ideal $\mathfrak{p}_0^{h_K}$.

Remark 2. Equivalently,

$$\lambda = \min\Big\{\, n \;\Big|\; \text{the } n\text{-fold Massey product } (\chi, \chi, \ldots, \chi, \alpha) \text{ is nonzero} \Big\}.$$

Remark 3. It is known that $\lambda \geq 1$ in this case. Gold's criterion [Gol74] states that

$$\lambda \geq 2 \iff \alpha^{p-1} \equiv 1 \pmod{\mathfrak{p}_0^2}.$$

Further calculations show that

$$\alpha^{p-1} \equiv 1 \pmod{\mathfrak{p}_0^2} \iff \log_p(\alpha) \equiv 0 \pmod{p^2} \iff \chi \cup \alpha = 0,$$

where $\log_p$ denotes the p-adic logarithm. Thus, the theorem may be regarded as both a new proof and a generalization of Gold's result.

Theorem 3. *Let $K = \mathbb{Q}(\mu_p)$, and let $\omega : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \mathbb{Z}_p$ be the Teichmüller character. Then the p-primary part of the class group admits the decomposition*

$$\mathrm{Cl}(K)[p^\infty] \;=\; \bigoplus_{i=0}^{p-2} \varepsilon_i \mathrm{Cl}(K)[p^\infty],$$

where

$$\varepsilon_i \;=\; \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\, \sigma_a^{-1} \;\in\; \mathbb{Z}_p\big[\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})\big].$$

Let λ_i denote the Iwasawa λ-invariant corresponding to $\varepsilon_i \mathrm{Cl}(K_l)[p^\infty]$.

Fix $i \in \{3, 5, \ldots, p-2\}$ and assume that $\varepsilon_i \mathrm{Cl}(K)[p^\infty]$ is cyclic. If $\varepsilon_i \mathrm{Cl}(K)[p] \cong \mathbb{F}_p$, we can define α_i as a lift of a generator of $\varepsilon_i \mathrm{Cl}(K)[p]$ by the map $\varepsilon_i H^1(G_{K,S}, \mu_p) \to \varepsilon_i \mathrm{Cl}(K)[p]$.

Let $n \geq 2$. If $\lambda_i \geq n-1$, then

$$\lambda_i \geq n \quad \Longleftrightarrow \quad \varepsilon_i(\underbrace{\chi, \chi, \ldots, \chi}_{n-1 \text{ copies}}, \alpha_i) = 0$$

for the n-fold Massey product with respect to a proper defining system.

Remark 4. The assumption $\varepsilon_i \mathrm{Cl}(K)[p] = \mathbb{F}_p$ implies that $\lambda_i \geq 1$ in this case. Note that $\varepsilon_i \mathrm{Cl}(K)[p^\infty]$ is cyclic if Vandiver's conjecture holds. The theorem further shows that

$$\lambda_i \geq 2 \iff \varepsilon_i(\chi, \alpha_i) = 0 \iff \chi \cup \alpha_i = 0.$$

Proposition 4.2 of McCallum–Sharifi [MS03] establishes a similar criterion, namely $\lambda_i \geq 2 \iff \chi \cup \alpha_i = 0$. Thus, the theorem may be viewed as a generalization of their result.

1.4. **Structure of the paper.** In Section 2, we discuss the generalized Bockstein map introduced by Lam–Liu–Sharifi–Wake–Wang [Lam+23], and recall its relation to Massey products. We also prove that the generalized Bockstein map preserves group actions. In Section 3, we establish a formula for determining the size of the second cohomology group using the generalized Bockstein map. In Section 4, we apply this formula to number theory in order to prove the main theorem. We then present four cases where the theorem yields interesting results. The first three cases concern cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields, while the final case concerns the cyclotomic $\mathbb{Z}_p$-extension of a cyclotomic field. In the first case, we also develop a numerical criterion for determining the λ-invariant, which spans about ten pages. For a first reading, the reader may wish to skip this numerical criterion.

2. Generalized Bockstein map and Massey product

2.1. **Generalized Bockstein map.** In this section, we recall the definition and properties of the generalized Bockstein map from [Lam+23].

Recall that a profinite group G is p-cohomologically finite if G has finite p-cohomological dimension and $H^i(G, M)$ is finite for every finite $\mathbb{Z}_p[G]$-module M and $i \geq 0$. As in the setup of [Lam+23], we always assume the profinite group G is p-cohomologically finite and of p-cohomological dimension d, and let N be a closed normal subgroup such that G/N is a finitely generated pro-p group. In our paper, we always take $G/N \cong \mathbb{Z}_p$ or $G/N \cong \mathbb{Z}/p^l\mathbb{Z}$, but the definition of the generalized Bockstein map works more generally in [Lam+23].

Let $\Omega = \mathbb{F}_p[[G/N]]$ denote the completed group algebra, which is naturally a G-module. Let σ be a topological generator of G/N, and let $I = \langle \sigma - 1 \rangle$ denote the augmentation ideal in Ω. For $0 \leq n < \#(G/N)$, we have the following short exact sequence of G-modules:

$$0 \longrightarrow I^n/I^{n+1} \longrightarrow \Omega/I^{n+1} \longrightarrow \Omega/I^n \longrightarrow 0.$$

After tensoring with a finite $\mathbb{F}_p[G]$-module T, the sequence remains exact since all the modules above are $\mathbb{F}_p$-modules:

$$0 \longrightarrow I^n/I^{n+1} \otimes_{\mathbb{F}_p} T \longrightarrow \Omega/I^{n+1} \otimes_{\mathbb{F}_p} T \longrightarrow \Omega/I^n \otimes_{\mathbb{F}_p} T \longrightarrow 0.$$

For $0 \leq n < \#(G/N)$, we define the *generalized Bockstein map* $\Psi^{(n)}$ to be the connecting homomorphism in cohomology:

$$\Psi^{(n)} \colon H^{d-1}(G,\, \Omega/I^n \otimes T) \longrightarrow H^d\big(G,\, I^n/I^{n+1} \otimes T\big)\,.$$

Since I^n/I^{n+1} is a trivial G-module, we have a natural isomorphism

$$H^d(G, I^n/I^{n+1} \otimes T) \;\cong\; H^d(G,T) \otimes I^n/I^{n+1}.$$

We set $\Psi^{(0)} = 0$. Recall that the Iwasawa cohomology groups are defined by

$$H^r_{\mathrm{Iw}}(N,T) \;=\; \varprojlim_{N \leq U \trianglelefteq^\circ G} H^r(U,T),$$

where the inverse limit is taken with respect to corestriction maps and U runs over all open normal subgroups of G containing N. In particular, if G/N is finite, then $H^i_{\mathrm{Iw}}(N,T) \;=\; H^i(N,T)$. In the work of Lam–Liu–Sharifi–Wake–Wang [Lam+23], the following fundamental result was established:

Theorem 4 (Theorem A in LLSWW[Lam+23])**.** *For each $0 \leq n < \#(G/N)$, there is a canonical isomorphism of $\mathbb{F}_p$-modules*

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

where d denotes the p-cohomological dimension of G.

Remark 5. Sharifi [Sha22] also applies Theorem A in LLSWW[Lam+23] to number theory, where he gets a six-term exact sequence.

For the remainder of this subsection, we establish an equivalent formulation of the isomorphism above. Specifically, we decompose the cohomology group into a direct sum of eigenspaces with respect to a certain group action. On each eigenspace, the same type of isomorphism continues to hold. However, verifying that the generalized Bockstein map $\Psi^{(n)}$ is compatible with this group action is somewhat tedious. Readers who wish to avoid these technical details may proceed directly to Remark 8.

We always take continuous cochains without mentioning it in the paper.

Lemma 5. *Suppose $G/N \cong \mathbb{Z}_p$, and let U_l be the unique open normal subgroup of G containing N such that $G/U_l \cong \mathbb{Z}/p^l\mathbb{Z}$. Let T be a finite $\mathbb{F}_p[G]$-module. Then*

$$\mathrm{CoInd}_{U_l}^G T := \mathrm{Hom}_{\mathbb{Z}[U_l]}(\mathbb{Z}[G], T) \;\cong\; \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$$

as $\mathbb{F}_p[G]$-modules. By Shapiro's lemma, we obtain an isomorphism

$$H^r(U_l, T) \;\cong\; H^r\big(G,\, \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T\big).$$

Proof. Write $G = \bigsqcup_{i=1}^{p^l} U_l\sigma_i$, where $\{\sigma_i\}$ is a set of right coset representatives of U_l in G. Define a homomorphism

$$\alpha : \mathrm{Hom}_{\mathbb{Z}[U_l]}(\mathbb{Z}[G], T) \longrightarrow \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$$

by

$$\alpha(\phi) \;=\; \sum_{i=1}^{p^l} \bar{\sigma}_i^{-1} \otimes \sigma_i^{-1}\phi(\sigma_i),$$

where $\bar{\sigma}_i$ denotes the image of σ_i in G/U_l.

We first check that the map α is independent of coset representatives. Suppose we take another set of right coset representatives $h_i\sigma_i$ with $h_i \in U_l$. Then

$$\sum_{i=1}^{p^l} \bar{\sigma}_i^{-1}\bar{h}_i^{-1} \otimes \sigma_i^{-1}h_i^{-1}\phi(h_i\sigma_i) \;=\; \sum_{i=1}^{p^l} \bar{\sigma}_i^{-1} \otimes \sigma_i^{-1}\phi(\sigma_i),$$

since $\phi(h_i\sigma_i) = h_i\phi(\sigma_i)$.

Then we check the map α preserves the G-action. Recall that the action of $g \in G$ on $\phi \in \mathrm{Hom}_{\mathbb{Z}[U_l]}(\mathbb{Z}[G], T)$ is given by

$$(g\phi)(x) = \phi(xg),$$

while the action of $g \in G$ on $\sum_{i=1}^{p^l} \bar{\sigma}_i \otimes t_i \in \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$ is

$$g\Big(\sum_{i=1}^{p^l} \bar{\sigma}_i \otimes t_i\Big) \;=\; \sum_{i=1}^{p^l} \bar{g}\bar{\sigma}_i \otimes gt_i.$$

Then

$$\alpha(g\phi) \;=\; \sum_{i=1}^{p^l} \bar{\sigma}_i^{-1} \otimes \sigma_i^{-1}(g\phi)(\sigma_i) \;=\; \sum_{i=1}^{p^l} \bar{\sigma}_i^{-1} \otimes \sigma_i^{-1}\phi(\sigma_i g).$$

Write $\sigma_i g = h_i\sigma_{\delta(i)}$ for some $h_i \in U_l$, where δ is a permutation of $\{1, \ldots, p^l\}$. Then

$$\sigma_i^{-1}\phi(\sigma_i g) = \sigma_i^{-1}\phi(h_i\sigma_{\delta(i)}) = \sigma_i^{-1}h_i\phi(\sigma_{\delta(i)}) = g\,\sigma_{\delta(i)}^{-1}\phi(\sigma_{\delta(i)}),$$

and moreover

$$\bar{\sigma}_i^{-1} = \big(\overline{h_i\sigma_{\delta(i)}g^{-1}}\big)^{-1} = \bar{g}\,\bar{\sigma}_{\delta(i)}^{-1}.$$

Hence

$$\alpha(g\phi) = \sum_{i=1}^{p^l} \bar{g}\,\bar{\sigma}_{\delta(i)}^{-1} \otimes g\sigma_{\delta(i)}^{-1}\phi(\sigma_{\delta(i)}) = \sum_{i=1}^{p^l} \bar{g}\,\bar{\sigma}_i^{-1} \otimes g\sigma_i^{-1}\phi(\sigma_i),$$

since δ is a permutation. Thus α is G-equivariant.

Finally, it is straightforward to check that α is bijective; one can also write down its inverse explicitly.

Therefore α is an $\mathbb{F}_p[G]$-isomorphism, and hence, $\mathrm{CoInd}_{U_l}^G T \;\cong\; \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$ as $\mathbb{F}_p[G]$-modules. □

We have computed $H^r(U_l, T)$. We now turn to the computation of $H^r_{\mathrm{Iw}}(N, T)$. For this we need the following result of Tate [Tat76].

Proposition 1. *Let $i > 0$, and let $M = \varprojlim M_l$ where each M_l is a finite discrete G-module. If $H^{i-1}(G, M_l)$ is finite for every l, then*

$$H^i(G, M) \;=\; \varprojlim_l H^i(G, M_l).$$

Lemma 6. *Let $G/N \cong \mathbb{Z}_p$, and let U_l be the unique open normal subgroup of G containing N such that $G/U_l \cong \mathbb{Z}/p^l\mathbb{Z}$. Let T be a finite $\mathbb{F}_p[G]$-module. Then*

$$H^r_{\mathrm{Iw}}(N,T) \;\cong\; H^r\big(G,\, \mathbb{F}_p[[G/N]] \otimes_{\mathbb{F}_p} T\big)\,.$$

Proof. By lemma 5,

$$\begin{aligned} H^r_{\mathrm{Iw}}(N,T) &= \varprojlim_{N\le U_l \trianglelefteq^\circ G} H^r(U_l,T) \\ &= \varprojlim_{N\le U_l \trianglelefteq^\circ G} H^r(G, \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T) \\ &= H^r(G, \varprojlim_{N\le U_l \trianglelefteq^\circ G} \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T) \\ &= H^r(G, \mathbb{F}_p[[G/N]] \otimes_{\mathbb{F}_p} T). \end{aligned}$$

To prove the third equality, it suffices to verify the hypotheses of Proposition 1. First, note that $\mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$ is a finite module. Second, by [Lam+23, Proposition 2.2.2], we know that $H^i(U_l,T) \;\cong\; H^i\big(G,\, \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T\big)$ is a finitely generated $\mathbb{F}_p[G/U_l]$-module for all $i \ge 0$. Since $\mathbb{F}_p[G/U_l]$ is finite, it follows that $H^i\big(G,\, \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T\big)$ is finite as well.

For the last equality, observe that T is a finite-dimensional vector space over $\mathbb{F}_p$. We have

$$\varprojlim_{l}\big(\mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T\big) \;\cong\; \mathbb{F}_p[[G/N]] \otimes_{\mathbb{F}_p} T$$

as $\mathbb{F}_p$-modules. Moreover, this isomorphism is compatible with the G-action, and thus it is an isomorphism of $\mathbb{F}_p[G]$-modules.

□

Remark 6. We have

$$\varprojlim_{l} \mathrm{CoInd}_{U_l}^G T \;\coloneqq\; \varprojlim_{l} \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T) \;\cong\; \mathbb{F}_p[[G/N]] \otimes_{\mathbb{F}_p} T.$$

However, in general $\mathrm{CoInd}_N^G T \;\coloneqq\; \mathrm{Hom}_{\mathbb{Z}N}(\mathbb{Z}G, T)$ is not isomorphic to $\varprojlim_l \mathrm{CoInd}_{U_l}^G T$. This is one reason why we separate the proofs of Lemma 5 and Lemma 6. For the same reason, we often write our induced module in the form $\Omega \otimes T$ rather than $\mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T)$.

Let $\mathscr{G}$ be a group containing G and N as normal subgroups such that $\mathscr{G}/G = \Delta$ is abelian and $\mathscr{G}/N$ is also abelian with $\mathscr{G}/N \;\cong\; \Delta \oplus G/N$, where G/N is a finitely generated pro-p quotient. Let T be an $\mathbb{F}_p[\mathscr{G}]$-module and set $\Omega = \mathbb{F}_p[[G/N]]$. We now define an action of Δ on

$$H^r(G, \Omega \otimes T), \quad H^r\big(G, I^n/I^{n+1} \otimes T\big)\,, \quad H^r(G, \Omega/I^n \otimes T), \quad \text{and} \quad H^r(G,T),$$

and show that the generalized Bockstein map $\Psi^{(n)}$ preserves this action. In this paper, we specialize to the cases $G/N \cong \mathbb{Z}_p$ or $G/N \cong \mathbb{Z}/p^l\mathbb{Z}$. However, the setup applies more broadly.

Theorem 7. *The generalized Bockstein map $\Psi^{(n)}$ is Δ-equivariant.*

Proof. Recall the action of $\tau \in \mathscr{G}$ on an element $\sum_i \bar{\sigma}_i \otimes t_i \in \Omega \otimes T$ is given by

$$\tau\left(\sum_i \bar{\sigma}_i \otimes t_i\right) \;=\; \sum_i \bar{\sigma}_i \otimes \tau t_i.$$

Recall that the action of $g \in G$ on $\Omega \otimes T$ is given by

$$g\left(\sum_i \bar{\sigma}_i \otimes t_i\right) \;=\; \sum_i \overline{g}\,\bar{\sigma}_i \otimes g t_i.$$

These two actions differ when $\tau \in G \subset \mathscr{G}$, but they coincide when $\tau \in N \subset \mathscr{G}$.

For every $\tau \in \mathscr{G}$, we obtain: a group homomorphism

$$\alpha : G \longrightarrow G, \qquad g \longmapsto \tau^{-1} g \tau,$$

and a module homomorphism

$$\beta : \Omega \otimes T \longrightarrow \Omega \otimes T, \qquad \sum_i \bar{\sigma}_i \otimes t_i \longmapsto \tau\left(\sum_i \bar{\sigma}_i \otimes t_i\right),$$

which are also compatible with each other in the following sense.

$$\begin{aligned}
\beta\left(\alpha(g)\Big(\sum_i \bar{\sigma}_i \otimes t_i\Big)\right) &= \beta\left(\sum_i \overline{\tau^{-1} g \tau}\,\bar{\sigma}_i \otimes \tau^{-1} g \tau\, t_i\right) \\
&= \sum_i \overline{\tau^{-1} g \tau}\,\bar{\sigma}_i \otimes \tau\big(\tau^{-1} g \tau\, t_i\big) \\
&= \sum_i \overline{g}\,\bar{\sigma}_i \otimes g(\tau t_i) \\
&= g\left(\beta\left(\sum_i \bar{\sigma}_i \otimes t_i\right)\right).
\end{aligned}$$

By the functoriality of cohomology [Mil20, Chapter 2, p. 66], we obtain a homomorphism $H^r(G, \Omega \otimes T) \longrightarrow H^r(G, \Omega \otimes T)$, which defines an action of $\mathscr{G}$ on $H^r(G, \Omega \otimes T)$.

Note that the actions of $\tau \in \mathscr{G}$ and $g \in G$ on $\Omega \otimes T$ coincide whenever $\tau \in N$. By a standard fact [Mil20, Example 1.27(d), p. 67], the induced action of $\tau \in N \subset \mathscr{G}$ on $H^r(G, \Omega \otimes T)$ is trivial. Consequently, the action of $\mathscr{G}$ on $H^r(G, \Omega \otimes T)$ factors through $\mathscr{G}/N \;\cong\; \Delta \oplus G/N$. In particular, we obtain an action of Δ on $H^r(G, \Omega \otimes T)$ by identifying Δ with a subgroup of $\mathscr{G}/N$.

Similarly, the action of $\mathscr{G}$ on $\Omega/I^n \otimes T$ and $I^n/I^{n+1} \otimes T$ is defined in the same way. These actions are compatible with the short exact sequences. In other words, for every $\tau \in \mathscr{G}$ we have the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I^n/I^{n+1} \otimes T & \longrightarrow & \Omega/I^{n+1} \otimes T & \longrightarrow & \Omega/I^n \otimes T & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} & & \\
0 & \longrightarrow & I^n/I^{n+1} \otimes T & \longrightarrow & \Omega/I^{n+1} \otimes T & \longrightarrow & \Omega/I^n \otimes T & \longrightarrow & 0.
\end{array}$$

Let $\cdots \to \mathbb{Z}G^{\oplus k} \to \mathbb{Z}G^{\oplus k-1} \to \cdots \to \mathbb{Z}G^{\oplus 2} \to \mathbb{Z}G \to \mathbb{Z} \to 0$ be a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module. Then (α, β) defines a homomorphism of complexes

$$\mathrm{Hom}(\mathbb{Z}G^{\oplus k}, \Omega \otimes T) \longrightarrow \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, \Omega \otimes T), \qquad \phi \longmapsto \beta \circ \phi \circ \alpha^k,$$

for each k. This, in turn, induces a homomorphism between two short exact sequences of complexes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, I^n/I^{n+1}\otimes T) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, \Omega/I^{n+1}\otimes T) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, \Omega/I^{n}\otimes T) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, I^n/I^{n+1}\otimes T) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, \Omega/I^{n+1}\otimes T) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}G^{\oplus k}, \Omega/I^{n}\otimes T) & \longrightarrow & 0. \end{array}$$

By the functoriality of cohomology, we obtain a homomorphism between the corresponding long exact sequences:

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^r(G, \Omega/I^{n+1}\otimes T) & \longrightarrow & H^r(G, \Omega/I^{n}\otimes T) & \longrightarrow & H^{r+1}(G, I^n/I^{n+1}\otimes T) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & H^r(G, \Omega/I^{n+1}\otimes T) & \longrightarrow & H^r(G, \Omega/I^{n}\otimes T) & \longrightarrow & H^{r+1}(G, I^n/I^{n+1}\otimes T) & \longrightarrow & \cdots. \end{array}$$

Each column defines an action of $\tau \in \mathscr{G}$, and these actions are compatible with one another. In particular, since the generalized Bockstein map is the connecting morphism, we have

$$\Psi^{(n)}(\tau\phi) \;=\; \tau\,\Psi^{(n)}(\phi) \qquad \text{for all } \phi \in H^{d-1}(G, T\otimes \Omega/I^n).$$

As before, all actions factor through $\mathscr{G}/N$, which induces an action of Δ on the cohomology groups. Therefore, the generalized Bockstein map $\Psi^{(n)}$ is Δ-equivariant. □

Remark 7. By Lemma 5, we have an isomorphism $\mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T) \;\cong\; \mathbb{F}_p[G/U_l]\otimes_{\mathbb{F}_p} T$. Under this identification, the action of $\tau \in \mathscr{G}$ on $\phi \in \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T)$ corresponds to $(\tau\phi)(g) \;=\; \tau\,\phi(\tau^{-1}g\tau)$.

Remark 8. The induced action of Δ on the cohomology groups is a left action.

We now introduce a convenient notation for elements in Ω, which will simplify future calculations. For simplicity, assume $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$, and let σ be a generator of G/N. Set $x = \sigma - 1$, so that $I = \langle \sigma - 1\rangle = \langle x\rangle$, and

$$\Omega = \mathbb{F}_p[[G/N]] \;\cong\; \begin{cases} \mathbb{F}_p[[x]] & \text{if } G/N \cong \mathbb{Z}_p, \\ \mathbb{F}_p[x]/(x^{p^l}) & \text{if } G/N \cong \mathbb{Z}/p^l\mathbb{Z}. \end{cases}$$

Elements in $\Omega\otimes T$ can be written as

$$\sum_i \sigma^i \otimes t_i = \sum_i (1+x)^i \otimes t_i = \sum_i x^i \otimes \psi_i$$

for some $\psi_i \in T$. Let $\chi : G \to G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$ be the canonical projection. Then the action of $g \in G$ on $\Omega\otimes T$ can be expressed as

$$g\left(\sum_i x^i\otimes\psi_i\right) \;=\; \sum_i (1+x)^{\chi(g)}x^i\otimes g\psi_i \;=\; \sum_i x^i \otimes \left(\sum_{k=0}^{i}\binom{\chi(g)}{k} g\psi_{i-k}\right).$$

2.2. **Massey products.** In this section, we recall some basic facts about Massey products, defining systems [LM21; MT17], and proper defining systems [Lam+23]. For further references, see also [Kra66; Dwy75].

We first recall the classical definition of Massey products in group cohomology. Let A be a commutative ring with trivial G-action and the discrete topology. By [NSW08], the complex of inhomogeneous continuous cochains

$$\mathcal{C}^\bullet = \bigoplus_{k\geq 0} \mathcal{C}^k(G, A)$$

forms a differential graded algebra (DGA) over A, equipped with the cup product $\cup$ and the differential

$$d : \mathcal{C}^n \longrightarrow \mathcal{C}^{n+1},$$

satisfying the Leibniz rule

$$d(a \cup b) = (da) \cup b + (-1)^k a \cup (db), \quad a \in \mathcal{C}^k,$$

and $d^2 = 0$. The cohomology groups are then given by

$$H^n(G, A) = \ker d^n / \operatorname{im} d^{n-1}.$$

Let $U_{n+1}(A)$ denote the group of $(n+1) \times (n+1)$ upper triangular matrices with diagonal entries equal to 1, and let $Z(U_{n+1}(A))$ be its center. Explicitly, $Z(U_{n+1}(A))$ consists of matrices with 1 on the diagonal and all entries zero except possibly in the $(1, n+1)$-position. Set $\bar{U}_{n+1}(A) = U_{n+1}(A)/Z(U_{n+1}(A))$.

Let $\chi_1, \chi_2, \ldots, \chi_n$ be elements of $H^1(G, A) = \operatorname{Hom}(G, A)$. A *defining system* with respect to $(\chi_1, \ldots, \chi_n)$ is a homomorphism $\bar{\rho} : G \longrightarrow \bar{U}_{n+1}(A)$ such that $\rho_{i,i+1} = \chi_i$, where $\rho_{i,j}$ denotes the composition of $\bar{\rho}$ with the projection onto the (i, j)-entry of $\bar{U}_{n+1}(A)$. One can check that

$$\sum_{j=2}^{n} \rho_{1,j}(g_1)\, \rho_{j,n+1}(g_2)$$

defines a 2-cocycle in $\mathcal{C}^2(G, A)$ representing an element in $H^2(G, A)$. We denote this cohomology class by $(\chi_1, \chi_2, \ldots, \chi_n)_{\bar{\rho}}$ and call it the *Massey product with respect to the defining system* $\bar{\rho}$. By [Dwy75], the Massey product $(\chi_1, \ldots, \chi_n)_{\bar{\rho}}$ vanishes if and only if $\bar{\rho}$ can be lifted to a homomorphism $\rho : G \longrightarrow U_{n+1}(A)$.

Here, a defining system $\bar{\rho} \in \operatorname{Hom}(G, \bar{U}_{n+1}(A))$ can be viewed as a degree-one cocycle in $\mathcal{C}^1(G, \bar{U}_{n+1}(A))$, where G acts trivially on $\bar{U}_{n+1}(A)$. In general, the action of G on the ring A may not be trivial. In this case, one can define defining systems as degree-one cocycles in the same spirit, which allows for applications in more general settings. Moreover, one can also define the defining system for the generalized matrix algebra $\mathcal{U}(\mathcal{A})$. For details, see [Lam+23]. The paper [RS25] also has a section on the defining system for the generalized matrix algebra, which is essentially the same as [Lam+23]. Here, we directly borrow the definitions and notations from Section 3 of [Lam+23] without repeating them.

However, our notion of *proper defining systems* differs slightly from the definition in [Lam+23]. We provide a new definition of proper defining systems below. We take the same meaning of the modules T_1 and T_2 and their pairing as in Section 3 of [Lam+23].

Definition 1. Let $\chi \in H^1(G, T_1)$ and $\psi_0 \in H^1(G, T_2)$. A defining system $\bar{\rho} : G \longrightarrow \mathcal{U}(\mathcal{A})$ with respect to $(\underbrace{\chi, \chi, \ldots, \chi}_{n \text{ copies}}, \psi_0)$ is called a *proper defining system* if $\bar{\rho}$

has the following matrix form:

$$\bar{\rho} = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Remark 9. In [Lam+23], a proper defining system is defined by first dividing the matrix into four blocks, as in Lemma 8. They then fix the upper-left and lower-right blocks, allowing the upper-right block to vary. Our definition can be viewed as a special case of this construction. Specifically, we fix and explicitly specify the first $(n+1) \times (n+1)$ block, while allowing the last column to vary except for the entries 1 and ψ_0.

Remark 10. If the Massey product $(\underbrace{\chi, \chi, \ldots, \chi}_{n \text{ copies}}, \psi_0)$ with respect to a proper defining system vanishes, we construct a proper system for $(\underbrace{\chi, \chi, \ldots, \chi}_{n+1 \text{ copies}}, \psi_0)$ by put $\binom{\chi}{i}$ in the first line. This simple observation gives us a way to proceed from $\lambda \geq n-1$ to $\lambda \geq n$ and from $\Psi^{(n-1)}$ to $\Psi^{(n)}$ by induction.

The following Lemma 8 and Remark 11 will only be used in the section of numerical criterion. One can skip if not interested in the numerical criterion.

Lemma 8. *Let $\bar{\rho} : G \to \bar{U}_{m+n}$ be a defining system. We can write the homomorphism $\bar{\rho}$ as a block matrix:*

$$\bar{\rho} = \begin{bmatrix} A_n & \bar{B}_{n,m} \\ 0 & D_m \end{bmatrix}$$

where A_n is a $n \times n$ matrix and D_m is a $m \times m$ matrix. $\bar{B}_{n,m}$ is a $n \times m$ matrix without (n,m)-entry. Let $\bar{\rho}' : G \to \bar{U}_{m+n}$ be another defining system with the same first n columns and last m rows as $\bar{\rho}$, i.e.

$$\bar{\rho}' = \begin{bmatrix} A_n & \bar{B}'_{n,m} \\ 0 & D_m \end{bmatrix}$$

Then

$$\begin{bmatrix} A_n & \bar{B}_{n,m} + \bar{B}'_{n,m} \\ 0 & D_m \end{bmatrix}$$

is also a defining system.

Proof. The proof is a trivial calculation of matrices by the definition of defining system. We omit here. □

Remark 11. This easy observation gives us a way to generate a new defining system from old defining systems. For proper defining system, let $\bar{\rho}_n : G \to \bar{U}_{n+1}$ be a

proper defining system, i.e,

$$\bar{\rho}_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

One can check that $\bar{\rho}_{n+m} : G \to \bar{U}_{m+n+1}$ induced by $\bar{\rho}_n$ is still a proper defining system:

$$\bar{\rho}_{n+m} = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \cdots & \psi_{n-2} \\ \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ \cdots & 0 & 1 & \chi & \binom{\chi}{2} & \cdots & \binom{\chi}{m} & \psi_0 \\ 0 & \cdots & 0 & 1 & \chi & \cdots & \binom{\chi}{m-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \chi & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

If we have another proper defining system $\bar{\rho}'_{n+m} : G \to \bar{U}_{n+m+1}$,

$$\bar{\rho}'_{n+m} = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \cdots & \psi'_{n+m-2} \\ \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ \cdots & 0 & 1 & \chi & \binom{\chi}{2} & \cdots & \binom{\chi}{m} & \psi'_m \\ 0 & \cdots & 0 & 1 & \chi & \cdots & \binom{\chi}{m-1} & \psi'_{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi'_2 \\ 0 & 0 & 0 & 0 & 0 & 1 & \chi & \psi'_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \psi'_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Then by Lemma 8, we can produce a new proper defining system

$$\begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \cdots & \psi'_{n+m-2} + \psi_{n-2} \\ \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ \cdots & 0 & 1 & \chi & \binom{\chi}{2} & \cdots & \binom{\chi}{m} & \psi'_m + \psi_0 \\ 0 & \cdots & 0 & 1 & \chi & \cdots & \binom{\chi}{m-1} & \psi'_{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi'_2 \\ 0 & 0 & 0 & 0 & 0 & 1 & \chi & \psi'_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \psi'_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The image of generalized Bockstein map $\operatorname{Im}\Psi^{(n)}$ is spanned by certain Massey products relative to a proper defining system. The next theorem is just a special case of theorem 4.3.1 in [Lam+23].

Theorem 9 (LLSWW[Lam+23])**.** *Let G be a group with p-cohomological dimension 2. View $\Omega/I^n \otimes T$ as a quotient of polynomial ring in terms of variable x with coefficient in T, Let $f(\sigma) = \psi_0(\sigma) + \psi_1(\sigma)x + \cdots + \psi_{n-1}(\sigma)x^{n-1}$ be a cocycle in $\mathcal{C}^1(G, \Omega/I^n \otimes T)$, where ψ_i is a cochain in $\mathcal{C}^1(G,T)$. Then $\Psi^{(n)}(f) = (\sum_{i=1}^n \binom{\chi}{i} \cup \psi_{n-i})x^n$, where χ is the quotient map $\chi : G \to G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$. And easy to see, $\sum_{i=1}^n \binom{\chi}{i} \cup \psi_{n-i}$ is Massey product $(\chi^{(n)}, \psi_0)$ relative to a proper defining system. Here $\chi^{(n)}$ denotes n-copies of χ. More precisely, the proper defining system is:*

$$\begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Remark 12. We have $(\binom{\chi}{i} \cup \psi_{n-i})(g_1, g_2) = \binom{\chi(g_1)}{i} \cup g_1\psi_{n-i}(g_2)$. And this is compatible with our action of G on $\Omega \otimes T$. And this is compatible with definition of defining system ρ to be a cocycle: $\rho(g_1g_2) = \rho(g_1)g_1\rho(g_2)$

3. Size of H^2

The philosophy of the strategy is to use Massey products to analyze the size of H^2. We first prove some lemmas we will use later. Since they all can be derived purely from group cohomology theory. We put them in this section. From now on, we assume G is p-cohomologically finite and G has p cohomological dimension $d = 2$.

Lemma 10. *Let G be a p-cohomologically finite profinite group with p cohomological dimension equal 2, N be a closed normal subgroup such that $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$. And T is a finite $\mathbb{F}_p[G]$-module. Assume $H^2(G,T) \cong \mathbb{F}_p$ and $\Psi^{(k)} \neq 0$ for some $0 < k < \#G/N$, then $\#H^2_{\mathrm{Iw}}(N,T) = p^n$ where $n = \min\{n | \Psi^{(n)} \neq 0\}$*

Proof. Take $n = \min\{n \in \mathbb{N} | \Psi^{(n)} \neq 0\}$, then $\Psi^{(n)} \neq 0$. We have $H^2(G,T) \cong \mathbb{F}_p \cong \operatorname{Im}\Psi^{(n)}$. By theorem 4, $I^nH^2_{\mathrm{Iw}}(N,T) = I^{n+1}H^2_{\mathrm{Iw}}(N,T)$. Since G is p-cohomologically finite, we know that $H^2_{\mathrm{Iw}}(N,T)$ is finitely generated Ω-module by [Lam+23, Prop 2.2.2]. By Nakayama's lemma, $I^nH^2_{\mathrm{Iw}}(N,T) = 0$. We have the filtration $H^2_{\mathrm{Iw}}(N,T) \supset IH^2_{\mathrm{Iw}}(N,T) \supset I^2H^2_{\mathrm{Iw}}(N,T) \supset \cdots \supset I^nH^2_{\mathrm{Iw}}(N,T) = 0$ and when $i < n$, $\frac{I^iH^2_{\mathrm{Iw}}(N,T)}{I^{i+1}H^2_{\mathrm{Iw}}(N,T)} = \mathbb{F}_p$. Hence $\#H^2_{\mathrm{Iw}}(N,T) = p^n$. □

Theorem 11. *Let G be a profinite group, N be a closed normal subgroup such that $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$ and T be a $\mathbb{F}_p[G]$ module. Fix an integer $n < \#G/N$. Assume the generalized Bockstein map $\Psi^{(i)} = 0$ for all $0 \leq i < n$, then the value $\Psi^{(n)}(f)$, where $f(\sigma) = \psi_0(\sigma) + \psi_1(\sigma)x + \cdots + \psi_{n-1}(\sigma)x^{n-1}$ is a cocycle in $\mathcal{C}^1(G, \Omega/I^n \otimes T)$, only depends on the cohomology class of ψ_0 and does not depend on other coefficients ψ_i, $0 < i < n$.*

Proof. Let $f' = \psi_0' + \psi_1' x + \cdots + \psi_{n-1}' x^{n-1}$ be another cocycle in $\mathcal{C}^1(G, \Omega/I^n \otimes T)$ such that ψ_0 and ψ_0' are in the same cohomology class. Then $(\psi_0 - \psi_0')(\sigma) = \sigma m - m$ for some $m \in T$. Let $\delta = (\psi_0 - \psi_0') + (\chi \cup m)x + (\binom{\chi}{2} \cup m)x^2 + \cdots + (\binom{\chi}{n-1} \cup m)x^{n-1}$. One can check that $\Psi^{(n)}(\delta) = d(\binom{\chi}{n} \cup m)x^n = 0 \in H^2(G,T) \otimes I^n/I^{n+1}$. By adding δ to f', we can assume that $\psi_0' = \psi_0$. Then $f - f' \in \mathcal{C}^1(G, I/I^n \otimes T)$. Since $\Omega/I^{n-1} \cong \mathbb{F}_p[x]/(x^{n-1})$ is isomorphic to $I/I^n \cong (x)/(x^n)$ by a multiplication of x, $\Psi^{(n)}(f - f') = \Psi^{(n-1)}(\frac{f-f'}{x}) = 0$ by assumption. Hence $\Psi^{(n)}(f)$ only depends on the cohomology class of ψ_0. □

Under the conditions $\Psi^{(i)} = 0$ for all $0 \leq i < n$, for convenience, we use $\Psi^{(n)}([\psi_0])$ to denote $\Psi^{(n)}(\psi_0 + \psi_1 x + \cdots + \psi_{n-1}x^{n-1})$ since the value only depends on the cohomology class of ψ_0. And in the language of Massey product, $\Psi^{(n)}([\psi_0])$ equals to the Massey product $(\chi^{(n)}, \psi_0)$ relative to a proper defining system.

Notice from the following exact sequence:

$$H^1(G, \Omega/I^{n+1} \otimes T) \to H^1(G, \Omega/I^n \otimes T) \to H^2(G, I^n/I^{n+1} \otimes T)$$

Hence $\Psi^{(n)}(f)$ is zero for a cocycle $f(\sigma) = \psi_0(\sigma) + \psi_1(\sigma)x + \cdots + \psi_{n-1}(\sigma)x^{n-1}$ in $\mathcal{C}^1(G, \Omega/I^n \otimes T)$ if and only if we can lift f to $\mathcal{C}^1(G, \Omega/I^{n+1} \otimes T)$, i.e. there is a cocycle in $\mathcal{C}^1(G, \Omega/I^{n+1} \otimes T)$ in the form of $\widetilde{f}(\sigma) = \psi_0(\sigma) + \psi_1(\sigma)x + \cdots + \psi_{n-1}(\sigma)x^{n-1} + \psi_n(\sigma)x^n$.

Definition 2. Let ψ be an element in $H^1(G,T) = H^1(G, \Omega/I \otimes T)$. We say ψ has p cyclic Massey product vanishing property, if we can lift ψ to an element in $H^1(G, \Omega \otimes T)$, i.e. there is an element in $\mathcal{C}^1(G, \Omega \otimes T)$ in the form $\sum_i \psi_i(\sigma)x^i$ with $\psi_0 = \psi$, where the sum over all $0 \leq i < \infty$ or $0 \leq i < p^k$ with respect to $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^k\mathbb{Z}$.

Remark 13. Assume $\Psi^{(i)} = 0$ for all $0 \leq i < n$ and ψ has p cyclic Massey product vanishing property. Then we have $\Psi^{(n)}([\psi]) = 0$.

Theorem 12. *The element $\psi \in H^1(G,T)$ has p cyclic Massey product vanishing property if and only if $\psi \in \mathrm{Im}(H^1_{\mathrm{Iw}}(N,T) \xrightarrow{Cor} H^1(G,T))$.*

Proof. By lemma 6, we have $H^1_{\mathrm{Iw}}(N,T) \cong H^1(G, \Omega \otimes T)$. And the map $H^1(G, \Omega \otimes T) \to H^1(G, \Omega/I \otimes T)$ induced by the quotient $\Omega \to \Omega/I$ corresponding to the corestriction map $H^1_{\mathrm{Iw}}(N,T) \to H^1(G,T)$ by definition.

□

4. Applications to number theory

Now we apply previous sections to number theory. Though all notations are standard, we list them here for convenience:

(1) p: odd prime.
(2) K: number field.
(3) μ_{p^l}: group of p^l-th roots of unity.
(4) S: set of primes of K above p.
(5) K_S: maximal algebraic extension of K which is unramified outside primes above p and infinite primes.
(6) $G_{K,S} = \mathrm{Gal}(K_S/K)$.
(7) $\mathcal{O}_K$: ring of integers of K.
(8) $\mathcal{O}_{K,S}$: ring of S -integers of K.

(9) $\mathrm{Cl}(K)$: class group of K.
(10) h_K: the size of $\mathrm{Cl}(K)$.
(11) $\mathrm{Cl}_S(K)$: S -class group of K.
(12) $Br(\mathcal{O}_K[1/p])$: The subgroup of the Brauer group $Br(K)$ of K consisting of all classes of central simple K-algebras, which are split outside of primes above p. Hence, we have $Br(\mathcal{O}_K[1/p]) \cong (\mathbb{Q}/\mathbb{Z})^{\#S-1}$ as abelian group.
(13) $A[n]$: subgroup of elements of abelian group A that annihilated by n.
(14) Let $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$ be a $\mathbb{Z}_p$ extension of K.
(15) X: the Iwasawa module $X = \varprojlim \mathrm{Cl}(K_l)[p^\infty]$.
(16) λ: the Iwasawa invariant λ for X.
(17) χ: character that equal the restriction $G_{K,S} \xrightarrow{Res} \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

Theorem 13. *Let K_l/K be a $\mathbb{Z}/p^l\mathbb{Z}$ extension of K inside K_S. Take $G = G_{K,S} = \mathrm{Gal}(K_S/K)$, $N = G_{K_l,S} = \mathrm{Gal}(K_S/K_l)$, $T = \mu_p$. Let $\alpha \in \mathrm{Nm}_{K_l/K}(\mathcal{O}^*_{K_l,S})$, then α has p cyclic Massey product vanishing property.*

Let K_∞/K be a $\mathbb{Z}_p$ extension of K inside K_S. Take $G = G_{K,S} = \mathrm{Gal}(K_S/K)$, $N = G_{K_\infty,S} = \mathrm{Gal}(K_S/K_\infty)$, $T = \mu_p$. Let $\alpha \in \mathrm{Im}(\varprojlim \mathcal{O}^*_{K_l,S} \xrightarrow{\mathrm{Nm}} K^*)$ where the inverse limit is taking over all sub-extension of K_∞/K with respect to norm map. Then α has p cyclic Massey product vanishing property.

Proof. By Kummer theory, $H^1(G,\mu_p) \cong K^* \cap (K_S^*)^p/(K^*)^p$ and $H^1(N,\mu_p) = K_l^* \cap (K_S^*)^p/(K_l^*)^p$. The corestriction map from $H^1(N,\mu_p)$ to $H^1(G,\mu_p)$ corresponds to Norm map[Mil20]. Notice that $\mathcal{O}^*_{K_l,S} \subset (K_S^*)^p$. And by theorem 12, the theorem holds. The second conclusion follows by taking the inverse limit. □

Remark 14. The map $\varprojlim \mathcal{O}^*_{K_l,S} \xrightarrow{\mathrm{Nm}} \mathcal{O}^*_{K,S} \hookrightarrow K^*$ is the projection map from the inverse limit $\varprojlim \mathcal{O}^*_{K_l,S}$ to the first factor.

From Kummer theory, we have the following two exact sequences: (good references are [Kol04][Sha18, Proposition 5.1.5][NSW08, Theorem 8.7.4])

$$0 \to \mathcal{O}^*_{K,S}/p := \mathcal{O}^*_{K,S}/(\mathcal{O}^*_{K,S})^p \to H^1(G_{K,S},\mu_p) \to \mathrm{Cl}_S(K)[p] \to 0 \tag{1}$$

$$0 \to \mathrm{Cl}_S(K)/p \to H^2(G_{K,S},\mu_p) \to Br(\mathcal{O}_K[1/p])[p] \to 0 \tag{2}$$

The map $\mathcal{O}^*_{K,S}/p \to H^1(G_{K,S},\mu_p)$ is the composite of the natural inclusion and Kummer map,i.e.: $\mathcal{O}^*_{K,S}/p \to K^* \cap (K_S^*)^p/(K^*)^p \cong H^1(G_{K,S},\mu_p)$. The map $H^1(G_{K,S},\mu_p) \to \mathrm{Cl}_S(K)[p]$ is the map $\alpha \in K^* \cap (K_S^*)^p/(K^*)^p \cong H^1(G_{K,S},\mu_p) \to [I] \in \mathrm{Cl}_S(K)[p]$ where I is an ideal such that $I^p = \alpha\mathcal{O}_{K,S}$. Since $Br(\mathcal{O}_K[1/p])[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\#S-1}$, so $Br(\mathcal{O}_K[1/p])[p] \cong \mathbb{F}_p^{\#S-1}$.

Now, we can state and prove our main theorem.

Theorem 14. *Let $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$ be a $\mathbb{Z}_p$ extension of K and S be the set of primes above p for K. Assume all primes in S are totally ramified in K_∞/K. Let $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty]$ and μ_{cs}, λ_{cs} be the Iwasawa invariant of X_{cs}. Assume X_{cs} has no finite Λ submodule and $H^2(G_{K,S},\mu_p) \cong \mathbb{F}_p$.*

Then $\mu_{cs} = 0$ if and only if there exists k such that $\Psi^{(k)} \neq 0$ for some k. If $\mu_{cs} = 0$, then $\lambda_{cs} = \min\{n|\Psi^{(n)} \neq 0\} - \#S + 1$.

Proof. We have the following exact sequence:

$$0 \to \mathrm{Cl}_S(K_l)/p \to H^2(G_{K_l,S},\mu_p) \to Br(\mathcal{O}_{K_l}[1/p])[p] \to 0$$

for every l. since $\mathrm{Cl}_S(K_l)/p$ is finite group, it satisfies Mittag-Leffler condition. Thus the above exact sequence remains exact after taking inverse limit.

$$0 \to \varprojlim \mathrm{Cl}_S(K_l)/p \to \varprojlim H^2(G_{K_l,S}, \mu_p) \to \varprojlim Br(\mathcal{O}_{K_l}[1/p])[p] \to 0$$

By definition of $\mathrm{Br}(\mathcal{O}_{K_l}[1/p])[p]$, we have

$$\mathrm{Br}(\mathcal{O}_{K_l}[1/p])[p] \simeq \ker\left(\bigoplus_{v|p} \mathrm{Br}(K_{l,v})[p] \cong \bigoplus_{v\in S_l} \frac{1}{p}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sum_v \mathrm{inv}_v} \frac{1}{p}\mathbb{Z}/\mathbb{Z}\right) \simeq \mathbb{F}_p^{\#S_l - 1}.$$

Since all primes in S are totally ramified K_∞/K, we have $\#S_l = \#S$. By [Tat67, Chapter VII, §9.7, equation (16)], we have the compatibility of corestriction with local invariants for a separable field extension L/K,

$$\mathrm{inv}_v\big(\mathrm{Cor}_{L/K}\,\alpha\big) = \sum_{w|v} \mathrm{inv}_w(\alpha_w).$$

As K_{l+1}/K_l is totally ramified at prime above p, we have $\mathrm{inv}_v\big(\mathrm{Cor}_{K_{l+1,w}/K_{l,v}}(\alpha_w)\big) = \mathrm{inv}_w(\alpha_w)$ for $\alpha_w \in \mathrm{Br}(K_{l+1,w})$. Hence, we have that

$$\mathrm{Cor}_{K_{l+1}/K_l} : \mathrm{Br}(\mathcal{O}_{K_{l+1}}[1/p])[p] \to \mathrm{Br}(\mathcal{O}_{K_l}[1/p])[p]$$

is an isomorphism. Hence, the inverse limit $\varprojlim Br(\mathcal{O}_{K_l}[1/p])[p] \cong Br(\mathcal{O}_K[1/p])[p] \cong \mathbb{F}_p^{\#S-1}$.

We have the following exact sequence:

$$0 \to \mathrm{Cl}_S(K_l)[p] \to \mathrm{Cl}_S(K_l)[p^\infty] \xrightarrow{\times p} \mathrm{Cl}_S(K_l)[p^\infty] \to \mathrm{Cl}_S(K_l)/p \to 0$$

Take the inverse limit, and it remains exact by the Mittag-Leffler condition,

$$0 \to \varprojlim \mathrm{Cl}_S(K_l)[p] \to X_{cs} \xrightarrow{\times p} X_{cs} \to \varprojlim \mathrm{Cl}_S(K_l)/p \to 0$$

Hence $\varprojlim \mathrm{Cl}_S(K_l)/p = X_{cs}/p$. We have $\mu_{cs} = 0$ if and only if X_{cs}/p is a finite group if and only if $\varprojlim H^2(G_{K_l,S}, \mu_p)$ is a finite group if and only if there exists k such that $\Psi^{(k)} \neq 0$ for some k by lemma 10 . Now assume $\mu_{cs} = 0$. It is well known that the $\mathbb{Z}_p$ rank of X_{cs} is λ_{cs}. Since we assume that X_{cs} has no Λ finite submodule, we have $\varprojlim \mathrm{Cl}_S(K_l)/p = X_{cs}/p \cong \mathbb{F}_p^{\lambda_{cs}}$.

Recall that p cohomological dimension of $G_{K,S}$ is 2. We have

$$\#\varprojlim H^2(G_{K_l,S}, \mu_p) = \#H^2_{\mathrm{Iw}}(G_{K_\infty,S}, \mu_p) = p^n,$$

where $n = \min\{n|\Psi^{(n)} \neq 0\}$ by lemma 10. Therefore, by the exact sequence, we have

$$\lambda_{cs} - \min\{n|\Psi^{(n)} \neq 0\} + \#S - 1 = 0$$

Hence $\lambda_{cs} = \min\{n|\Psi^{(n)} \neq 0\} - \#S + 1$

□

Remark 15. The condition $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$ is restrictive. If $H^2(G_{K,S}, \mu_p)$ is large, we may use the following theorem 16 where we decompose $H^2(G_{K,S}, \mu_p)$ into smaller eigenspaces such that each small piece is 1-dimensional. We impose the condition $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$ to make corollaries in terms of Massey products clean. Since $H^2(G_{K,S}, \mu_p)$ is one-dimensional, one nonzero Massey product can expand the whole space. Hence we just need to consider whether the Massey product is nonzero, and it is easy to develop a numerical criterion as we just need to calculate only one Massey product. If $H^2(G_{K,S}, \mu_p)$ is large, we need many

Massey products to expand the group $H^2(G_{K,S}, \mu_p)$. Hence, we need to consider many Massey products and how they intertwine with each other. The results of our paper have been generalized by [RS25], where they do not require $H^2(G_{K,S}, \mu_p)$ to be one-dimensional, and they have to use the language that many Massey products are used to expand the group $H^2(G_{K,S}, \mu_p)$. Since it would be difficult to get a clean calculation when considering a bunch of Massey products, they do not develop the numerical criterion. In summary, the strategy of the proof allows one to remove the condition on $H^2(G_{K,S}, \mu_p)$. It may look beautiful in theory, but it would be difficult if one wants to calculate explicitly when $H^2(G_{K,S}, \mu_p)$ is large.

In the proof of the theorem, to use the lemma 10, we take $G = G_{K,S}$, $N = G_{K_\infty,S}$, $\chi : G \to G/N \cong \mathbb{Z}_p$ and $\Omega = \mathbb{F}_p[[G/N]]$. And these are the set up that we use for most of the section. The purpose of the setup is purely for theoretical consistency. In practice, to calculate the Massey product, we would like $\Omega = \mathbb{F}_p[[G/N]]$ to be small. If we know $\lambda_{cs} < p^l$ for some l in advance, we can take $G = G_{K,S}$, $N = G_{K_l,S}$, $\chi : G \to G/N \cong \mathbb{Z}/p^l\mathbb{Z}$ and $\Omega = \mathbb{F}_p[[G/N]]$.

Theorem 15. *Let $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$ be a $\mathbb{Z}_p$ extension of K and S be the set of primes above p for K. Assume all primes in S are totally ramified in K_∞/K. Let $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty]$ and μ_{cs}, λ_{cs} be the Iwasawa invariant of X_{cs}. Assume X_{cs} has no finite Λ submodule and $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$ and $\mu_{cs} = 0$. Assume $\lambda_{cs} < p^l$. Then $\lambda_{cs} = \min\{n | \Psi^{(n)} \neq 0\} - \#S + 1$. Here the definition of $\Psi^{(n)}$ is with respect to $G = G_{K,S}$, $N = G_{K_l,S}$, $\chi : G \to G/N \cong \mathbb{Z}/p^l\mathbb{Z}$ and $\Omega = \mathbb{F}_p[[G/N]]$.*

Proof. We have the following exact sequence:

$$0 \to \mathrm{Cl}_S(K_l)/p \to H^2(G_{K_l,S}, \mu_p) \to Br(\mathcal{O}_{K_l}[1/p])[p] \to 0$$

We will use Lemma 13.15 in [Was97] and the same notation as [Was97, Lemma 13.15]. We have $\mathrm{Cl}_S(K_l)/p = X_{cs}/(\frac{(1+T)^{p^l}-1}{T}Y_0, pX_{cs}) = X_{cs}/(T^{p^l-1}Y_0, pX_{cs})$. Let f be the characteristic polynomial of X_{cs}. Since X_{cs} has no finite Λ submodule, we have $fX_{cs} = 0$. We have

$$\begin{aligned}\mathrm{Cl}_S(K_l)/p &= X_{cs}/(T^{p^l-1}Y_0, pX_{cs}) = X_{cs}/(T^{p^l-1}Y_0, pX_{cs}, fX_{cs}) \\ &= X_{cs}/(T^{p^l-1}Y_0, pX_{cs}, T^{\lambda_{cs}}X_{cs}) = X_{cs}/(pX_{cs}, T^{\lambda_{cs}}X_{cs}) \\ &= X_{cs}/(pX_{cs}, fX_{cs}) = X_{cs}/pX_{cs} \cong \mathbb{F}_p^{\lambda_{cs}}\end{aligned}$$

since $\lambda_{cs} < p^l$.

The remaining proof is similar to the proof of Theorem 14 □

Next, we will discuss the situation when we have a group Δ acting on our Iwasawa module. We can decompose our Iwasawa module as a direct sum of eigenspace with respect to the action. For each direct sum, we can also define the Iwasawa λ invariant. We will show that we can compute the Iwasawa λ invariant in the same strategy since we have proved that the generalized Bockstein map preserves the group action in section 2.1.

Let k be a number field and K/k be an abelian extension. Denote $\mathrm{Gal}(K/k) = \Delta$. Let $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$ be a $\mathbb{Z}_p$ extension of K and K_∞/k is an abelian extension. Suppose all the field extensions K_l/k, K_∞/k, K_S/k are Galois extensions. Assume $\mathrm{Gal}(K_\infty/k) \cong \Delta \oplus \mathbb{Z}_p$. Let $\mathscr{G} = G_{k,S} = \mathrm{Gal}(K_S/k)$, $G =$

$G_{K,S} = \mathrm{Gal}(K_S/K)$, $N = G_{K_\infty,S} = \mathrm{Gal}(K_S/K_\infty)$ and $T = \mu_p$. By subsection 2.1, the Galois group $\mathrm{Gal}(K/k) = \Delta$ can act on $H^i(G_{K,S}, \Omega/I^n \otimes \mu_p)$ and $\Psi^{(n)}(\tau\phi) = \tau\Psi^{(n)}(\phi)$ for any $\phi \in H^1(G, \Omega/I^n \otimes \mu_p)$ and $\tau \in \Delta$.

Let $\hat{\Delta} \coloneqq \mathrm{Hom}(\Delta, \bar{\mathbb{Q}}^\times)$ be the character group. Let $\omega \in \hat{\Delta}$ and define

$$\varepsilon_\omega = \frac{1}{\#\Delta} \sum_{\sigma \in \Delta} \omega(\sigma)\sigma^{-1} \in \bar{\mathbb{Q}}[\Delta].$$

Let X be any $\bar{\mathbb{Q}}[\Delta]$ module. Then the standard process gives us a decomposition of X:

$$X = \bigoplus_{\omega \in \hat{\Delta}} \varepsilon_\omega X.$$

Theorem 16. *Let K_∞/K be the $\mathbb{Z}_p$ extension as set up above. Assume all primes in S are totally ramified in K_∞/K. Let $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty]$. Assume all characters of Δ is $\mathbb{Z}_p$-valued, The action of Δ on X_{cs} gives a decomposition $X_{cs} = \oplus_\omega \varepsilon_\omega X_{cs}$. Let $\mu_{\omega,cs}$, $\lambda_{\omega,cs}$ be the Iwasawa invariant of $\varepsilon_\omega X_{cs}$. Assume $\varepsilon_\omega X_{cs}$ has no finite Λ submodule and $\varepsilon_\omega H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$. Then $\mu_{\omega,cs} = 0$ if and only if there exist k such that $\varepsilon_\omega \Psi^{(k)} \neq 0$ for some k. If $\mu_{\omega,cs} = 0$ then $\lambda_{\omega,cs} = \min\{n | \varepsilon_\omega \Psi^{(n)} \neq 0\} - dim_{\mathbb{F}_p} \varepsilon_\omega Br(\mathcal{O}_K[1/p])[p]$*

Proof. The proof is almost the same as Theorem 14, we give a sketch of proof here.

We have the following exact sequence:

$$0 \to \mathrm{Cl}_S(K_l)/p \to H^2(G_{K_l,S}, \mu_p) \to Br(\mathcal{O}_{K_l}[1/p])[p] \to 0$$

for every l. The action of Δ gives us:

$$0 \to \varepsilon_\omega \mathrm{Cl}_S(K_l)/p \to \varepsilon_\omega H^2(G_{K_l,S}, \mu_p) \to \varepsilon_\omega Br(\mathcal{O}_{K_l}[1/p])[p] \to 0$$

Take inverse limit,

$$0 \to \varepsilon_\omega \varprojlim \mathrm{Cl}_S(K_l)/p \to \varepsilon_\omega \varprojlim H^2(G_{K_l,S}, \mu_p) \to \varepsilon_\omega \varprojlim Br(\mathcal{O}_{K_l}[1/p])[p] \to 0$$

We have $\mu_{\omega,cs} = 0$ if and only if $\varepsilon_\omega \varprojlim \mathrm{Cl}_S(K_l)/p$ is finite if and only if $\varepsilon_\omega \varprojlim H^2(G_{K_l,S}, \mu_p)$ is finite if and only if there exist k such that $\varepsilon_\omega \Psi^{(k)} \neq 0$ for some k.

Assume $\mu_{\omega,cs} = 0$ now. Similar argument as proof of Theorem 14, we have

$$\varepsilon_\omega \varprojlim Br(\mathcal{O}_{K_l}[1/p])[p] = \varepsilon_\omega Br(\mathcal{O}_K[1/p])[p]$$

and

$$\varepsilon_\omega \varprojlim \mathrm{Cl}_S(K_l)/p \cong \mathbb{F}_p^{\lambda_{\omega,cs}}$$

and

$$\dim_{\mathbb{F}_p} \varepsilon_\omega \varprojlim H^2(G_{K_l,S}, \mu_p) = \min\{n | \Psi^{(n)}|_{\varepsilon_\omega H^1(G_{K,S}, \Omega/I^n \otimes \mu_p)} \neq 0\},$$

where $\Psi^{(n)}|_{\varepsilon_\omega H^1(G_{K,S}, \Omega/I^n \otimes \mu_p)}$ denotes $\Psi^{(n)}$ restricting on $\varepsilon_\omega H^1(G_{K,S}, \Omega/I^n \otimes \mu_p)$. Since $\Psi^{(n)}(\tau\phi) = \tau\Psi^{(n)}(\phi)$ for any $\phi \in H^1(G, \Omega/I^n \otimes \mu_p)$ and $\tau \in \Delta$, we have $\Psi^{(n)}|_{\varepsilon_\omega H^1(G_{K,S}, \Omega/I^n \otimes \mu_p)} = 0$ if and only if $\varepsilon_\omega \Psi^{(n)} = 0$. Hence the conclusion follows from the exact sequence. □

Remark 16. We can have a similar theorem as theorem 15 with the action of Δ. We omit it here since it is essentially the same.

Remark 17. As we said before, the theory of the Generalized Bockstein map and Massey products works generally. The strategy of the paper also works generally. The results of our paper have been partially generalized by [RS25] by the same strategy. In their paper, they consider higher-dimensional representations, for example, $E[p]$, not just μ_p as in our case.

Before we apply the theorem to a specific field, we first recall some well-known lemmas in the classical Iwasawa theory. They will be used in the next section. The next lemma is Proposition 13.26 in the book [Was97].

Lemma 17. *Let p be odd. Suppose K is a CM-field and K_∞/K is the cyclotomic $\mathbb{Z}_p$ extension. The complex conjugation action gives us the decomposition $\mathrm{Cl}(K_l)[p^\infty] = \mathrm{Cl}(K_l)[p^\infty]^+ \oplus \mathrm{Cl}(K_l)[p^\infty]^-$. Assume all primes which are ramified in K_∞/K are totally ramified. Then the map*

$$\mathrm{Cl}(K_l)[p^\infty]^- \to \mathrm{Cl}(K_{l+1})[p^\infty]^-$$

is injective.

By using the lemma 17, one can get the following lemma. It is Proposition 13.28 in [Was97].

Lemma 18. *The same assumption as Lemma 17, then $X^- = \varprojlim \mathrm{Cl}(K_l)[p^\infty]^-$ contains no finite Λ-submodules.*

In the paper [Gol74], Gold refined the Lemma 17 to the following theorem.

Theorem 19. *The same assumption as lemma 17, let D_l be the subgroup of $\mathrm{Cl}(K_l)[p^\infty]$ generated by primes of K_l above p. Hence we have $\mathrm{Cl}_S(K_l)[p^\infty] = \mathrm{Cl}(K_l)[p^\infty]/D_l$ and $\mathrm{Cl}_S(K_l)[p^\infty]^- = \mathrm{Cl}(K_l)[p^\infty]^-/D_l^-$ by definition. Then the map*

$$\mathrm{Cl}_S(K_l)[p^\infty]^- \to \mathrm{Cl}_S(K_{l+1})[p^\infty]^-$$

is injective. Moreover $\#D_m^- = p^{s(m-l)}\#D_l^-$ for any integer $m \geq l$, where s is the number of primes of K_l^+ lying over p which split in K_l/K_l^+.

The conclusion about the size of D_l is hidden in Gold's proof of his theorem.

Theorem 20. *The same assumption as lemma 17, then $X_{cs}^- = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty]^-$ contains no finite Λ-submodules.*

Proof. One can use a similar argument as the proof that lemma 17 implies lemma 18 in [Was97]. I omit the proof here since it is almost the same argument. □

5. Application to concrete examples

In this section, we will apply the theorems that we get in the previous section 4 to some concrete examples. In the following examples, they all are the cyclotomic $\mathbb{Z}_p$ extension. The same strategy can apply to other $\mathbb{Z}_p$ extensions as long as it satisfies the conditions in the theorem. The first three cases are about imaginary quadratic fields. The last case is about cyclotomic fields. In the first case of the imaginary quadratic field, we also develop a numerical criterion, which can help us to compute the λ invariant through the computer. The section of numerical criterion is independent from other cases. It is suggested to skip the numerical criterion subsection for the first time reading.

5.1. **Imaginary Quadratic field.**

5.1.1. *case 1.* Let K be an imaginary quadratic field and $h_K = \#Cl(K)$, $p \nmid h_K$, p splits in K. Let $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$ be the cyclotomic $\mathbb{Z}_p$ extension of K. Let $p\mathcal{O}_{K_l} = \mathfrak{p}_l\tilde{\mathfrak{p}}_l$ where $\tilde{\mathfrak{p}}_l$ is the complex conjugation of $\mathfrak{p}_l$. Let $(\alpha) = \mathfrak{p}_0^{h_K}$, $(\tilde{\alpha}) = \tilde{\mathfrak{p}}_0^{h_K}$, $\tilde{\alpha}$ is the conjugation of α. By Kummer theory, α corresponds to an element in $H^1(G, \mu_p)$, i.e. $\sigma \to \sigma(\sqrt[p]{\alpha})/\sqrt[p]{\alpha}$. Recall χ is a character $\chi : G_{K,S} \xrightarrow{Res} \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

Theorem 21. *Let K be an imaginary quadratic field, $p \nmid h_K$, p splits in K and $n \geq 2$. Assume $\lambda \geq n-1$, then $\lambda \geq n \Leftrightarrow$ n-fold Massey product $(\underbrace{\chi, \chi, \ldots, \chi}_{n-1 \ copies}, \alpha)$ vanishes with respect to a proper defining system.*

Remark 18. It is well known that $\lambda \geq 1$ is always true. Hence $\lambda \geq 2 \Leftrightarrow$ the cup product $\chi \cup \alpha = 0$. Later, in the section on numerical criterion, we will show that it is easy to see that $\chi \cup \alpha = 0 \Leftrightarrow \log_p \alpha \equiv 0 \mod p^2$, where $\log_p$ is the p-adic log. And this is a version of Gold's criterion [Gol74]. Our theorem gives a new proof of Gold's criterion and generalizes the criterion.

proof of theorem 21.

We have that K is an imaginary quadratic field and K_∞/K is a cyclotomic $\mathbb{Z}_p$ extension. Hence, it satisfies the assumption in theorem 19 and theorem 20 and we will use the same notation as them. By using Proposition 13.22 in [Was97], we know $\mathrm{Cl}(K_l)[p^\infty]^+ = 0$. Hence $D_l^- = D_l$ and $\mathrm{Cl}(K_l)[p^\infty]^- = \mathrm{Cl}(K_l)[p^\infty]$. By definition, we have that D_l^- is generated by one element $\mathfrak{p}_l/\tilde{\mathfrak{p}}_l$. Hence $D_l = D_l^-$ is a cyclic group. There is only one prime in K_l^+ lying over p that splits in K_l/K_l^+. Thus $\#D_l = p^l \# D_0 = p^l$. We have $D_l = \mathbb{Z}/p^l\mathbb{Z}$. We have the following exact sequence:

$$0 \to D_l \to Cl(K_l)[p^\infty] \to Cl_S(K_l)[p^\infty] \to 0$$

Take the inverse limit. We have the following exact sequence by the Mittag-Leffler condition

$$0 \to \mathbb{Z}_p \to X \to X_{cs} \to 0.$$

By lemma 18 and theorem 20, we know that X and X_{cs} have no finite Λ-submodule. View them as $\mathbb{Z}_p$ module, we have $Rank_{\mathbb{Z}_p}\mathbb{Z}_p - Rank_{\mathbb{Z}_p}X + Rank_{\mathbb{Z}_p}X_{cs} = 0$. So $\lambda = \lambda_{cs} + 1$.

By the exact sequence (2), we have

$$0 \to \mathrm{Cl}_S(K)/p = 0 \to H^2(G_{K,S}, \mu_p) \to Br(\mathcal{O}_K[1/p])[p] = \mathbb{F}_p \to 0$$

Hence $H^2(G_{K,S}, \mu_p) \cong F_p$. Thus, our case satisfies all conditions in the theorem 14. We have $\lambda_{cs} = \min\{n | \Psi^{(n)} \neq 0\} - 2 + 1$. Therefore, we have $\lambda = \min\{n | \Psi^{(n)} \neq 0\}$. Hence $\lambda \geq n \Leftrightarrow \Psi^{(i)} = 0$ for all $0 \leq i < n$.

By exact sequence (1) and $\mathrm{Cl}(K)[p] = 0$, $H^1(G_{K,S}, \mu_p) \cong \mathcal{O}_{K,S}^*/p =< \alpha, \tilde{\alpha} >$. Assume $\Psi^{(i)} = 0$ for all $0 \leq i < n-1$ now, then by theorem 11, $\mathrm{Im}\,\Psi^{(n-1)}$ is generated by $\Psi^{(n-1)}([\alpha])$ and $\Psi^{(n-1)}([\tilde{\alpha}])$.

Let ζ_{p^l} be the primitive p^l-th root of unit. Let $\mathbb{Q}_{l-1}$ be the unique subfield of $\mathbb{Q}(\mu_{p^l})$ such that $\mathrm{Gal}(\mathbb{Q}_{l-1}/\mathbb{Q}) = \mathbb{Z}/p^{l-1}\mathbb{Z}$. Then $K_l = K\mathbb{Q}_l$. We have

$$p = \mathrm{Nm}_{\mathbb{Q}(\mu_{p^l})/\mathbb{Q}}(1 - \zeta_{p^l})$$

and

$$1 - \zeta_{p^l} = \mathrm{Nm}_{\mathbb{Q}(\mu_{p^{l+1}})/\mathbb{Q}(\mu_{p^l})}(1 - \zeta_{p^{l+1}}).$$

Let

$$\eta_l \coloneqq \mathrm{Nm}_{\mathbb{Q}(\mu_{p^{l+1}})/\mathbb{Q}_l}(1-\zeta_{p^{l+1}}),$$

then

$$p = \mathrm{Nm}_{\mathbb{Q}_l/\mathbb{Q}}(\eta_l), \eta_l = \mathrm{Nm}_{\mathbb{Q}_{l+1}/\mathbb{Q}_l}(\eta_{l+1}).$$

Since $K_l = K\mathbb{Q}_l$ and $K \cap \mathbb{Q}_l = \mathbb{Q}$, then

$$\mathrm{Gal}(K_l/K) = \mathrm{Gal}(\mathbb{Q}_l/\mathbb{Q}), \mathrm{Gal}(K_{l+1}/K_l) = \mathrm{Gal}(\mathbb{Q}_{l+1}/\mathbb{Q}_l).$$

So $p = \mathrm{Nm}_{K_l/K}(\eta_l)$ and $\eta_l = \mathrm{Nm}_{K_{l+1}/K_l}(\eta_{l+1})$. We know

$$\eta_l = \mathrm{Nm}_{\mathbb{Q}(\mu_{p^{l+1}})/\mathbb{Q}_l}(1-\zeta_{p^{l+1}}) \in \mathcal{O}^*_{\mathbb{Q}_l,S} \subset \mathcal{O}^*_{K_l,S}.$$

Hence the sequence $(\eta_l)_l \in \varprojlim \mathcal{O}^*_{K_l,S}$. By theorem 13, we know p has p cyclic Massey product vanishing property.

On the other hand, $\alpha\widetilde{\alpha} = \pm p^{h_K}$. Hence,

$$\Psi^{(n-1)}([\alpha]) + \Psi^{(n-1)}([\tilde{\alpha}]) = h_K \Psi^{(n-1)}([\pm p]) = 0.$$

So $\mathrm{Im}\,\Psi^{(n-1)}$ is generated by $\Psi^{(n-1)}([\alpha])$.

We have $\Psi^{(n-1)} = 0$ if and only if $\Psi^{(n-1)}([\alpha]) = 0$ i.e. the Massey product $(\chi^{(n-1)}, \alpha)$ relative to a proper defining system vanishes by theorem 9.

□

Remark 19. Suppose we know $\lambda < p^l$ in advance. Assume $\lambda \geq n-1$, then $\lambda \geq n \Leftrightarrow n$-fold Massey product $(\chi, \chi, \cdots \chi, \alpha) = 0$ with respect to a proper defining system, where we could take $\chi : G \to \mathrm{Gal}(K_l/K) \cong \mathbb{Z}/p^l\mathbb{Z}$ instead of $\chi : G \to \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ as above. The proof is similar by using Theorem 15 instead of Theorem 14. We will use this idea to develop a numerical criterion.

5.1.2. *numerical criterion.* In this subsection, we will translate the Massey product language in the previous case 5.1.1 to numerical criterion. One is suggested to skip this subsection for the first time reading. It does not influence the reading for other cases.

Let K be an imaginary quadratic field, $p \nmid h_K$, p splits in K. Assume we know $\lambda < p$ in advance. By the remark 19, we can take $G = G_{K,S}$, $N = G_{K_1,S}$, $\chi : G \to G/N \cong \mathbb{F}_p$, $\Omega = \mathbb{F}_p[G/N]$ through this subsection. Now, we can state our numerical criterion:

(1) The Iwasawa invariant $\lambda \geq 1$, always true.
(2) The Iwasawa invariant $\lambda \geq 2 \Leftrightarrow \log_p \alpha \equiv 0 \mod p^2$, where $\log_p$ is the p-adic log.
(3) Assume $\lambda \geq 2$ is true, then $\chi \cup \alpha = 0 \Longleftrightarrow \exists \beta \in K_1^*$ s.t. $\mathrm{Nm}_{K_1/K}(\beta) = \alpha$. Define $A_1' = \prod_{i=0}^{p-1} \sigma^i(\beta^i) \in K_1^*$, where σ is the generator of the group $G/N = \mathrm{Gal}(K_1/K) \cong \mathbb{F}_p$ such that $\chi(\sigma) = 1$.
   Claim: There exists $\alpha_1 \in K^*$ s.t. $v_{\mathfrak{p}}(\alpha_1 A_1') \equiv 0 \mod p$ for all primes $\mathfrak{p}$ in K such that $\mathfrak{p} \nmid p$, where $v_{\mathfrak{p}}$ is the valuation corresponding to the prime ideal $\mathfrak{p}$.
   Then $\lambda \geq 3 \Longleftrightarrow \chi \cup \alpha_1 = 0 \Longleftrightarrow \log_p \alpha_1 \equiv 0 \mod p^2$.
(4) Assume $\lambda \geq 3$, then $\chi \cup \alpha_1 = 0 \Longleftrightarrow \exists \beta_1 \in K_1^*$ s.t. $\mathrm{Nm}_{K_1/K}(\beta_1) = \alpha_1$, Define $A_2' = \prod_{i=0}^{p-1} \sigma^i(\beta^{i(i-1)/2}) \in K_1^*$ and $B_1' = \prod_{i=0}^{p-1} \sigma^i(\beta_1^i) \in K_1^*$.
   Claim: There exists $\alpha_2 \in K^*$ s.t. $v_{\mathfrak{p}}(\alpha_2 A_2' B_1') \equiv 0 \mod p$ for all primes $\mathfrak{p}$ in K such that $\mathfrak{p} \nmid p$.
   Then $\lambda \geq 4 \Longleftrightarrow \chi \cup \alpha_2 = 0 \Longleftrightarrow \log_p \alpha_2 \equiv 0 \mod p^2$.

(5) continues in a similar way $\cdots$

In the remaining subsection, we will explain the reason for the numerical criterion. Here is the idea. To prove the Massey product relative to a proper defining system $\bar{\rho}_n : G_K \to \bar{U}_{n+1}(\mathbb{F}_p), n \leq p$ vanishes,

$$\bar{\rho}_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

we would like to construct the cochain ψ_{n-1} explicitly to fill the $*$ spot. We first construct ψ'_{n-1} when we view the Massey product over $G_K = \mathrm{Gal}(K^{sep}/K)$ instead of $G_{K,S}$. In this case, it does not matter if we assume that K has p-th root of units. Hence, we can exploit the classical results and generalize them. Then we compare the Massey product when we view it over G_K and $G_{K,S}$ differently. The difference of ψ_{n-1} and ψ'_{n-1} is an element α_{n-1} in K. Finally, to check the Massey product is zero over $G_{K,S}$, we restrict the Massey product to $G_{K_{\mathfrak{p}_0}}$, where $K_{\mathfrak{p}_0}$ is the completion of K at prime $\mathfrak{p}_0$.

Next, we introduce some classical results. Let K be any field (not necessarily a number field) such that $char(K) \neq p$. Let $G_K = \mathrm{Gal}(K^{sep}/K)$ be the absolute Galois group. Let ζ_p be the p-th root of the unit. Then $[K(\zeta_p) : K]$ has degree which is prime to p. Hence

$$Cor \circ Res : H^i(G_K, \mu_p) \to H^i(G_{K(\zeta_p)}, \mu_p) \to H^i(G_K, \mu_p)$$

is an isomorphism. Therefore, $Res : H^i(G_K, \mu_p) \to H^i(G_{K(\zeta_p)}, \mu_p)$ is an injective map. To consider the Massey product relative to certain defining system vanishing in $H^2(G_K, \mu_p)$, we just need to restrict all cochains to $G_{K(\zeta_p)}$ and consider the Massey product vanishing inside $H^2(G_{K(\zeta_p)}, \mu_p)$. It does not matter if we assume $\zeta_p \in K$. Now we can assume that $\zeta_p \in K$. In other words, the action G_K on μ_p is trivial. We can view μ_p as $\mathbb{F}_p$ by identifying $\zeta_p \in \mu_p$ with $1 \in \mathbb{F}_p$.

As mentioned before, to give a defining system is the same to give a homomorphism $\bar{\rho} : G_K \to \bar{U}_{n+1}(\mu_p) = \bar{U}_{n+1}(\mathbb{F}_p)$. The Massey product vanishing is equivalent to that $\bar{\rho}$ can be lifted to a homomorphism $\rho : G_K \to U_{n+1}(\mu_p)$. Let $K_{\bar{\rho}}$ be the subfield fixed by $\ker \bar{\rho}$. Then the Massey product $(\chi_1, \chi_2, \cdots, \chi_n)_{\bar{\rho}}$ vanishing is equivalent to that we can extend the Galois extension $K_{\bar{\rho}}/K$ to a Galois extension K_ρ/K such that

$$\begin{array}{ccc} \mathrm{Gal}(K_\rho/K) & \hookrightarrow & U_{n+1}(\mu_p) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K_{\bar{\rho}}/K) & \hookrightarrow & \bar{U}_{n+1}(\mu_p) \end{array}$$

is commutative.

To understand this better, we first consider 2-fold Massey products i.e. cup products. Let a, b be two linearly independent elements in $K^*/(K^*)^p$ corresponding to $\chi_a, \chi_b \in H^1(G_K, \mu_p) \cong K^*/(K^*)^p$. Then $K(a^{1/p})$ is the subfield fixed by group $\ker \chi_a$ and $K(b^{1/p})$ is the subfield fixed by group of $\ker \chi_b$. The cup product $\chi_a \cup$

$\chi_b = 0$ is equivalent that $\exists \beta \in K(a^{1/p})$ such that $\mathrm{Nm}_{K(a^{1/p})/K}(\beta) = b$. Translating in the language of Massey product, we have a defining system

$$\bar{\rho} : G_K \to \bar{U}_3(\mu_p) \cong \mathbb{F}_p \oplus \mathbb{F}_p, \sigma \to (\chi_a(\sigma), \chi_b(\sigma))$$

The 2-fold Massey product vanishing is equivalent to that we can extend the Galois extension $K(a^{1/p}, b^{1/p})/K$ to a Heisenberg extension $K(a^{1/p}, b^{1/p}, A^{1/p})/K$ such that $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A^{1/p})/K) \cong U_3(\mathbb{F}_p)$. This is a theorem proved by Romyar Sharifi[Sha99]. Another reference is [MT16]:

Theorem 22 (Sharifi)**.** *The same notation as before. Assume $\chi_a \cup \chi_b = 0$. Let $A_1 = \prod_{i=0}^{p-1} \sigma^i(\beta^i)$ where σ is a generator of $\mathrm{Gal}(K(a^{1/p}/K)$ such that $\chi(\sigma) = 1$, then $\sigma(A_1) = A_1 \frac{\beta^p}{b}$.*

Theorem 23 (Sharifi)**.** *The same notation as before. Assume $\chi_a \cup \chi_b = 0$. Let $A = fA_1$ where $f \in K^*$, then the homomorphism*

$$\bar{\rho} : G_K \to \bar{U}_3(\mu_p) \cong \mathbb{F}_p \oplus \mathbb{F}_p, \sigma \to (\chi_a(\sigma), \chi_b(\sigma))$$

can be lifted to a Heisenberg extension $\rho : G_K \to U_3(\mu_p)$ such that $Res_{\ker \chi_a}(\rho_{1,3}) = \chi_A$.

Remark 20. When we have another lifting corresponding to A', the difference between A and A' is an element in K^*. If we have another lifting ρ', then $-d\rho_{1,3} = \chi_a \cup \chi_b$ and $-d\rho'_{1,3} = \chi_a \cup \chi_b$. So $d(\rho_{1,3} - \rho'_{1,3}) = 0$. Hence $\rho_{1,3} - \rho'_{1,3}$ is a cocycle in $\mathcal{C}^1$. There exists $f \in K$ such that $\rho_{1,3} - \rho'_{1,3} = \chi_f$. We have $A = fA'$ up to multiplication by an element of $K(a^{1/p})^{*p}$.

The theorem gives us an explicit description of $\rho_{1,3}$. And the converse is also true. If we can find such Heisenberg extension $K(a^{1/p}, b^{1/p}, A^{1/p})/K$ then the cup product $\chi_a \cup \chi_b$ is zero.

Now, we generalize the idea to give a similar description for Massey product $(\chi^{(n)}, \psi_0)$ relative to a proper defining system $\bar{\rho}_{n+1} : G_K \to \bar{U}_{n+2}(\mathbb{F}_p)$.

Because we use the proper defining system, the $\mathrm{Im}\,\bar{\rho}_{n+1}$ is not the whole group $\bar{U}_{n+2}(\mathbb{F}_p)$. We need the following definition and lemma to describe $\mathrm{Im}\,\bar{\rho}_{n+1}$.

Definition 3. Define group $M_n :=< s, t_0, t_1, \cdots, t_n \mid s^p = 1, t_0^p = 1, t_1^p = 1, \cdots, t_n^p = 1, t_i t_j t_i^{-1} t_j^{-1} = 1, st_0 s^{-1} t_0^{-1} = t_1, st_1 s^{-1} t_1^{-1} = t_2, st_2 s^{-1} t_2^{-1} = t_3, \cdots, st_{n-1} s^{-1} t_{n-1}^{-1} = t_n, st_n s^{-1} t_n^{-1} = 1 >$ for $n < p$.

Remark 21. One can check that M_n is a semidirect product. We have $M_n \cong \mathbb{F}_p \ltimes \mathbb{F}_p^{n+1}$, where $\mathbb{F}_p =< s >$ and $\mathbb{F}_p^{n+1} =< t_0, t_1, \cdots, t_n >$.

Lemma 24. *Let $\rho_{n+1} : G_K \to U_{n+2}(\mathbb{F}_p)$ be the homomorphism defined by*

$$\rho_{n+1} = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \psi_n \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $\ker\chi \neq \ker\psi_0$. *Then* $\operatorname{Im}\rho_{n+1}$ *is isomorphic to* M_n. *If we view* $\operatorname{Im}\rho_{n+1} \subset U_{n+2}(\mathbb{F}_p)$ *as a subgroup, then we can take*

$$s = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, t_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$t_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \cdots, t_n = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Proof. Since $\ker\chi \neq \ker\psi_0$, $[G_K : \ker\chi] = p$ and $[G_K : \ker\psi_0] = p$, so $\ker\chi$ and $\ker\psi_0$ do not contain each other. Hence $\operatorname{Im}\rho_{n+1}$ contains

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \cdots & * \\ 0 & 1 & 1 & 0 & 0 & 0 & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 1 & 0 & * \\ 0 & 0 & 0 & 0 & 1 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, B_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & * \\ 0 & 1 & 0 & 0 & 0 & 0 & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 1 & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

One can define $B_1 = AB_0A^{-1}B_0^{-1}, \cdots, B_n = AB_{n-1}A^{-1}B_{n-1}^{-1}$. We can directly map s to A and t_0 to B_0. This gives us an isomorphism between M_n and ρ_{n+1}. To check the group relations, it is a trivial matrix calculation. One can show B_i are linearly independent, and the two groups have the same size. The proof of isomorphism is only a tedious calculation. We omit the calculation here.

On the other hand, we can use A, B_0 to generate the following matrices:

$$t_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \cdots, t_n = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This gives us the description of $\operatorname{Im}\rho_{n+1}$ as in the lemma. □

Remark 22. If we take subgroup $V_{n+1} \subset U_{n+2}(\mathbb{F}_p)$ whose elements are of the form:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \cdots & * \\ 0 & 1 & 0 & 0 & 0 & 0 & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 1 & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

then we have an exact sequence,

$$0 \to V_{n+1} \to \operatorname{Im} \rho_{n+1} \to \operatorname{Im} \rho_{n+1}/V_{n+1} \to 0$$

Easy to see that $V_{n+1} \cong \mathbb{F}_p^{n+1}$ is generated by $t_0, t_1, \cdots, t_n$ and $\operatorname{Im} \rho_{n+1}/V_{n+1} \cong \mathbb{F}_p$ is generated by s. And $\operatorname{Im} \rho_{n+1} \cong \mathbb{F}_p \ltimes V_{n+1}$. Hence, to describe the presentation of $\operatorname{Im} \rho_{n+1}$, all we need is to describe the presentations of V_{n+1} and $\mathbb{F}_p$ and the action of $\mathbb{F}_p$ on V_{n+1}. These are how we define M_n.

Remark 23. By the lemma 24, if we can find a Galois extension L/K such that $\operatorname{Gal}(L/K) \cong M_n$, then we can determine a proper defining system $\bar{\rho}_{n+2} : G_K \to \bar{U}_{n+3}$. And the converse is also true.

To determine whether a group is isomorphic to M_n, we only need to determine what elements are mapped to s, t_0 and check all relations if we know the group has the same size as M_n.

As before, Assume K is a field that contains p-th root of the unit. Let $\chi \in H^1(G_K, \mu_p) \cong \operatorname{Hom}(G_K, \mathbb{F}_p)$ and $\psi_0 \in H^1(G_K, \mu_p) \cong \operatorname{Hom}(G_K, \mathbb{F}_p)$. Let $K(a^{1/p})$ be the fixed subfield of $\ker \chi$ and $K(b^{1/p})$ be the fixed subfield of $\ker \psi_0$ and assume they are different field. Let σ_a and σ_b be the generator of $\operatorname{Gal}(K(a^{1/p}, b^{1/p})/K)$ such that

$$\sigma_a(a^{1/p}) = \zeta_p a^{1/p} \qquad \sigma_a(b^{1/p}) = b^{1/p}$$
$$\sigma_b(a^{1/p}) = a^{1/p} \qquad \sigma_b(b^{1/p}) = \zeta_p b^{1/p}$$

Lemma 25. *Assume $\chi \cup \psi_0 = 0$,i.e. there exists $\beta \in K(a^{1/p})$ such that $\operatorname{Nm}_{K(a^{1/p})/K}(\beta) = b$. Define*

$$A_1 = \prod_{i=0}^{p-1} \sigma_a^i(\beta^i), A_2 = \prod_{i=0}^{p-1} \sigma_a^i(\beta^{\frac{i(i-1)}{2}}), A_3 = \prod_{i=0}^{p-1} \sigma_a^i(\beta^{\frac{i(i-1)(i-2)}{6}}), \cdots, A_n = \prod_{i=0}^{p-1} \sigma_a^i(\beta^{\binom{i}{n}})$$

where $n < p$, Then

$$\frac{\sigma_a(A_1)}{A_1} b = \beta^p, \frac{\sigma_a(A_2)}{A_2} \sigma_a(A_1) = \beta^{\frac{p(p-1)}{2}}, \cdots, \frac{\sigma_a(A_n)}{A_n} \sigma_a(A_{n-1}) = \beta^{\binom{p}{n}}$$

Proof. Easy to check the following equation:

$$(\sigma_a - 1)(\sum_{i=0}^{p-1} i\sigma_a^i) + \sum_{i=0}^{p-1} \sigma_a^i = p$$

$$(\sigma_a - 1)(\sum_{i=0}^{p-1} \frac{i(i-1)}{2} \sigma_a^i) + \sigma_a \sum_{i=0}^{p-1} i\sigma_a^i = \frac{p(p-1)}{2}$$

$$\cdots$$

$$(\sigma_a - 1)(\sum_{i=0}^{p-1} \binom{i}{n} \sigma_a^i) + \sigma_a \sum_{i=0}^{p-1} \binom{i}{n-1} \sigma_a^i = \binom{p}{n}$$

□

Lemma 26. *Notations as before and $n < p$, then the field extension*

$$K(a^{1/p}, b^{1/p}, A_1^{1/p}, A_2^{1/p}, \cdots, A_n^{1/p})/K$$

is a Galois extension. And

$$\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p}, A_2^{1/p}, \cdots, A_n^{1/p})/K) \cong M_n.$$

Therefore, it corresponds a proper defining system $\bar{\rho}_{n+2} : G_K \to \bar{U}_{n+3}$. And $Res_{\ker \chi} \psi_i = \chi_{A_i}$ for $1 \leq i \leq n \leq p-1$.

Proof. We have

$$\sigma_a(A_1)/A_1 = \beta^p/b \in K(a^{1/p}, b^{1/p})^{*p}$$

and

$$\sigma_b(A_1)/A_1 = 1 \in K(a^{1/p}, b^{1/p})^{*p}.$$

Hence $K(a^{1/p}, b^{1/p}, A_1^{1/p})/K$ is a Galois extension.

Lift σ_a and σ_b to $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K)$. We denote them as $\widetilde{\sigma}_a$ and $\widetilde{\sigma}_b$.

As said in remark 23, to prove $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K) \cong M_1$, we only need to determine what is mapped to s, t_0 and check that it satisfies the relations in the presentation of group M_1. Lift σ_a and σ_b to $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K)$ since two groups obviously have the same size. We denote them as $\widetilde{\sigma}_a$ and $\widetilde{\sigma}_b$. We would like to map $\widetilde{\sigma}_a$, $\widetilde{\sigma}_b$ to s, t_0 respectively. Next, we will check it satisfies the relations.

By lemma 25,

$$\widetilde{\sigma}_a(A_1^{1/p}) = \zeta_p^{j_1} A_1^{1/p} \beta/b^{1/p} \tag{3}$$

for some $j_1 \in \mathbb{F}_p$. Then

$$\widetilde{\sigma}_a^2(A_1^{1/p}) = \zeta_p^{j_1} A_1^{1/p} \beta/b^{1/p} \zeta_p^{j_1} \widetilde{\sigma}_a(\beta)/b^{1/p}$$

$$\cdots$$

$$\widetilde{\sigma}_a^p(A_1^{1/p}) = \zeta_p^{j_1 p} A_1^{1/p} \,\mathrm{Nm}(\beta)/b = A_1^{1/p}$$

Hence $\widetilde{\sigma}_a^p = 1$.

We have $\widetilde{\sigma}_b(A_1^{1/p}) = \zeta_p^{i_1} A_1^{1/p}$ for some $i_1 \in \mathbb{F}_p$. Hence $\widetilde{\sigma}_b^p(A_1^{1/p}) = A_1^{1/p}$. So $\widetilde{\sigma}_b^p = 1$.

We have

$$\widetilde{\sigma}_a \widetilde{\sigma}_b(A_1^{1/p}) = \widetilde{\sigma}_a(\zeta_p^i A_1^{1/p}) = \zeta_p^{i_1 + j_1} A_1^{1/p} \beta/b^{1/p}$$

$$\widetilde{\sigma}_b \widetilde{\sigma}_a(A_1^{1/p}) = \widetilde{\sigma}_b(\zeta_p^{j_1} A_1^{1/p} \beta/b^{1/p}) = \zeta_p^{j_1 + i_1 - 1} A_1^{1/p} \beta/b^{1/p}$$

$$\widetilde{\sigma}_a \widetilde{\sigma}_b \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_b^{-1}(A_1^{1/p}) = \zeta_p A_1^{1/p}$$

Define $\widetilde{\sigma}_{A_1} = \widetilde{\sigma}_a \widetilde{\sigma}_b \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_b^{-1}$. We have

$$\widetilde{\sigma}_{A_1}^p = 1, \widetilde{\sigma}_a \widetilde{\sigma}_{A_1} \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_{A_1}^{-1} = 1, \widetilde{\sigma}_b \widetilde{\sigma}_{A_1} \widetilde{\sigma}_b^{-1} \widetilde{\sigma}_{A_1}^{-1} = 1$$

Hence, $\widetilde{\sigma}_{A_1}$ plays the role t_1 in the presentation of M_1 and we checked that the relations are satisfied. Therefore, we have $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K) \cong M_1$. And $G_K \to \mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K) \cong M_1 \subset U_3(\mathbb{F}_p)$ gives us $Res_{\ker \chi} \psi_1 = \chi_{A_1}$.

For next step: Similarly, we have

$$\widetilde{\sigma}_a(A_2)/A_2 = \beta^{p(p-1)/2}/\widetilde{\sigma}_a(A_1) = \beta^{p(p-1)/2}b/(A_1\beta^p) \in K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p}$$

and

$$\widetilde{\sigma}_b(A_2)/A_2 = 1 \in K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p}.$$

And we know from last paragraph, $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K)$ is generated by $\widetilde{\sigma}_a, \widetilde{\sigma}_b$. Hence for any $\sigma \in \mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K)$, we have $\sigma(A_2)/A_2 \in K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p}$. Therefore, $K(a^{1/p}, b^{1/p}, A_1^{1/p}, A_2^{1/p})/K$ is a Galois extension.

Lift $\widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_{A_1}$ to $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p}, A_2^{1/p})/K)$. And we still denote the lifting as $\widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_{A_1}$ by a little abusing notation. Similarly, we will check that $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ are mapped to $s, t_0 \in M_2$ and they satisfy the relations in the definition of M_2.

By lemma 25

$$\widetilde{\sigma}_a(A_2^{1/p}) = \zeta_p^{j_2} A_2^{1/p} b^{1/p} \beta^{\frac{p-3}{2}} / A_1^{1/p}$$

for some $j_2 \in \mathbb{F}_p$. By equation (3), we have

$$\prod_{i=0}^{p-1} \widetilde{\sigma}_a^i(A_1^{1/p}) = A_1 \prod_{i=0}^{p-1} \widetilde{\sigma}_a^i(\beta^{p-1-i})/b^{\frac{p-1}{2}} = b^{\frac{p-1}{2}}$$

$$\widetilde{\sigma}_a^p(A_2^{1/p}) = A_2^{1/p} b \prod_{i=0}^{p-1} \widetilde{\sigma}_a^i(\beta^{\frac{p-3}{2}}) / \prod_{i=0}^{p-1} \widetilde{\sigma}_a^i(A_1^{1/p}) = A_2^{1/p}$$

Hence $\widetilde{\sigma}_a^p = 1$.

We have $\widetilde{\sigma}_b(A_2) = A_2$, so $\widetilde{\sigma}_b(A_2^{1/p}) = \zeta_p^{i_2} A_2^{1/p}$ for some $i_2 \in \mathbb{F}_p$. So $\widetilde{\sigma}_b^p = 1$

We have

$$\widetilde{\sigma}_a^{-1}(A_2^{1/p}) = \zeta_p^{-j_2-j_1} A_2^{1/p} A_1^{1/p} / \widetilde{\sigma}_a^{-1}(\beta^{\frac{p-1}{2}})$$

$$\widetilde{\sigma}_b^{-1}(A_2^{1/p}) = \zeta_p^{-i_2} A_2^{1/p}$$

$$\widetilde{\sigma}_{A_1}(A_2^{1/p}) = \widetilde{\sigma}_a \widetilde{\sigma}_b \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_b^{-1}(A_2^{1/p}) = \zeta_p^{i_1} A_2^{1/p}$$

Hence $\widetilde{\sigma}_{A_1}^p = 1$.

$$\widetilde{\sigma}_a \widetilde{\sigma}_{A_1} \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_{A_1}^{-1}(A_2^{1/p}) = \zeta_p A_2^{1/p}$$

Define $\widetilde{\sigma}_{A_2} = \widetilde{\sigma}_a \widetilde{\sigma}_{A_1} \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_{A_1}^{-1}$. Then $\widetilde{\sigma}_{A_2}^p = 1$. And one can check

$$\widetilde{\sigma}_a \widetilde{\sigma}_{A_2} \widetilde{\sigma}_a^{-1} \widetilde{\sigma}_{A_2}^{-1} = 1, \widetilde{\sigma}_b \widetilde{\sigma}_{A_2} \widetilde{\sigma}_b^{-1} \widetilde{\sigma}_{A_2}^{-1} = 1, \widetilde{\sigma}_{A_1} \widetilde{\sigma}_{A_2} \widetilde{\sigma}_{A_1}^{-1} \widetilde{\sigma}_{A_2}^{-1} = 1$$

These imply that $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ satisfies the relations in the definition of M_2. And $\widetilde{\sigma}_{A_1}, \widetilde{\sigma}_{A_2}$ plays the role as t_1, t_2. Hence we have an isomorphism $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p}, A_2^{1/p})/K) \cong M_2$. It determines a proper defining system $G_K \to \mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p}, A_2^{1/p})/K) \cong M_2 \subset U_4(\mathbb{F}_p) \subset \bar{U}_5(\mathbb{F}_p)$. And $Res_{\ker \chi} \psi_2 = \chi_{A_2}$.

The general case can be checked by a similar process, and the calculation is tedious. We omit it here.

□

Remark 24. The proof for the case M_1 is the same as the proof of theorem 23 in [MT16] and [Sha99]. We just imitate the proof and get the generalized result. But the calculation becomes more and more tedious.

Now, if we have $\chi \cup \psi_0 = 0$, we can construct a Galois field extension and it corresponds to a proper defining system. How do we get all proper defining systems? We need the following definition and lemma.

Definition 4. The proper defining system we get by the way in Lemma 26 is called the standard proper defining system.

By previous lemmas, fix χ and ψ_0, the standard proper defining system depends on the choice of a, b, β and choices of the lifting of σ_a and σ_b.

Lemma 27. *All proper defining systems with respect to χ can be obtained from the standard proper defining system by operations in lemma 8 and remark 11.*

Proof. Assume we have a proper defining system $\bar{\rho}_n : G_K \to \bar{U}_{n+1}(\mathbb{F}_p), n \leq p$.

$$\bar{\rho}_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Then $\chi \cup \psi_0 = 0$. By lemma 26, we can get a standard proper defining system:

$$\bar{\rho}'_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi'_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi'_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi'_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi'_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where $\psi_0 = \psi'_0$. Assume $\psi_i = \psi'_i$ for $0 \leq i \leq m$. Then by lemma 8

$$\begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \cdots & \psi'_{n-2} - \psi_{n-2} \\ \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ \cdots & 0 & 1 & \chi & \binom{\chi}{2} & \cdots & \binom{\chi}{m+1} & \psi'_{m+1} - \psi_{m+1} \\ 0 & \cdots & 0 & 1 & \chi & \cdots & \binom{\chi}{m} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \chi & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

is a proper defining system that is induced by the following defining system:

$$\begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi'_{n-2} - \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi'_{m+3} - \psi_{m+3} \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi'_{m+2} - \psi_{m+2} \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi'_{m+1} - \psi_{m+1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

It has a smaller size. Continuing similarly, we can see that the standard proper defining system can generate all proper defining systems by operations in lemma 8 and remark 11.

□

In the lemma 26, we can construct a standard proper defining system from a field extension. Conversely, we can get a field extension from a proper defining system.

Lemma 28. *Given a proper defining system $\bar{\rho}_n : G_K \to \bar{U}_{n+1}$, the fixed subfield by $\ker \bar{\rho}_n$ can be written in the form*

$$K\left(\begin{array}{c} a^{1/p}, b_0^{1/p}, (A_{0,1}b_1)^{1/p}, (A_{0,2}A_{1,1}b_2)^{1/p}, (A_{0,3}A_{1,2}A_{2,1}b_3)^{1/p}, \\ \cdots, (A_{0,n-2}A_{1,n-3}\cdots A_{n-2,1}b_{n-2})^{1/p} \end{array} \right)$$

where $a, b_0, b_1, \cdots, b_{n-2} \in K$ and there exist $\beta_i \in K(a^{1/p})$ satisfying that $\mathrm{Nm}_{K(a^{1/p})/K}(\beta_i) = b_i$ for $0 \le i \le n-3$ and $A_{i,j} := \prod_{k=0}^{p-1} \sigma_a^k(\beta_i^{\binom{k}{j}})$

Proof. The result directly follows from lemma 27 by using the correspondence between the standard proper defining system and M_n-field extension.

Another method to check the lemma is by using the same method in the proof of lemma 26. Check that the field extension is Galois extension and $\widetilde{\sigma}_a$ and $\widetilde{\sigma}_{b_0}$ are generators of M_n and satisfy the relations and have the same size. The calculation will become tedious; we omit it here. □

Now, back to our case that K is a number field. Instead consider the group $G_K = \mathrm{Gal}(K^{sep}/K)$, we consider the group $G_{K,S} = \mathrm{Gal}(K^S/K)$. For a defining system $\bar{\rho}_n : G_{K,S} \to \bar{U}_{n+1}$, the subfield L fixed by $\ker \bar{\rho}_n$ is a field extension that is unramified outside S. Conversely, if we have a field extension L/K that is unramified outside S and $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of $\bar{U}_{n+1}$, then we have a defining system $\bar{\rho}_n : G_{K,S} \to \mathrm{Gal}(L/K) \subset \bar{U}_{n+1}$. We need the following known fact.

Lemma 29. *Let K be a number field containing p-th root of the unit. Let $a \in K^*$ and $\mathfrak{p}$ be a prime that does not divide p, then $K(a^{1/p})/K$ is unramified at $\mathfrak{p}$ if and only if the valuation $v_{\mathfrak{p}}(a) \equiv 0 \mod p$*

Now, we apply all we have to the case 5.1.1 where K is an imaginary quadratic field and p splits in K and the size of the class group h_K is prime to p. Notations as the beginning of case 5.1.1 and the beginning of this subsection 5.1.2, recall that the character χ is $G_{K,S} \to \mathrm{Gal}(K_1/K) \cong \mathbb{F}_p$ where $K_1 = K\mathbb{Q}_1$.

Here is a reminder that in the previous, we assume $\zeta_p \in K$. To determine when the Massey product relative to a certain defining system vanishes in $H^2(G_K, \mu_p)$, we can restrict all cochains to $G_{K(\zeta_p)}$ and consider the Massey product vanishing

inside $H^2(G_{K(\zeta_p)}, \mu_p)$. Hence, we may apply previous results if we only care about when the Massey products vanish.

Lemma 30. *Let $\psi_0 \in H^1(G_{K,S}, \mu_p) \cong K^* \cap K_S^{*p}/K^{*p}$ correspond $\alpha \in K^* \cap K_S^{*p}/K^{*p}$. Then $\chi \cup \psi_0 = 0$ if and only if that $\log_p(\alpha) \equiv 0 \mod p^2$ where $\log_p$ is the p-adic log.*

Proof. Let $p\mathcal{O}_K = \mathfrak{p}_0\widetilde{\mathfrak{p}}_0$ and $p\mathcal{O}_{K_1} = \mathfrak{p}_1\widetilde{\mathfrak{p}}_1$. Let $K_{\mathfrak{p}_0}$ and $K_{\widetilde{\mathfrak{p}}_0}$ be the completion of K at prime $\mathfrak{p}_0$ and $\widetilde{\mathfrak{p}}_0$ respectively. Similarly for the definition $K_{1,\mathfrak{p}_1}$ and $K_{1,\widetilde{\mathfrak{p}}_1}$. We will use Poitou-Tate Duality which is the theorem 8.6.7 in [NSW08]. We use the same notation as in chapter 8.6 of [NSW08]. Take $A = \mu_p$, then $A' = \mathrm{Hom}(\mu_p, \mathcal{O}_S^*) \cong \mathbb{F}_p$ as $G_{K,S}$ module. Lemma 8.6.3 in [NSW08] tells us $Ш^1(G_{K,S}, \mathbb{F}_p) \cong \mathrm{Hom}(\mathrm{Cl}_S(K), \mathbb{F}_p) = 0$. By theorem 8.6.7 in [NSW08], We have $Ш^2(G_{K,S}, \mu_p) \cong Ш^1(G_{K,S}, \mathbb{F}_p)^\vee = 0$. This implies that the map $H^2(G_{K,S}, \mu_p) \to H^2(G_{K_{\mathfrak{p}_0}}, \mu_p) \oplus H^2(G_{K_{\widetilde{\mathfrak{p}}_0}}, \mu_p)$ is injective. The cup product $\chi \cup \psi_0$ vanishes in $H^2(G_{K,S}, \mu_p)$ if and only if $Res\chi \cup Res\psi_0$ vanishes both in $H^2(G_{K_{\mathfrak{p}_0}}, \mu_p)$ and $H^2(G_{K_{\widetilde{\mathfrak{p}}_0}}, \mu_p)$. In local field $K_{\mathfrak{p}_0}$, $\chi \cup \psi_0$ vanishes if and only if $\alpha \in \mathrm{Nm}_{K_{1,\mathfrak{p}_1}/K_{\mathfrak{p}_0}}(K_{1,\mathfrak{p}_1}^*)$. One can check that $K_{\mathfrak{p}_0} = \mathbb{Q}_p$ and $K_{1,\mathfrak{p}_1} = \mathbb{Q}_{1,p}$ which is the completion of $\mathbb{Q}_1$ at p. And $\mathbb{Q}_{1,p}/\mathbb{Q}_p$ is totally ramified degree p extension. We can decompose $\mathbb{Q}_p^* = p^{\mathbb{Z}} \oplus \mathbb{F}_p^* \oplus (1 + p\mathbb{Z}_p)$ since p is odd and $\mathbb{Z}_p^* \cong \mathbb{F}_p^* \oplus (1 + p\mathbb{Z}_p) \cong \mathbb{F}_p^* \oplus \mathbb{Z}_p$ is given by $t \to (t \mod p, \log_p(t)/\log_p(1+p))$. By local class field theory, we have $\mathrm{Nm}_{K_{1,\mathfrak{p}_1}/K_{\mathfrak{p}_0}}(K_{1,\mathfrak{p}_1}^*) \cong \mathbb{Z} \oplus \mathbb{F}_p^* \oplus (1 + p^2\mathbb{Z}_p)$ as a subgroup of $\mathbb{Q}_p^*$. We have $\alpha \in \mathrm{Nm}_{K_{1,\mathfrak{p}_1}/K_{\mathfrak{p}_0}}(K_{1,\mathfrak{p}_1}^*)$ if and only if $\log_p(\alpha) = 0 \mod p^2$. And similar story happened when we complete at $\widetilde{\mathfrak{p}}_0$. Hence $\log_p(\alpha) = 0 \mod p^2$ if and only if $\chi \cup \psi_0 = 0$

□

Remark 25. The value $\log_p \alpha$ depends on the embedding $K \to \mathbb{Q}_p^{sep}$. But the criterion $\log_p(\alpha) \equiv 0 \mod p^2$ does not depend on the embedding. In fact, by kummer exact sequence (1) and $p \nmid h_K$, we can write $\alpha = \mu\beta^p$ for $\mu \in \mathcal{O}_{K,S}^*$ and $\beta \in K^*$. Then $\mathrm{Nm}_{K/\mathbb{Q}}(\mu) = p^m$ for some integer m up to a root of the unity, which is killed by p-adic logarithm. For two different embeddings $\iota_{\mathfrak{p}}, \iota_{\bar{\mathfrak{p}}} : K \to \mathbb{Q}_p^{sep}$, we have

$$\log_p(\iota_{\mathfrak{p}}(\alpha)) + \log_p(\iota_{\bar{\mathfrak{p}}}(\alpha)) = \log_p(\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)) \equiv 0 \mod p^2.$$

Hence, the criterion $\log_p(\alpha) \equiv 0 \mod p^2$ does not depend on the embedding.

Here is the relation between our result and the classical result Gold criterion [Gol74]

Theorem 31. *Let K be an imaginary quadratic field, $p \nmid h_K$, p splits in K i.e. $p\mathcal{O}_K = \mathfrak{p}_0\widetilde{\mathfrak{p}_0}$. Take $(\alpha) = \mathfrak{p}_0^{h_K}$, then $\lambda \geq 2 \Leftrightarrow$ the cup product $\chi \cup \alpha = 0 \Leftrightarrow \log_p(\alpha) \equiv 0 \mod p^2 \Leftrightarrow \alpha^{p-1} \equiv 1 \mod \widetilde{\mathfrak{p}}_0^2$ where $\log_p$ is p-adic log.*

Proof. We only need to prove the last equivalent relation. Complete K at $\widetilde{\mathfrak{p}}_0$, We have $K_{\widetilde{\mathfrak{p}}_0} \cong \mathbb{Q}_p$ and $\alpha \in \mathbb{Z}_p^* \cong \mathbb{F}_p^* \oplus 1 + p\mathbb{Z}_p$. And $\log_p(\alpha) \equiv 0 \mod p^2 \iff \alpha \in \mathbb{F}_p^* \oplus 1 + p^2\mathbb{Z}_p \iff \alpha^{p-1} \equiv 1 \mod p^2$ in $\mathbb{Q}_p \iff \alpha^{p-1} \equiv 1 \mod \widetilde{\mathfrak{p}}_0^2$ in K. □

Let $\bar{\rho}_n : G_{K,S} \to \bar{U}_{n+1}$ be a proper defining system.

$$\bar{\rho}_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & * \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

When restricted on $G_{K_1,S} = \ker \chi$, the cochain $\psi_i \in \mathcal{C}^1(G_{K,S}, \mu_p)$ becomes a cocycle in $\mathcal{C}^1(G_{K_1,S}, \mu_p)$. So $Res_{G_{K_1,S}}\psi_i$ corresponds to a cocycle $(\sigma \to \sigma(A_i^{1/p})/A_i^{1/p})$ for some $A_i \in K_1^* \cap K_S^{*p}$ and the cocycle depends on the choice of $A_i^{1/p}$ since we do not have $\mu_p \in K$. Assume that the Massey product relative to a proper defining system $\bar{\rho}_n : G_{K,S} \to \bar{U}_{n+1}$ vanishes, i.e. there exists a cochain $\psi_{n-1} \in \mathcal{C}^1(G_{K,S}, \mu_p)$ fitting in the lifting $\rho_n : G_{K,S} \to U_{n+1}$.

$$\rho_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \psi_{n-1} \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Similarly, $Res_{G_{K_1,S}}\psi_{n-1}$ is a cocycle and corresponds to a element $A_{n-1} \in K_1^* \cap K_S^{*p}$. Let $\bar{\rho}'_n : G_K \to G_{K,S} \xrightarrow{\bar{\rho}_n} \bar{U}_{n+1}$ be the composition of $G_K \to G_{K,S}$ and $\bar{\rho}_n$. Then $\bar{\rho}'_n$ is a proper defining system over G_K. Then the Massey product relative to $\bar{\rho}'_n$ also vanishes. Then there exists a cochain $\psi'_{n-1} : G_K \to \mu_p$ fitting in the cochain $\rho'_n : G_K \to U_{n+1}$.

$$\rho'_n = \begin{bmatrix} 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \binom{\chi}{4} & \cdots & \psi'_{n-1} \\ 0 & 1 & \chi & \binom{\chi}{2} & \binom{\chi}{3} & \cdots & \psi_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & \chi & \binom{\chi}{2} & \psi_2 \\ 0 & 0 & 0 & 0 & 1 & \chi & \psi_1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \psi_0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

And $Res_{G_{K_1}}\psi'_{n-1}$ is a cocycle in $\mathcal{C}^1(G_{K_1}, \mu_p)$ and corresponds to $A'_{n-1} \in K_1^*$. By definition of Massey product, we have $d(\psi'_{n-1} - \psi_{n-1}) = 0$. Hence $\psi'_{n-1} - \psi_{n-1}$ is a cocycle in $\mathcal{C}^1(G_K, \mu_p)$ which corresponds to $\sigma \to \frac{\sigma(f^{1/p})}{f^{1/p}}$ for some $f \in K^*$. When restricting on G_{K_1}, we have $fA_{n-1} = A'_{n-1}$. We remark here that we have to choose the p-th root of A_{n-1}, A'_{n-1}, f properly so that cocycles are compatible. A different choice of p-th root of A_i changes the corresponding cocycle a multiple of $(\sigma \to \frac{\sigma(\zeta_p)}{\zeta_p})$. And $\chi \cup (\sigma \to \frac{\sigma(\zeta_p)}{\zeta_p}) = 0$. For our case now, we care about when the Massey products vanish. Therefore, we do not need to care too much about the choice of the p-th root of the element. For our purpose, the key is that there exists

$f \in K^*$ such that $fA_{n-1} = A'_{n-1}$ where $A_{n-1} \in K_1^* \cap K_S^{*p}$ and $A'_{n-1} \in K_1^*$. By lemma 29, we have an element $A \in K_1^* \cap K_S^{*p}$ if and only if the valuation $v_{\mathfrak{p}}(A) \equiv 0 \mod p$ where $\mathfrak{p}$ does not divide p.

Now we combine all we have and explain how our numerical criterion works:

(1) The Iwasawa invariant $\lambda \geq 1$, always true.
(2) The Iwasawa invariant $\lambda \geq 2 \Leftrightarrow \log_p \alpha \equiv 0 \mod p^2$, where $\log_p$ is the p-adic log (Reason: lemma 30).
(3) Assume $\lambda \geq 2$ is true, then $\chi \cup \alpha = 0 \Longleftrightarrow \exists \beta \in K_1^*$ s.t. $\mathrm{Nm}_{K_1/K}(\beta) = \alpha$. Define $A'_1 = \prod_{i=0}^{p-1} \sigma^i(\beta^i) \in K_1^*$, where σ is the generator of the group $G/N = \mathrm{Gal}(K_1/K) \cong \mathbb{F}_p$

    Claim: There exists $\alpha_1 \in K^*$ s.t. $v_{\mathfrak{p}}(\alpha_1 A'_1) \equiv 0 \mod p$ for all $\mathfrak{p} \nmid p$, where $v_{\mathfrak{p}}$ is the valuation corresponding to prime ideal $\mathfrak{p}$. (Reason: by previous argument, the difference between "correct" A_1 and A'_1 we constructed is an element in $\alpha_1 \in K^*$. We want $\alpha_1 A'_1$ to be our A_1.)

    Then $\lambda \geq 3 \Longleftrightarrow \chi \cup \alpha_1 = 0 \Longleftrightarrow \log_p \alpha_1 \equiv 0 \mod p^2$(Reason: Let ψ'_1, ψ'_2 be the cochain in $\mathcal{C}^1(G_K, \mu_p)$ corresponding to A'_1 and $A'_2 = \prod_{i=0}^{p-1} \sigma^i(\beta^{i(i-1)/2})$. Over G_K, we have $\chi \cup \psi'_1 + \binom{\chi}{2} \cup \psi_0 = -d\psi'_2$. Restrict on $G_{K_{\mathfrak{p}_0}}$ through $G_K \to G_{K_{\mathfrak{p}_0}}$, we have $\chi \cup \psi'_1 \mid_{G_{K_{\mathfrak{p}_0}}} + \binom{\chi}{2} \cup \psi_0 \mid_{G_{K_{\mathfrak{p}_0}}} = -d\psi'_2 \mid_{G_{K_{\mathfrak{p}_0}}}$. Let $\psi_1 \in \mathcal{C}^1(G_{K,S}, \mu_p)$ correspond to the A_1. Restrict to $G_{K_{\mathfrak{p}_0}}$, the Massey product $\chi \cup \psi_1 + \binom{\chi}{2} \cup \psi_0 = \chi \cup \psi'_1 + \binom{\chi}{2} \cup \psi_0 + \chi \cup (\psi_1 - \psi'_1)$ vanishes in $H^2(G_{K_{\mathfrak{p}_0}}, \mu_p)$ if and only if $\chi \cup (\psi_1 - \psi'_1) \mid_{G_{K_{\mathfrak{p}_0}}} = 0$,i.e. $\chi \cup \alpha_1 = 0$ in $H^2(G_{K_{\mathfrak{p}_0}}, \mu_p)$. A similar argument as lemma 30, we have the Massey product vanishing if and only if $\log_p(\alpha_1) \equiv 0 \mod p^2$. Notice that we can not directly use lemma 30 since α_1 may not be in $H^1(G_{K,S}, \mu_p)$. However, since we have restricted $\psi_1 - \psi'_1$ on $G_{K_{\mathfrak{p}_0}}$, we can directly work in $H^2(G_{K_{\mathfrak{p}_0}}, \mu_p)$. And similarly, restricting on $G_{K_{\tilde{\mathfrak{p}}_0}}$, we get the same result. Since $H^2(G_{K,S}, \mu_p) \to H^2(G_{K_{\mathfrak{p}_0}}, \mu_p) \oplus H^2(G_{K_{\tilde{\mathfrak{p}}_0}}, \mu_p)$ is injective, we conclude the Massey product vanishing if and only if $\log_p(\alpha_1) \equiv 0 \mod p^2$.)
(4) Assume $\lambda \geq 3$, then $\chi \cup \alpha_1 = 0 \Longleftrightarrow \exists \beta_1 \in K_1^*$ s.t. $\mathrm{Nm}_{K_1/K}(\beta_1) = \alpha_1$, (Reason: the cup product $\chi \cup \alpha_1$ should be viewed in $H^2(G_K, \mu_p)$). Define $A'_2 = \prod_{i=0}^{p-1} \sigma^i(\beta^{i(i-1)/2}) \in K_1^*$ and $B'_1 = \prod_{i=0}^{p-1} \sigma^i(\beta_1^i) \in K_1^*$. (Reason: we want the Massey product vanishing on G_K first. So we construct A'_2 and B'_1 correspond to the cocycle in this way. See lemma 26 and lemma 27.)

    Claim: There exists $\alpha_2 \in K^*$ s.t. $v_{\mathfrak{p}}(\alpha_2 A'_2 B'_1) \equiv 0 \mod p$ for all $\mathfrak{p} \nmid p$.(Reason: similarly to the previous case, the difference between "correct" A_2 and $A'_2 B'_1$ is an element $\alpha_2 \in K^*$.)

    Then $\lambda \geq 4 \Longleftrightarrow \chi \cup \alpha_2 = 0 \Longleftrightarrow \log_p \alpha_2 \equiv 0 \mod p^2$.(Reason: similar as previous case.)
(5) continues in a similar way $\cdots$

Remark 26. Easy to see by the construction and definition, the choice of β_i and α_i won't influence the numerical criterion.

Remark 27. The numerical criterion is not entirely satisfactory: it only guarantees the existence of the elements β_i and α_i, while we do not have a good algorithm that allows us to compute them quickly. In SageMath, however, there are algorithms for solving norm equations. More precisely, if L/K is a field extension and $\alpha \in K$,

SageMath can find an element $\beta \in L$ satisfying

$$\mathrm{Norm}_{L/K}(\beta) = \alpha,$$

provided that such a β exists.

The difficulty is that the available algorithms are not polynomial-time algorithms, and their running time can become prohibitively large when the discriminant of the field is large, which make us difficult to compute β_i and α_i quickly. In our setting, however, we know a priori that the relevant norm equations admit solutions, namely the elements β_i and α_i whose existence has already been established. This additional information may allow for a more efficient algorithm tailored to our particular situation.

I hope the following lemma can inspire people to come up with explicit numerical criteria, though I can not do it.

Lemma 32. *Let K be a imaginary quadratic field, $p \nmid h_K$, p split in K i.e. $p\mathcal{O}_K = \mathfrak{p}_0\widetilde{\mathfrak{p}_0}$. Let $\bar{\rho}_n : G_{K,S} \to \bar{U}_{n+1}$ be a defining system. Then the Massey product $(\chi_1, \chi_2, \cdots, \chi_n)_{\bar{\rho}_n}$ relative to a defining system $\bar{\rho}_n$ vanishes over $G_{K,S}$ if and only if it vanishes over G_K*

Proof. We have the following commutative diagram.

$$\begin{array}{ccc} G_{K_{\mathfrak{p}_0}} & \hookrightarrow & G_K \\ & \searrow & \downarrow \\ & & G_{K,S} \end{array}$$

It induces the following diagram.

$$\begin{array}{ccc} H^2(G_{K,S}, \mu_p) & \hookrightarrow & H^2(G_{K_{\mathfrak{p}_0}}, \mu_p) \oplus H^2(G_{K_{\tilde{\mathfrak{p}}_0}}, \mu_p) \\ \downarrow & \nearrow & \\ H^2(G_K, \mu_p) & & \end{array}$$

The row is an injective map by Poitou-Tate Duality (See proof of lemma 30). The column is an inflation map. If the Massey product vanishes over $G_{K,S}$, then after the inflation map, it vanishes over G_K. If the Massey product vanishes over G_K, we restrict on local field, then it vanishes over $G_{K_{\mathfrak{p}_0}}$ and $G_{K_{\tilde{\mathfrak{p}}_0}}$. Since the row map is injective, it vanishes in $G_{K,S}$. □

Remark 28. By the following well-known exact sequence:

$$H^1(G_K, \mu_p) \xrightarrow{\chi\cup -} H^2(G_K, \mu_p) \xrightarrow{Res} H^2(G_{K_1}, \mu_p)$$

The Massey product $\sum_{i=0}^{n-1} \binom{\chi}{i} \cup \psi_i$ in our case will be zero when restrict on G_{K_1}. Therefore, there exists $\chi_b \in H^1(G_K, \mu_p)$ such that $\chi \cup \chi_b = \sum_{i=0}^{n-1} \binom{\chi}{i} \cup \psi_i$.

5.1.3. *case 2.* Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty]$ be a nonzero cyclic group. Assume p remains prime over $K/\mathbb{Q}$, i.e. $p\mathcal{O}_K = \mathfrak{p}_0$. Then there is only one prime that is ramified in the $\mathbb{Z}_p$ cyclotomic extension $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$. Let I be an ideal in K such that $[I] \neq 0 \in \mathrm{Cl}(K)[p]$. Let α be the generator of the principal ideal I^p.

Theorem 33. *Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty]$ be a nonzero cyclic group. Assume p remains prime over $K/\mathbb{Q}$ and $n \geq 2$. Assume $\lambda \geq n-1$. Then $\lambda \geq n \Leftrightarrow$ n-fold Massey product $(\chi, \chi, \cdots \chi, \alpha)$ is zero with respect to a proper defining system.*

Remark 29. It is well known that $\lambda \geq 1$ is always true in the case.

proof of theorem 33.

In this case, we have $\mathrm{Cl}(K_l)[p^\infty]^+ = 0$ by Proposition 13.22 in [Was97]. We have D_l is a subgroup of $\mathrm{Cl}(K_l)[p^\infty]$ generated by $\mathfrak{p}_l$. Hence $D_l = D_l^+ = 0$ by definition. Therefore, we have $\mathrm{Cl}_S(K_l)[p^\infty] = \mathrm{Cl}(K_l)[p^\infty] = \mathrm{Cl}(K_l)[p^\infty]^-$. Our case satisfies conditions in lemma 18. We have $X \cong X_{cs}$ and $\lambda = \lambda_{cs}$.

By the exact sequence (2),

$$0 \to \mathrm{Cl}_S(K)/p = \mathbb{F}_p \to H^2(G_{K,S}, \mu_p) \to Br(\mathcal{O}_K[1/p])[p] = 0 \to 0$$

We have $H^2(G_{K,S}, \mu_p) = \mathbb{F}_p$. The theorem 14 implies

$$\lambda = \lambda_{cs} = \min\{n | \Psi^{(n)} \neq 0\} - 1 + 1 = \min\{n | \Psi^{(n)} \neq 0\}.$$

By the exact sequence (1),

$$0 \to \mathcal{O}_{K,S}^*/p \cong \mathbb{F}_p \to H^1(G_{K,S}, \mu_p) \to \mathrm{Cl}_S(K)[p] \cong \mathbb{F}_p \to 0$$

we know that $H^1(G_{K,S}, \mu_p)$ is generated by p and α. A similar argument as in theorem 21, we know p has p cyclic Massey product vanishing property. Similarly, the Iwasawa invariant $\lambda \geq n \Leftrightarrow \Psi^{(i)} = 0$ for all $0 \leq i < n$. Assume $\Psi^{(i)} = 0$ for all $0 \leq i < n-1$, then by theorem 11, $\mathrm{Im}\,\Psi^{(n-1)}$ is generated by $\Psi^{(n-1)}([\alpha])$. So $\Psi^{(n-1)} = 0$ if and only if $\Psi^{(n-1)}([\alpha]) = 0$ i.e. the Massey product $(\chi^{(n-1)}, \alpha)$ relative to a proper defining system vanishes by theorem 9. □

5.1.4. *case 3.* Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty]$ be a nonzero cyclic group. Assume p is ramified in $K/\mathbb{Q}$, i.e. $p\mathcal{O}_K = \mathfrak{p}_0^2$. Then there is only one prime that is ramified in the $\mathbb{Z}_p$ cyclotomic extension $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty$. Let I be an ideal in K such that $[I] \neq 0 \in \mathrm{Cl}(K)[p]$. Let α be the generator of the principal ideal I^p.

Theorem 34. *Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty]$ be a nonzero cyclic group and p is ramified in $K/\mathbb{Q}$ and $n \geq 2$. Assume $\lambda \geq n-1$. Then $\lambda \geq n \Leftrightarrow$ n-fold Massey product $(\chi, \chi, \cdots \chi, \alpha)$ is zero with respect to a proper defining system.*

Remark 30. It is well known that $\lambda \geq 1$ is always true in the case.

proof of theorem 34 .

Similar as Theorem 33, we have $\mathrm{Cl}(K_l)[p^\infty]^+ = 0$ and $D_l = D_l^+ = 0$ by definition. These imply $\mathrm{Cl}_S(K_l)[p^\infty]^- = \mathrm{Cl}(K_l)[p^\infty]^- = \mathrm{Cl}(K_l)[p^\infty]$. By the exact sequence (2),

$$0 \to \mathrm{Cl}_S(K)/p \cong \mathbb{F}_p \to H^2(G_{K,S}, \mu_p) \to Br(\mathcal{O}_K[1/p])[p] = 0 \to 0$$

we have $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$. Our case satisfies conditions in Theorem 14. The same argument as Theorem 33 gives us the conclusion.

□

5.2. **Cyclotomic field.** Let $K = \mathbb{Q}(\mu_p)$ where μ_p is the group of p-th roots of unit as before. Let $\omega : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}_p^*$ be the Teichmüller character. Let X be the Iwasawa module which is the inverse limit of the p-part of the class group of $\mathbb{Q}(\mu_{p^l})$ with respect to the norm map. By Corollary 10.15 in [Was97], $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on X and X is decomposed as direct sum of eigenspace, i.e. $X = \oplus_{i=0}^{p-2}\varepsilon_i X$ where $\varepsilon_i = \frac{1}{p-1}\sum_{a=1}^{p-1}\omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})]$. Fix $i = 3, 5, \cdots, p-2$. Assume that $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ is cyclic, we have $\varepsilon_i X = \Lambda/(f_i)$ by [Was97, Thm 10.16]. Notice that by Theorem 10.16 in [Was97], $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ is cyclic if Vandiver's conjecture holds. Let $\lambda_i = deg(f_i)$. Let I_i be an ideal in K such that $[I_i] \neq 0 \in \varepsilon_i\mathrm{Cl}(K)[p]$. Let α_i be the lift of $[I_i]$ by the map $\varepsilon_i H^1(G_{K,S}, \mu_p) \to \varepsilon_i\mathrm{Cl}(K)[p]$.

Theorem 35. *Let $K = \mathbb{Q}(\mu_p)$. Fix $i = 3, 5, \cdots p-2$ and assume that $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ is a nonzero cyclic group. Let $n \geq 2$. Assume $\lambda_i \geq n-1$. Then $\lambda_i \geq n \Leftrightarrow$ n-fold Massey product $\varepsilon_i(\chi, \chi, \cdots \chi, \alpha_i)$ is zero with respect to a proper defining system.*

proof of theorem 35 .

Our case satisfies the setting up in Theorem 16, where $k = \mathbb{Q}$, $K = \mathbb{Q}(\mu_p)$, $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. We have $\mathrm{Cl}(K_l) = \mathrm{Cl}_S(K_l)$. By the exact sequence:

$$0 \to \varepsilon_i\mathrm{Cl}_S(K)/p = \mathbb{F}_p \to \varepsilon_i H^2(G_{K,S}, \mu_p) \to \varepsilon_i Br(\mathcal{O}_K[1/p])[p] = 0 \to 0$$

we have $\varepsilon_i H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$. By Theorem 16, we have

$$\lambda_i = \lambda_{i,cs} = \min\{n|\varepsilon_i\Psi^{(n)} \neq 0\} - dim_{\mathbb{F}_p}\varepsilon_i Br(\mathcal{O}_K[1/p])[p] = \min\{n|\varepsilon_i\Psi^{(n)} \neq 0\}.$$

By the exact sequence:

$$0 \to \varepsilon_i\mathcal{O}_{K,S}^*/p = 0 \to \varepsilon_i H^1(G_{K,S}, \mu_p) \to \varepsilon_i\mathrm{Cl}(K)[p] = \mathbb{F}_p \to 0$$

we know that $\varepsilon_i H^1(G_{K,S}, \mu_p)$ is generated by α_i by our definition. Assume $\lambda_i \geq n-1$, then $\Psi^{(j)}|_{\varepsilon_i H^1(G_{K,S}, \Omega/I^n \otimes \mu_p)} = 0$ for $0 \leq j < n-1$. So $\mathrm{Im}\,\Psi^{(n-1)}|_{\varepsilon_i H^1(G_{K,S}, \Omega/I^{n-1} \otimes \mu_p)}$ is generated by $\Psi^{(n-1)}|_{\varepsilon_i H^1(G_{K,S}, \Omega/I^{n-1} \otimes \mu_p)}([\alpha_i])$. And $\Psi^{(n-1)}|_{\varepsilon_i H^1(G_{K,S}, \Omega/I^{n-1} \otimes \mu_p)}([\alpha_i]) = \varepsilon_i\Psi^{(n-1)}(f)$ for certain cocycle $f = \sum_{k=0}^{n-2}\psi_k x^k \in \mathcal{C}^1(G, \Omega/I^{n-1} \otimes \mu_p)$ such that $\psi_0 = \alpha_i$. Hence $\varepsilon_i\Psi^{(n-1)} = 0$ if and only if the n-fold Massey product $\varepsilon_i(\chi, \chi, \cdots \chi, \alpha_i) = 0$ with respect to a proper defining system. □

Remark 31. This is a generalization of McCallum and Sharifi's result of proposition 4.2 in [MS03].

References

[Dwy75] W. G. Dwyer. "Homology, Massey products and maps between groups". In: *J. Pure Appl. Algebra* 6.2 (1975), pp. 177–190.

[Gol74] R. Gold. "The nontriviality of certain Z_1-extensions". In: *J. Number Theory* 6 (1974), pp. 369–373.

[Kol04] M. Kolster. "K-theory and arithmetic". In: *Contemporary developments in algebraic K-theory*. ICTP Lect. Notes, XV. Abdus Salam Int. Cent. Theoret. Phys., Trieste, 2004, pp. 191–258.

[Kra66] D. Kraines. "Massey higher products". In: *Trans. Amer. Math. Soc.* 124 (1966), pp. 431–449.

[Lam+23] Y. H. J. Lam, Y. Liu, R. Sharifi, P. Wake, and J. Wang. "Generalized Bockstein maps and Massey products". In: *Forum Math. Sigma* 11 (2023), Paper No. e5, 41.

[LM21] I. Limonchenko and D. Millionshchikov. "Higher order Massey products and applications". In: *Topology, geometry, and dynamics—V. A. Rokhlin-Memorial*. Vol. 772. Contemp. Math. Amer. Math. Soc., [Providence], RI, 2021, pp. 209–240.

[Mil20] J. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[MS03] W. G. McCallum and R. T. Sharifi. "A cup product in the Galois cohomology of number fields". In: *Duke Math. J.* 120.2 (2003), pp. 269–310.

[MT16] J. Mináč and N. ê. D. Tân. "Triple Massey products vanish over all fields". In: *J. Lond. Math. Soc. (2)* 94.3 (2016), pp. 909–932.

[MT17] J. Mináč and N. ê. D. Tân. "Triple Massey products and Galois theory". In: *J. Eur. Math. Soc. (JEMS)* 19.1 (2017), pp. 255–284.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008, pp. xvi+825.

[RS25] A. Ray and R. Sujatha. *Massey products and the Iwasawa theory of fine Selmer groups*. 2025. arXiv: `2508.17156 [math.NT]`.

[Sha07] R. T. Sharifi. "Massey products and ideal class groups". In: *J. Reine Angew. Math.* 603 (2007), pp. 1–33.

[Sha18] R. T. Sharifi. *Modular Curves and Cyclotomic Fields*. Lecture notes for the Arizona Winter School 2018. 2018.

[Sha22] R. T. Sharifi. "Reciprocity maps with restricted ramification". In: *Transactions of the American Mathematical Society* 375.8 (2022), pp. 5361–5392.

[Sha99] R. T. Sharifi. *Twisted Heisenberg representations and local conductors*. Thesis (Ph.D.)–The University of Chicago. ProQuest LLC, Ann Arbor, MI, 1999, p. 65.

[Tat67] J. Tate. "Global Class Field Theory". In: *Algebraic Number Theory*. Ed. by J. W. S. Cassels and A. Fröhlich. London: Academic Press, 1967. Chap. VII, pp. 162–203.

[Tat76] J. Tate. "Relations between K_2 and Galois cohomology". In: *Invent. Math.* 36 (1976), pp. 257–274.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487.

Morningside Center of Mathematics, Chinese Academy of Science, Beijing, China
Email address: qipeikai@amss.ac.cn