IWASAWA λ INVARIANT AND MASSEY PRODUCT

PEIKAI QI

Abstract. We compute Iwasawa λ invariant in terms of Massey products in Galois cohomology with restricted ramification. When applied to imaginary quadratic fields and cyclotomic fields, we obtain a new proof and generalization of results of Gold [2] and McCallum-Sharifi [7]. The main tool is the generalized Bockstein map introduced by Lam-Liu-Sharifi-Wake-Wang[5].

1. Introduction

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

Massey products of Galois cohomology are introduced in number theory to study the structure of Galois groups. We will introduce the definition of Massey products in section 2.2. One can view Massey products as a generalization of cup products in cohomology and for example, the cup product is a 2-fold Massey product.

The idea of using Massey products to study Iwasawa theory first appears in Sharifi's paper [12]. McCallum and Sharifi proved that under some assumptions, we have $\lambda \geq 2$ if and only if a certain cup product vanishes for cyclotomic fields in [7, Proposition 4.2]. One can also translate Gold's criterion [2] into group cohomology. It also has the form that $\lambda \geq 2$ if and only if a certain cup product vanishes for imaginary quadratic fields under some assumptions. The two results have completely different proof. We want to find the deep reason behind it. Our main theorem unifies these two results and when applied to these cases, we get a generalization for them. Roughly speaking, we proved that under some assumptions, if $\lambda \geq n-1$, then $\lambda \geq n$ if and only if a certain Massey product vanishes.

For readers who are familiar with Massey products, here are some differences one should notice. In Ján Mináč and Nguyễn Duy Tân's Massey products vanishing conjecture [10], Massey products vanishing means that Massey products vanish relative to all defining systems. In our paper, Massey products vanishing means that Massey products vanish relative to a particular defining system, which we call the proper defining system. In addition, they consider the Massey products for absolute Galois groups and we consider the Galois groups with restricted ramifications.

1.2. **The strategy and notations.** The strategy of the project is divided into four steps.

(1) *The Iwasawa invariant λ and λ_{cs}*

Date: January 10, 2024.

Let S be the set of primes of K above p and $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)[p^\infty]$. Let μ_{cs} and λ_{cs} be the Iwasawa invariant for the Iwasawa module X_{cs}. Let D_l be the subgroup of $\mathrm{Cl}(K_l)[p^\infty]$ generated by primes in S. Then we have

$$0 \to \varprojlim D_l \to X \to X_{cs} \to 0$$

We can relate λ with λ_{cs} if we know $\varprojlim D_l$.

(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 $G_{K_l,S} = \mathrm{Gal}(K_S/K_l)$. We have the following exact sequences from Kummer theory:

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

To know the information about λ_{cs}, we need information about the size of the group $\mathrm{Cl}_S(K_l)[p^\infty]$. Hence, we need 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-Wang's paper [5, 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 augmentation ideal of $\mathbb{F}_p[[\mathrm{Gal}(K_l/K)]]$ and $\Psi^{(n)} : H^1(G_{K,S}, \mu_p \otimes I^n/I^{n+1}) \to H^2(G_{K,S}, \mu_p)$ is the generalized Bockstein map defined in [5]. We have a filtration $H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \supset IH^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \supset I^2 H^2_{\mathrm{Iw}}(N, \mu_p) \supset \cdots \supset I^n H^2_{\mathrm{Iw}}(G_{K_l,S}, \mu_p) \cdots$. Once we know the size of $H^2(G_{K,S}, \mu_p)$ and the size of $\mathrm{Im}\, \Psi^{(n)}$, we can determine the filtration and get the information about 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-Wang's paper [5], they proved that under some circumstances, the image of generalized Bockstein map $\mathrm{Im}\, \Psi^{(n)}$ is spanned by certain n-fold Massey products.

1.3. **Main theorem and corollaries.** As one can see, our strategy does not involve the Iwasawa Main Conjecture. And the Iwasawa λ invariant that we computed is the algebraic Iwasawa λ invariant. By following the strategy, one of the main theorems is the following:

Theorem 1. *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 $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)$ and μ_{cs}, λ_{cs} be the Iwasawa invariants of X_{cs}. Assume X_{cs} has no torsion element and $H^2(G_{K,S}, \mu_p) \cong \mathbb{F}_p$.*

Then $\mu_{cs} = 0$ if and only if there exists integer k such that $\Psi^{(k)} \neq 0$ for some k. If $\mu_{cs} = 0$, then

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

When we have a Galois group Δ acts on the Iwasawa module $X = \varprojlim \mathrm{Cl}(K_n)$ and the action gives us a decomposition $X = \oplus_i \varepsilon_i X$, the techniques used to prove Theorem 1 also apply equivalently to calculate the Iwasawa invariant λ_i of $\varepsilon_i X$. See Theorem 15.

We applied the Theorem 1 in many cases in the paper. In the introduction, we list two cases that correspond to the setting of results of Gold [2] and McCallum-Sharifi [7].

Theorem 2. *Let K be an imaginary quadratic field and assume that $p \nmid h_K$, p splits in K as $p\mathcal{O}_K = \mathfrak{P}_0\tilde{\mathfrak{P}}_0$. For cyclotomic $\mathbb{Z}_p$ extension, the λ-invariants of K can be determined in terms of Massey products as follows:*

Let $n \geq 2$ and suppose $\lambda \geq n-1$. Then $\lambda \geq n$ if and only if n-fold Massey product $(\chi, \chi, \cdots \chi, \alpha)$ is zero with respect to the proper defining system.

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

Remark 1. In other words, it means

$$\lambda = \min\{n \mid n \text{ fold Massey products } (\chi, \chi, \cdots \chi, \alpha) \text{ is nonzero}\}$$

Remark 2. It is a fact that $\lambda \geq 1$ in the case. Gold's criterion [2] said that $\lambda \geq 2 \Leftrightarrow \alpha^{p-1} \equiv 1 \mod \mathfrak{P}_0^2$. Further calculation shows that $\alpha^{p-1} \equiv 1 \mod \mathfrak{P}_0^2 \Leftrightarrow \log_p(\alpha) \equiv 0 \mod p^2 \Leftrightarrow \chi \cup \alpha = 0$, where $\log_p$ is the p-adic logarithm. The theorem can be viewed as new proof of Gold's result and a generalization of Gold's result.

Theorem 3. *Let $K = \mathbb{Q}(\mu_p)$ and $\omega : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{Z}_p$ be the Teichmüller character. We can decompose the class group $\mathrm{Cl}(K)[p^\infty]$ as*

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

where $\varepsilon_i = \frac{1}{p-1}\sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}]$. Let λ_i be the λ invariant corresponding to $\varepsilon_i\mathrm{Cl}(K_l)[p^\infty]$.

Fix $i = 3, 5, \cdots p-2$ and assume that $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ is cyclic. Let $n \geq 2$ and suppose $\lambda_i \geq n-1$, then $\lambda_i \geq n$ if and only if n-fold Massey product $\varepsilon_i(\chi, \chi, \cdots \chi, \alpha_i) = 0$ with respect to the proper defining system.

Remark 3. The assumption $\varepsilon_i\mathrm{Cl}(K)[p] = \mathbb{F}_p$ implies that $\lambda_i \geq 1$ in the case. Note that $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ is cyclic if Vandiver's conjecture holds. The theorem implies that $\lambda_i \geq 2 \Leftrightarrow \varepsilon_i(\chi, \alpha_i) = 0 \Leftrightarrow \chi \cup \alpha_i = 0$. Proposition 4.2 in McCallum and Sharifi's paper [7] describes a similar result that $\lambda_i \geq 2 \Leftrightarrow \chi \cup \alpha_i = 0$. The theorem can be viewed as a generalization of McCallum and Sharifi's results.

1.4. **Structure of the paper.** In section 2, we discuss the generalized Bockstein map introduced by Lam-Liu-Sharifi-Wake-Wang[5] and recall the relation of generalized Bockestein map and Massey products. We will also prove that the generalized Bockstein map preserves the group action. In section 3, we prove a formula to determine the size of the second cohomology group by the generalized Bockstein map. In section 4, we prove the main theorem by applying the formula into number theory. We also list four cases in which we apply our theorem to get some interesting results. The first three cases are cyclotomic $\mathbb{Z}_p$ extensions of imaginary quadratic fields. The last case is the cyclotomic $\mathbb{Z}_p$ extension of cyclotomic fields. In the first case, we also develop a numerical criterion to determine λ, which takes 10 pages. One can skip the numerical criterion for the first reading.

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 [5].

Let G be a profinite group of finite p-cohomological dimension d and N be a closed normal subgroup such that G/N is a finitely generated pro-p quotient. In the paper, we take $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$. However, the definition of generalized

Bockstein map works more generally. Let $\Omega = \mathbb{F}_p[[G/N]]$ be the completed group algebra which is a G-module in a natural way. Let σ be the generator of G/N and $I =< \sigma - 1 >$ be the augmentation ideal in Ω. For $0 \leq n < \#G/N$, we have the following exact sequence of $G-$module:

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

After taking tensor product with a finite $\mathbb{F}_p[G]-$module T, it is still an exact sequence since every module that appeared above is a $\mathbb{F}_p$ module:

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

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

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

where the last isomorphism uses the fact that I^n/I^{n+1} is a trivial G-module. We view $\Psi^{(0)} = 0$. Recall the definition of Iwasawa cohomology groups:

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

where the inverse limit is taken with respect to correstriction maps and U runs over all open normal subgroups of G containing N. Notice that if G/N is finite, then $H^i_{\mathrm{Iw}}(N, T) = H^i(N, T)$. In Lam-Liu-Sharifi-Wake-Wang's paper, they proved:

Theorem 4 (Theorem A in LLSWW[5])**.** *For each $0 \leq n < \#G/N$, there is a canonical isomorphism*

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

of $\mathbb{F}_p$-modules, where d is the p-cohomological dimension of G.

For the remaining part of this subsection, we will show that the isomorphism above has a certain equivalence. We can decompose the cohomological group into a direct sum of eigenspaces with respect to a group action. For each eigenspace, we still have such isomorphism. However, the process of checking that the generalized Bockstein map $\Psi^{(n)}$ preserves the group action is tedious. One can skip the part to Remark 6.

Lemma 5. *Let $G/N \cong \mathbb{Z}_p$ and U_l be the unique open normal subgroup of G containing N such that $G/U_l \cong \mathbb{Z}/p^l\mathbb{Z}$. And T is a finite $\mathbb{F}_p[G]-$module. Then $\mathrm{CoInd}^G_{U_l} T := \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T) \cong \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$ as $\mathbb{F}_p[G]-$ module. By Shapiro's lemma,*

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

Proof. Let $G = \bigsqcup_{i=1}^{p^l} U_l \sigma_i$ where σ_i are right coset representatives. Now we define a homomorphism $\alpha : \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T) \to \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$ by mapping the element $\phi \in \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T)$ to the element $\sum_{i=1}^{p^l} \bar{\sigma}_i^{-1} \otimes \sigma_i^{-1}\phi(\sigma_i)$, where $\bar{\sigma}_i$ represents the image of σ_i in the quotient G/U_l.

First, the map does not depend on the choice of right coset representatives. Let $h_i\sigma_i$ be another set of right coset representatives where $h_i \in U_l$. 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 $\phi(h_i\sigma_i) = h_i\phi(\sigma_i)$.

Second, the map preserves $\mathbb{F}_p[G]$ actions. Recall the action $g \in G$ on $\phi \in \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T)$ is

$$(g\psi)(x) = \psi(xg).$$

The action $g \in G$ 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

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

Then

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

Assume $\sigma_i g = h_i\sigma_{\delta(i)}$, where δ is a permutation of $1 \le i \le p^l$. We have

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

and

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

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.

Lastly, easy to see α is bijection or one can write out the inverse map of α. Hence $\mathrm{CoInd}_{U_l}^G T$ is isomorphice to $\mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$ as $\mathbb{F}_p[G]-$modules. □

Here, we computed $H^r(U_l, T)$. Next, we will compute $H^r_{\mathrm{Iw}}(N, T)$. We need the following propositions due to Tate [14].

Proposition 1. *Suppose $i > 0$ and $M = \varprojlim M_l$ 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 U_l be the unique open normal subgroup of G containing N such that $G/U_l \cong \mathbb{Z}/p^l\mathbb{Z}$. And T is a finite $\mathbb{F}_p[G]-$module. Then $H^r_{\mathrm{Iw}}(N, T) \cong H^r(G, \mathbb{F}_p[[G/N]] \otimes_{\mathbb{F}_p} T)$.*

Proof. By lemma 5,

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

To prove the third equality is true, we need to check that it satisfies conditions in Proposition 1. First, we have that $\mathbb{F}_p[G/U_l]\otimes_{\mathbb{F}_p} T$ is finite module. Second, by [5, Proposition 2.2.2], we know that $H^i(U_l,T)\cong H^i(G,\mathbb{F}_p[G/U_l]\otimes_{\mathbb{F}_p} T)$ is finitely generated $\mathbb{F}_p[G/U_l]$ module for all $i\geq 0$. Since $\mathbb{F}_p[G/U_l]$ is finite, we have that $H^i(G,\mathbb{F}_p[G/U_l]\otimes_{\mathbb{F}_p} T)$ is also finite.

For the last equality, note that T is a finite dimensional vector space over F_p. Hence $\varprojlim \mathbb{F}_p[G/U_l]\otimes_{\mathbb{F}_p} T\cong \mathbb{F}_p[[G/N]]\otimes_{\mathbb{F}_p} T$ as F_p module. One can see that the isomorphism also preserves G action. Hence it is also a $\mathbb{F}_p[G]$- isomorphism.

□

Remark 4. We know $\varprojlim \mathrm{CoInd}^G_{U_l} T \coloneqq \varprojlim \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G,T)\cong \mathbb{F}_p[[G/N]]\otimes_{\mathbb{F}_p} T$. But $\mathrm{CoInd}^G_N T\coloneqq \mathrm{Hom}_{\mathbb{Z}N}(\mathbb{Z}G,T)$ may not be isomorphic to $\varprojlim \mathrm{CoInd}^G_{U_l} T$. That is one reason why we separate the proof of lemma 5 and lemma 6 and we often write our induced module as $\Omega\otimes T$ instead of $\mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G,T)$.

Let $\mathscr{G}$ be a group containing G and N as normal subgroups such that $\mathscr{G}/G=\Delta$ is an abelian group and $\mathscr{G}/N$ is also abelian and $\mathscr{G}/N\cong\Delta\oplus G/N$, where G/N is a finitely generated pro-p quotient. Let T be a $\mathbb{F}_p[\mathscr{G}]$-module and $\Omega=\mathbb{F}_p[[G/N]]$. Next, We will define an action of group Δ on $H^r(G,\Omega\otimes T)$, $H^r(G,I^n/I^{n+1}\otimes T)$, $H^r(G,\Omega/I^n\otimes T)$, and $H^r(G,T)$. And we will show that the generalized Bockstein map $\Psi^{(n)}$ preserves the action. We take $G/N\cong\mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$ in our paper. But the setting up works generally.

Define $\tau\in\mathscr{G}$ acting on $\sum_i \bar{\sigma}_i\otimes t_i\in\Omega\otimes T$ as $\tau(\sum_i\bar{\sigma}_i\otimes t_i)=\sum_i\bar{\sigma}_i\otimes\tau t_i$. Recall the action $g\in G$ on $\Omega\otimes T$ is $g(\sum_i\bar{\sigma}_i\otimes t_i)=\sum_i\bar{g}\bar{\sigma}_i\otimes gt_i$. These two actions have different effects when $\tau\in G\subset\mathscr{G}$. But they have the same effect when $\tau\in N\subset\mathscr{G}$. For every $\tau\in\mathscr{G}$, we have a group homomorphism $\alpha: G\to G, g\to\tau^{-1}g\tau$ and a module homomorphsim $\beta:\Omega\otimes T\to\Omega\otimes T, \sum_i\bar{\sigma}_i\otimes t_i\to\tau(\sum_i\bar{\sigma}_i\otimes t_i)$. And

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

By the functorial properties of the cohomology groups [8, Chapter 2,p. 66], we have a homomorphism $H^r(G,\Omega\otimes T)\to H^r(G,\Omega\otimes T)$. This gives us an action of $\mathscr{G}$ on $H^r(G,\Omega\otimes T)$.

We know the action $\tau \in \mathscr{G}$ on $\Omega \otimes T$ and the action G on $\Omega \otimes T$ have the same effect when $\tau \in N$. By a well known fact [8, Example 1.27(d),p. 67], the induced action $\tau \in N \subset \mathscr{G}$ on $H^r(G, \Omega \otimes T)$ is trivial. So the action $\mathscr{G}$ on $H^r(G, \Omega \otimes T)$ factors through $\mathscr{G}/N \cong \Delta \oplus G/N$. Hence, we get an action Δ on $H^r(G, \Omega \otimes T)$ by viewing Δ as a subgroup of $\mathscr{G}/N$.

Similarly, we can define the action of $\mathscr{G}$ on $\Omega/I^n \otimes T$ and $I^n/I^{n+1} \otimes T$ in the same way. And actions are compatible, i.e.

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

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 $\mathbb{Z}[G]$ projective resolution of $\mathbb{Z}$. Then (α, β) defines a homomorphism of complexes

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

for any k. And it induces a homomorphism between two exact sequences of complexes:

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

By the functorial property of cohomology, we get a homomorphism between two long exact sequences.

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

Each column gives an action of $\tau \in \mathscr{G}$ and they are compatible with each other. In particular, since the generalized Bockstein map is the connecting mapping, we have $\Psi^{(n)}(\tau\phi) = \tau\Psi^{(n)}(\phi)$ for any $\phi \in H^{d-1}(G, T \otimes \Omega/I^n)$. As before, all actions factor through $\mathscr{G}/N$. It induces an action of Δ on the cohomology group. And the generalized Bockstein map $\Psi^{(n)}$ preserves the actions.

Remark 5. By lemma 5, we have $\mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T) \cong \mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$. Corresponding to the action $\tau \in \mathscr{G}$ on $\mathbb{F}_p[G/U_l] \otimes_{\mathbb{F}_p} T$, the action $\tau \in \mathscr{G}$ on $\phi \in \mathrm{Hom}_{\mathbb{Z}U_l}(\mathbb{Z}G, T)$ is $(\tau\phi)(g) = \tau\phi(\tau^{-1}g\tau)$.

Remark 6. The action Δ on the cohomology group is a left action.

Now we introduce a new notation to express elements in Ω which will simplify our future calculation. For simplicity, assume $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$ and σ is the generator of G/N. Let $x = \sigma - 1$, then $I =< \sigma - 1 >=< x >$ and $\Omega = \mathbb{F}_p[[G/N]] \cong \mathbb{F}_p[[x]]$ or $\mathbb{F}_p[x]/(x^{p^l})$ with respect to $G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$. Elements in $\Omega \otimes T$ can be write 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 χ be the group homomorphism $\chi : G \to G/N \cong \mathbb{Z}_p$ or $\mathbb{Z}/p^l\mathbb{Z}$. Then the action $g \in G$ on $\Omega \otimes T$ can be writen as

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

2.2. **Massey product.** In this section, we recall some facts of Massey products, defining systems[6][10] and proper defining systems[5]. More reference are [4][1]

For the classical definition of Massey products in group cohomology. Let A be a commutative ring with trivial G action and discrete topology. By [11], we know that inhomogeneous continuous cochains $\mathcal{C}^\cdot = \bigoplus_{k\geq 0} \mathcal{C}^k(G, A)$ form a differential graded algebra over A. It equips with product $\cup$ and differential $d : \mathcal{C}^n \to \mathcal{C}^{n+1}$ such that: $d(a \cup b) = (d\,a) \cup b + (-1)^k a \cup (d\,b)$ where $a \in \mathcal{C}^k$ and $d^2 = 0$. We have $H^n(G, A) = \ker d^n / \operatorname{Im} d^{n-1}$.

Let $U_{n+1}(A)$ be the group of $(n+1) \times (n+1)$ upper triangular matrix with diagonal entries equal 1. Let $Z(U_{n+1}(A))$ be the center of $U_{n+1}(A)$. It is a group of matrix whose diagonal entries equal to 1 and other only possible non zero entry is in the spot $(1, n+1)$. Let $\bar{U}_{n+1}(A) = U_{n+1}(A)/Z(U_{n+1}(A))$.

Let $\chi_1, \chi_2, \cdots, \chi_n$ be n elements in $H^1(G, A) = \operatorname{Hom}(G, A)$. The defining system with respect to $\chi_1, \chi_2, \cdots, \chi_n$ is a homomorphism $\bar{\rho} : G \to \bar{U}_{n+1}(A)$ with $\rho_{i,i+1} = \chi_i$, where $\rho_{i,j}$ is the composition of map $\bar{\rho} : G \to \bar{U}_{n+1}(A)$ with the projection of $\bar{U}_{n+1}(A)$ to its (i, j) entries. One can check: $\sum_{j=2}^{j=n} \rho_{1,j}(g_1)\rho_{j,n+1}(g_2)$ is a cocyle inside $\mathcal{C}^2$ which represents an element in $H^2(G, A)$. We denote the element as $(\chi_1, \chi_2, \cdots, \chi_n)_{\bar{\rho}}$ and call it the Massey product with respect to the defining system $\bar{\rho}$. By [1], the Massey product $(\chi_1, \chi_2, \cdots, \chi_n)_{\bar{\rho}}$ vanishing is equivalent to that $\bar{\rho}$ can be lifted to a homomorphism $\rho : G \to U_{n+1}(A)$.

Here $\bar{\rho} \in \operatorname{Hom}(G, \bar{U}_{n+1}(A))$ can be think as degree one cocycle in $\mathcal{C}^1(G, \bar{U}_{n+1}(A))$ with G acting trivially on $\bar{U}_{n+1}(A)$. In general, the action of G on the ring A may not be trivial. We could define defining systems as a degree one cocycle in the same philosophy and it can be applied in general situations. References are [5]. We directly borrow definitions from Section 3 of [5] without giving definitions again here.

But our definition of proper defining systems is a little different from the definition in [5]. We give a new definition here.

Definition 1. Let $\chi \in H^1(G, T_1)$ and $\psi_0 \in H^1(G, T_2)$. Then we call the defining system $\bar{\rho} : G \to \mathcal{U}(\mathcal{A})$ with respect to $\underbrace{\chi, \chi, \cdots .\chi}_{\text{n copies}}, \psi_0$ as proper defining system if $\bar{\rho}$ is of the following forms:

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

Remark 7. In [5], when they define the proper defining system, they first divide the matrix into four blocks that looks like the one in the following Lemma 7. And then

they fix the up-left block and down-right block and let the up-right block varies. Here, our definition of the proper defining system can be viewed as a special case of them. In our definition, we fix and give a explicit form of the first $(n+1)\times(n+1)$ block and we let the last column varies except 1 and ψ_0.

The following Lemma 7 and Remark 8 will only be used in the section of numerical criterion. One can skip if not interested in the numerical criterion.

Lemma 7. *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 8. 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 7, 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 [5].

Theorem 8 (LLSWW[5])**.** *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 the 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 9. 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, we assume G has p cohomological dimension $d = 2$.

Lemma 9. *Let G be a 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 $\mathbb{F}_p[G]$ 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, $I^nH^2_{\mathrm{Iw}}(N, T) = I^{n+1}H^2_{\mathrm{Iw}}(N, T)$. 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 $\#H^2(N, T) = p^n$. □

Theorem 10. *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 $f' = \psi'_0 + \psi'_1x + \cdots + \psi'_{n-1}x^{n-1}$ 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 $\Psi^{(n)}(\psi_0 + \psi_1x + \cdots + \psi_{n-1}x^{n-1})$ 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 $\tilde{f}(\sigma) = \psi_0(\sigma) + \psi_1(\sigma)x + \cdots + \psi_{n-1}(\sigma)x^{n-1} + \psi_n(\sigma)x^n$.

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 10. 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 11. *The element $\psi \in H^1(G,T)$ has p cyclic Massey product vanishing property if and olny 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 correstriction 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 $X = \varprojlim \mathrm{Cl}(K_l)$.
(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 12. *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[8]. Notice that $\mathcal{O}_{K_l,S} \in (K_S^*)^p$. And by theorem 11, the theorem holds. The second conclusion follows by taking the inverse limit. □

Remark 11. The map $\varprojlim \mathcal{O}_{K_l,S} \xrightarrow{\text{Nm}} \mathcal{O}_{K,S} \hookrightarrow K$ 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 [3][5][11])

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

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

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 $Br(\mathcal{O}_K[1/p]) \cong (\mathbb{Q}/\mathbb{Z})^{\#S-1}$, so $Br(\mathcal{O}_K[1/p])[p] \cong \mathbb{F}_p^{\#S-1}$

Now, we can state and prove our main theorem.

Theorem 13. *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 $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)$ and μ_{cs}, λ_{cs} be the Iwasawa invariant of X_{cs}. Assume X_{cs} has no torsion element 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.

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

Since all primes in S are totally ramified K_∞/K, we have $Br(\mathcal{O}_{K_l}[1/p])[p] \cong Br(\mathcal{O}_{K_{l+1}}[1/p])[p] : [A] \to [A \otimes_{K_l} K_{l+1}]$ for every l, where $[A]$ is a class of central simple K_l-algebra represented by A . And we know the composite map $Cor \circ Res : Br(\mathcal{O}_{K_l}[1/p])[p] \cong Br(\mathcal{O}_{K_{l+1}}[1/p])[p] \to Br(\mathcal{O}_{K_l}[1/p])[p]$ is the multiplication by p. Hence the composite map is 0. Therefore, the correstriction map $Br(\mathcal{O}_{K_{l+1}}[1/p])[p] \to Br(\mathcal{O}_{K_l}[1/p])[p]$ is zero map. And take inverse limit with respect to the correstriction map, we have $\varprojlim Br(\mathcal{O}_{K_l}[1/p])[p] \cong Br(\mathcal{O}_K[1/p])[p] \cong \mathbb{F}_p^{\#S-1}$.

We have the following exact sequence:

$$0 \to p\mathrm{Cl}_S(K_l) \to \mathrm{Cl}_S(K_l) \to \mathrm{Cl}_S(K_l)/p \to 0$$

Take inverse limit,

$$0 \to pX_{cs} \to X_{cs} \to \varprojlim \mathrm{Cl}_S(K_l)/p \to 0$$

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 9 . 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 torsion element, 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 9. Therefore, by the exact sequence, we have

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

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

□

In the proof of the theorem, to use the lemma 9, 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 $G = G_{K,S}$, $N = G_{K_{p^l},S}$, $\chi : G \to G/N \cong \mathbb{Z}/p^l\mathbb{Z}$ and $\Omega = \mathbb{F}_p[[G/N]]$.

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 $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)$ and μ_{cs}, λ_{cs} be the Iwasawa invariant of X_{cs}. Assume X_{cs} has no torsion element 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 [15] and the same notation as [15, 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 torsion element, we have $fX_{cs} = 0$. We have $\mathrm{Cl}_S(K_l)/p = X_{cs}/(T^{p^l-1}Y_0, pX_{cs}) = X_{cs}/(T^{p^l-1}Y_0, pX_{cs}, fX_{cs}) = X_{cs}/(T^{p^l-1}Y_0, pX_{cs}, T^{\lambda_{cs}}X_{cs}) = X_{cs}/(pX_{cs}, T^{\lambda_{cs}}X_{cs}) = X_{cs}/(pX_{cs}, fX_{cs}) = X_{cs}/pX_{cs} \cong \mathbb{F}_p^{\lambda_{cs}}$ since $\lambda_{cs} < p^l$.

The remaining proof is similar to the proof of Theorem 13 □

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 $\hat{\Delta} \coloneqq \mathrm{Hom}(\Delta, \mathbb{Z}_p)$ be the character group. Let $\omega \in \hat{\Delta}$ and define

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

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

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

Theorem 15. *Let K_∞/K be the $\mathbb{Z}_p$ extension as set up above. Assume all primes in S begin totally ramified starting K. Let $X_{cs} = \varprojlim \mathrm{Cl}_S(K_l)$. Assume $p \nmid \#\Delta$. 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 torsion element 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 13, 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 13, 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

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

where $\Psi^{(n)}|_{\varepsilon_\omega H^2(G_{K,S}, \Omega/I^n \otimes \mu_p)}$ denotes $\Psi^{(n)}$ restricting on $\varepsilon_\omega H^2(G_{K,S}, \Omega/I^n \otimes \mu_p)$. 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 $\Psi^{(n)}|_{\varepsilon_\omega H^2(G_{K,S}, \Omega/I^n \otimes \mu_p)} = 0$ if and only if $\varepsilon_\omega \Psi^{(n)} = 0$. Hence the conclusion follows from the exact sequence. □

Remark 12. We can have a similar theorem as theorem 14 with the action of Δ. We omit it here since it is essentially the same.

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 [15].

Lemma 16. *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 16, one can get the following lemma. It is Proposition 13.28 in [15].

Lemma 17. *The same assumption as Lemma 16, then $X^- = \varprojlim \mathrm{Cl}(K_l)[p^\infty]^-$ contains no finite Λ-submodules.*

In the paper [2], Gold refined the Lemma 16 to the following theorem.

Theorem 18. *The same assumption as lemma 16, 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 19. *The same assumption as lemma 16, 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 16 implies lemma 17 in [15]. 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 20. *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 $(\chi, \chi, \cdots \chi, \alpha)$ vanishes with respect to a proper defining system.*

Remark 13. 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 [2]. Our theorem gives a new proof of Gold's criterion and generalizes the criterion.

proof of theorem 20.

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 18 and theorem 19 and we will use the same notation as them. By using Proposition 13.22 in [15], 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

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

By lemma 17 and theorem 19, we know that X and X_{cs} have no finite Λ-module. 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 13. 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 10, $\mathrm{Im}\,\Psi^{(n-1)}$ 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

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

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 12, we know p has p cyclic Massey product vanishing property.

On the other hand, $\alpha\tilde{\alpha} = \pm p^{h_K}$. 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 8.

□

Remark 14. 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 14 instead of Theorem 13. We will use this idea to develop 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 14, 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 the 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 $F^*/(F^*)^p$ corresponding to $\chi_a, \chi_b \in H^1(G_K, \mu_p) \cong F^*/(F^*)^p$. 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[13]. Another reference is [9]:

Theorem 21 (Sharifi)**.** *The same notation as before. Assume $\chi_a \cup \chi_b = 0$. Let $A_1 = \prod_{i=0}^{p-1} \sigma^j(\beta^j)$ 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 22 (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 15. 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 $M_n :=< s, t_0, t_1, \cdots, t_n \mid s^p = 1, t_0^p = 1, t_1^p = 1, \cdots, t_n^p = 1, t_i t_j t_i^{-1} t_j^{-1} = 1, st_0 s^{-1} t_0^{-1} = t_1, st_1 s^{-1} t_1^{-1} = t_2, st_2 s^{-1} t_2^{-1} = t_3, \cdots, st_{n-1} s^{-1} t_{n-1}^{-1} = t_n, st_n s^{-1} t_n^{-1} = 1 >$

Remark 16. One can check that M_n is a semiproduct. 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 23. *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 calculation of matrices. We omit the calculation here.

On the other hand, we can use A, B_0 generating the following two 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 17. 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 18. By the lemma 23, 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 24. *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 $A_1 = \prod_{i=0}^{p-1} \sigma_a^i(\beta^i), A_2 = \prod_{i=0}^{p-1} \sigma_a^i(\beta^{\frac{i(i-1)}{2}}), A_3 = \prod_{i=0}^{p-1} \sigma_a^i(\beta^{\frac{i(i-1)(i-2)}{3}}), \cdots, A_n = \prod_{i=0}^{p-1} \sigma_a^i(\beta^{\binom{i}{n}})$ 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 25. *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 $1 \leq i \leq n < p-1$.

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 $\tilde{\sigma}_a$ and $\tilde{\sigma}_b$.

As said in remark 18, 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 $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})/K)$. We denote them as $\tilde{\sigma}_a$ and $\tilde{\sigma}_b$. We would like to map $\tilde{\sigma}_a$, $\tilde{\sigma}_b$ to s, t_0 respectively. Next, we will check it satisfies the relations.

By lemma 24,

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

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

$$\tilde{\sigma}_a^2(A_1^{1/p}) = \zeta_p^{j_1} A_1^{1/p} \beta/b^{1/p} \zeta_p^{j_1} \tilde{\sigma}_a(\beta)/b^{1/p}$$
$$\cdots$$
$$\tilde{\sigma}_a^p(A_1^{1/p}) = \zeta_p^{j_1 p} A_1^{1/p} \,\mathrm{Nm}(\beta)/b = A_1^{1/p}$$

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

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

We have

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

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

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

Hence, $\tilde{\sigma}_{A_1}$ 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 $\tilde{\sigma}_a(A_2)/A_2 = \beta^{p(p-1)/2}/\tilde{\sigma}_a(A_1) = \beta^{p(p-1)/2}b/(A_1\beta^p) \in K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p}$ and $\tilde{\sigma}_b(A_2)/A_2 = 1 \in K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p}$. And we know from last paragraph, $\mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p})/K)$ is generated by $\tilde{\sigma}_a, \tilde{\sigma}_b$. Hence for any $\sigma \in \mathrm{Gal}(K(a^{1/p}, b^{1/p}, A_1^{1/p})^{*p}/K)$, 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 $\tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_{A_1}$ 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 $\tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_{A_1}$ by a little abusing notation. Similarly, we will check that $\tilde{\sigma}_a, \tilde{\sigma}_b$ are mapped to $s, t_0 \in M_2$ and they satisfy the relations in the definition of M_2.

By lemma 24

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

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

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

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

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

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

We have

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

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

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

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

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

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

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

These imply that $\tilde{\sigma}_a, \tilde{\sigma}_b$ satisfies the relations in the definition of M_2. And $\tilde{\sigma}_{A_1}, \tilde{\sigma}_{A_2}$ 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 the same process and the calculation is tedious. We omit here.

□

Remark 19. The proof for the case M_1 is the same as the proof of theorem 22 in [9] and [13]. 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 25 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 26. *All proper defining systems with respect to χ can be obtained from the standard proper defining system by operations in lemma 7 and remark 8.*

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 25, 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 7

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

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

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

Then the lemma is followed by induction. □

In the lemma 25, 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 27. *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 writen in the form*

$K(a^{1/p}, b_0^{1/p}, (A_{0,1}b_1)^{1/p}, (A_{0,2}A_{1,1}b_2)^{1/p}, (A_{0,3}A_{1,2}A_{2,1}b_3)^{1/p}, \cdots, (A_{0,n-2}A_{1,n-3}\cdots A_{n-2,1}b_{n-2})^{1/p})$ *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* $0 \leq i \leq n-3$ *and* $A_{i,j} := \prod_{k=0}^{p-1} \sigma_a^k(\beta_i^{\binom{k}{j}})$

Proof. The result directly follows from lemma 26 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 25. Check that the field extension is Galois extension and $\tilde{\sigma}_a$ and $\tilde{\sigma}_{b_0}$ are generators of M_n and satisfy the relations. 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 28. *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 $K_1 = K\mathbb{Q}_1$.

Lemma 29. *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* $\log_p(\alpha) \cong 0 \mod p^2$ *where* $\log_p$ *is the* p*-adic log.*

Proof. Let $p\mathcal{O}_K = \mathfrak{P}_0\tilde{\mathfrak{P}}_0$ and $p\mathcal{O}_{K_1} = \mathfrak{P}_1\tilde{\mathfrak{P}}_1$. Let $K_{\mathfrak{P}_0}$ and $K_{\tilde{\mathfrak{P}}_0}$ be the completion of K at prime $\mathfrak{P}_0$ and $\tilde{\mathfrak{P}}_0$ respectively. Similarly for the definition $K_{1,\mathfrak{P}_1}$ and $K_{1,\tilde{\mathfrak{P}}_1}$. We will use Poitou-Tate Duality which is the theorem 8.6.7 in [11]. We use the same notation as in chapter 8.6 of [11]. 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 [11] 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 [11], 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 $H^2(G_{K,S}, \mu_p) \to H^2(G_{K_{\mathfrak{P}_0}}, \mu_p) \oplus H^2(G_{K_{\tilde{\mathfrak{P}}_0}}, \mu_p)$ 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 $H^2(G_{K_{\tilde{\mathfrak{P}}_0}}, \mu_p)$. 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 $\tilde{\mathfrak{P}}_0$. Hence $\log_p(\alpha) = 0 \mod p^2$ if and only if $\chi \cup \psi_0 = 0$ □

Remark 20. The value $\log_p \alpha$ depends on the embedding $K \to \mathbb{Q}_p^{sep}$. But the criterion $\log_p(\alpha) \equiv 0 \bmod p^2$ does not depend on the embedding.

Here is the relation between our result and the classical result Gold criterion [2]

Theorem 30. *Let K be a imaginary quadratic field, $p \nmid h_K$, p split in K i.e. $\mathfrak{P}\mathcal{O}_K = \mathfrak{P}_0\tilde{\mathfrak{P}}_0$. Take $(\alpha) = \mathfrak{P}_0^{h_K}$, then $\lambda \geq 2 \Leftrightarrow$ the cup product $\chi \cup \alpha = 0 \Leftrightarrow \log_p(\alpha) \equiv 0 \bmod p^2 \Leftrightarrow \alpha^{p-1} \equiv 1 \mod \tilde{\mathfrak{P}}_0^2$ where $\log_p$ is p-adic log.*

Proof. We only need to prove the last equivalent relation. Complete K at $\tilde{\mathfrak{P}}_0$, We have $K_{\tilde{\mathfrak{P}}_0} \cong \mathbb{Q}_p$ and $\alpha \in \mathbb{Z}_p^* \cong \mathbb{F}_p^* \oplus 1 + p\mathbb{Z}_p$. And $\log_p(\alpha) \equiv 0 \bmod p^2 \Longleftrightarrow \alpha \in \mathbb{F}_p^* \oplus 1 + p^2\mathbb{Z}_p \Longleftrightarrow \alpha^{p-1} \equiv 1 \mod p^2$ in $\mathbb{Q}_p \Longleftrightarrow \alpha^{p-1} \equiv 1 \mod \tilde{\mathfrak{P}}_0^2$ 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 the 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 28, 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 29).
(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 29, 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 29 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 $G_{K_{\bar{\mathfrak{P}}_0}}$, we get the same result. Since $H^2(G_{K,S}, \mu_p) \to H^2(G_{K_{\mathfrak{P}_0}}, \mu_p) \oplus H^2(G_{K_{\bar{\mathfrak{P}}_0}}, \mu_p)$ is injective, we conclude the Massey product vanishing if and only if $\log_p(\alpha) \equiv 0 \mod p^2$.)

(4) Assume $\lambda \geq 3$, then $\chi \cup \alpha_1 = 0 \iff \exists \beta_1 \in K_1^*$ 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 25 and lemma 26.)

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 $\lambda \geq 4 \iff \chi \cup \alpha_2 = 0 \iff \log_p \alpha_2 \equiv 0 \mod p^2$.(Reason: similar as previous case.)

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

Remark 21. The numerical criterion is not perfect, we only know the existence of β_i and α_1 and we do not have a logarithm to compute them.

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

Lemma 31. *Let K be a imaginary quadratic field, $p \nmid h_K$, p split in K i.e. $\mathfrak{P}\mathcal{O}_K = \mathfrak{P}_0\tilde{\mathfrak{P}}_0$. 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 29). 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 22. 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 $\mathrm{Cl}(K)[p^\infty] = \mathbb{Z}/p^l\mathbb{Z}$. 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 32. *Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty] = \mathbb{Z}/p^n\mathbb{Z}$. 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 23. It is well known that $\lambda \geq 1$ is always true in the case.

proof of theorem 32.

In this case, we have $\mathrm{Cl}(K_l)[p^\infty]^+ = 0$ by Proposition 13.22 in [15]. 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 17. 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 13 implies

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

By the exact sequence (1),

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

we know that $H^1(G_{K,S}, \mu_p)$ is generated by p and α. A similar argument as in theorem 20, 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 10, $\mathrm{Im}\,\Psi^{(n-1)}$ 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 8. □

5.1.4. *case 3.* Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty] = \mathbb{Z}/p^l\mathbb{Z}$. 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 33. *Let K be an imaginary quadratic field and $\mathrm{Cl}(K)[p^\infty]$ be a 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 24. It is well known that $\lambda \geq 1$ is always true in the case.

proof of theorem 33 .

Similar as Theorem 32, 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 13. The same argument as Theorem 32 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 [15], $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ 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, in other words, we have $\varepsilon_i X = \Lambda/(f_i)$. Notice that by Theorem 10.16 in [15], $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ 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 34. *Let $K = \mathbb{Q}(\mu_p)$. Fix $i = 3, 5, \cdots p-2$ and assume that $\varepsilon_i\mathrm{Cl}(K)[p^\infty]$ is cyclic. 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 34 .

Our case satisfies the setting up in Theorem 15, 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 15, 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 $\Psi^{(j)}|_{\varepsilon_i H^2(G_{K,S}, \Omega/I^n \otimes \mu_p)} = 0$ for $0 \leq j < n-1$. So $\mathrm{Im}\ \Psi^{(n-1)}|_{\varepsilon_i H^2(G_{K,S}, \Omega/I^{n-1} \otimes \mu_p)}$ is generated by $\Psi^{(n-1)}|_{\varepsilon_i H^2(G_{K,S}, \Omega/I^{n-1} \otimes \mu_p)}([\alpha_i])$. And $\Psi^{(n-1)}|_{\varepsilon_i H^2(G_{K,S}, \Omega/I^{n-1} \otimes \mu_p)}([\alpha_i]) = \varepsilon_i\Psi^{(n-1)}(f)$ 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 25. This is a generalization of McCallum and Sharifi's result of proposition 4.2 in [7].

References

[1] William G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), no. 2, 177–190. MR385851

[2] Robert Gold, *The nontriviality of certain Z_1-extensions*, J. Number Theory **6** (1974), 369–373. MR369316

[3] Manfred Kolster, *K-theory and arithmetic*, Contemporary developments in algebraic K-theory, 2004, pp. 191–258. MR2175640

[4] David Kraines, *Massey higher products*, Trans. Amer. Math. Soc. **124** (1966), 431–449. MR202136

[5] Yeuk Hay Joshua Lam, Yuan Liu, Romyar Sharifi, Preston Wake, and Jiuya Wang, *Generalized Bockstein maps and Massey products*, Forum Math. Sigma **11** (2023), Paper No. e5, 41. MR4537772

[6] Ivan Limonchenko and Dmitry Millionshchikov, *Higher order Massey products and applications*, Topology, geometry, and dynamics—V. A. Rokhlin-Memorial, [2021] ©2021, pp. 209–240. MR4305541

[7] William G. McCallum and Romyar T. Sharifi, *A cup product in the Galois cohomology of number fields*, Duke Math. J. **120** (2003), no. 2, 269–310. MR2019977

[8] J.S. Milne, *Class field theory (v4.03)*, 2020. Available at www.jmilne.org/math/.

[9] Ján Mináč and Nguyễn Duy Tân, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc. (2) **94** (2016), no. 3, 909–932. MR3614934

[10] ———, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. (JEMS) **19** (2017), no. 1, 255–284. MR3584563

[11] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Second, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026

[12] Romyar T. Sharifi, *Massey products and ideal class groups*, J. Reine Angew. Math. **603** (2007), 1–33. MR2312552

[13] Romyar Thomas Sharifi, *Twisted Heisenberg representations and local conductors*, ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–The University of Chicago. MR2716836

[14] John Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274. MR429837

[15] Lawrence C. Washington, *Introduction to cyclotomic fields*, Second, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575

Michigan State University, East Lansing, Michigan, USA
Email address: qipeikai@msu.edu