TRIPLE MASSEY PRODUCTS VANISH OVER ALL FIELDS

JÁN MINÁČ AND NGUYỄN DUY TÂN

ABSTRACT. We show that the absolute Galois group of any field has the vanishing triple Massey product property. Several corollaries for the structure of maximal pro-p-quotient of absolute Galois groups are deduced. Furthermore, the vanishing of some higher Massey products is proved.

1. INTRODUCTION

Let F be a field and F_s a separable closure of F. The Galois group $G_F := \mathrm{Gal}(F_s/F)$ is called the absolute Galois group of F. Every such Galois group is a profinite group. One may ask what special properties absolute Galois groups have among all profinite groups. This is a difficult problem, and at this moment only few properties have been found. However those discovered properties are of great interest and considerable depth.

In the classical papers [AS1, AS2] published in 1927, E. Artin and O. Schreier developed a theory of real fields, and they showed in particular that the only non-trivial finite subgroups of absolute Galois groups are groups of order 2. More recently, in some remarkable work M. Rost and V. Voevodsky proved the Bloch-Kato conjecture, thereby establishing a very special property of Galois cohomology of absolute Galois groups. Relatively recently, two new conjectures, the Vanishing n-Massey Conjecture and the Kernel n-Unipotent Conjecture were proposed (see [MT1] and [MT2]). These conjectures are based on a number of previous considerations. One motivation is coming from topological considerations. (See [DGMS] and [HW].) Another motivation is a program to describe various n-central series of absolute Galois groups as kernels of simple Galois representations. (See [Ef, EM1, EM2, MSp, Vi].)

In this paper we shall consider only the special case of the Vanishing n-Massey Conjecture when $n = 3$ with the exception of Section 5 when we consider $n > 3$ as well. In the papers [MT1, MT2], the Vanishing n-Massey Conjecture was formulated only in the case when the base field F contains a primitive p-th root of unity. In this paper we consider a stronger version of this conjecture when there is no condition on the field F. For the sake of simplicity we shall recall below the definition of n-Massey products only in the case $n = 3$, and we refer the reader to [MT1, Sections 2 and 3] for the more general case. See [MT1, Definition 3.3] for a definition of the vanishing n-fold Massey product

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. NDT is partially supported by the National Foundation for Science and Technology Development (NAFOSTED).

property. Also see Section 5 for reviews of some basic definitions and facts related to n-fold Massey products.

Conjecture 1.1 (Vanishing n-Massey Conjecture). *Let p be a prime number and $n \geq 3$ an integer. Let F be a field. Then the absolute Galois group G_F of F has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$.*

Let G be a profinite group and p a prime number. We consider the finite field $\mathbb{F}_p$ as a trivial discrete G-module. Let $\mathcal{C}^\bullet = (C^\bullet(G,\mathbb{F}_p),\partial,\cup)$ be the differential graded algebra of inhomogeneous continuous cochains of G with coefficients in $\mathbb{F}_p$ (see [NSW, Ch. I, §2] and [MT1, Section 3]). We write $H^i(G,\mathbb{F}_p)$ for the corresponding cohomology groups. We denote by $Z^1(G,\mathbb{F}_p)$ the subgroup of $C^1(G,\mathbb{F}_p)$ consisting of all 1-cocycles. Because we use trivial action on the coefficients $\mathbb{F}_p$, we have $Z^1(G,\mathbb{F}_p) = H^1(G,\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p)$. Let χ_1,χ_2,χ_3 be elements in $H^1(G,\mathbb{F}_p)$. Assume that

$$\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0 \in H^2(G,\mathbb{F}_p).$$

In this case we say that the triple Massey product $\langle \chi_1,\chi_2,\chi_3\rangle$ is defined. Then there exist cochains D_{12} and D_{23} in $C^1(G,\mathbb{F}_p)$ such that

$$\partial D_{12} = \chi_1 \cup \chi_2 \text{ and } \partial D_{23} = \chi_2 \cup \chi_3$$

in $C^2(G,\mathbb{F}_p)$. Then we say that $D := \{\chi_1,\chi_2,\chi_3,D_{12},D_{23}\}$ (or sometimes for simplicity $\{D_{12},D_{23}\}$) is a defining system for the triple Massey product $\langle \chi_1,\chi_2,\chi_3\rangle$. Observe that

$$\partial(\chi_1 \cup D_{23} + D_{12} \cup \chi_3) = 0,$$

hence $\chi_1 \cup D_{23} + D_{12} \cup \chi_3$ is a 2-cocycle. We define the value $\langle \chi_1,\chi_2,\chi_3\rangle_D$ of the triple Massey product $\langle \chi_1,\chi_2,\chi_3\rangle$ with respect to the defining system D to be the cohomology class of $\chi_1 \cup D_{23} + \chi_3 \cup D_{12}$ in $H^2(G,\mathbb{F}_p)$. The set of all values $\langle \chi_1,\chi_2,\chi_3\rangle_D$ when D runs over the set of all defining systems, is called the triple Massey product $\langle \chi_1,\chi_2,\chi_3\rangle \subseteq H^2(G,\mathbb{F}_p)$. If $0 \in \langle \chi_1,\chi_2,\chi_3\rangle$, then we say that our triple Massey product vanishes. We say that G has the vanishing triple Massey product property (with respect to $\mathbb{F}_p$) if every triple Massey product vanishes whenever it is defined.

The Vanishing 3-Massey Conjecture then claims that for any field F and any prime p, the absolute Galois group G_F has the vanishing triple Massey product property. It was proved by M. Hopkins and K. Wickelgren in [HW] that if F is a global field of characteristic not 2 and $p = 2$, then G_F has the vanishing triple Massey product property. In [MT1] it was proved that the result of [HW] is valid for any field F. In [MT3] it was proved that G_F has the vanishing triple Massey product property with respect to $\mathbb{F}_p$ for any global field F containing a primitive p-th root of unity. In [EMa1], I. Efrat and E. Matzri provided alternative proofs for the above mentioned results in [MT1] and [MT3]. In [Ma], E. Matzri proved that for any prime p and for any field F containing a primitive p-th root of unity, G_F has the vanishing triple Massey product property. In this paper we shall provide a cohomological proof to the main result in [Ma] (see Theorem 4.10). We also remove the assumption that F contains a primitive p-th root of unity (see Theorem 4.15). Thus every absolute Galois group has the vanishing triple Massey product property. This is a fundamental new restriction on absolute Galois groups. See Subsection 4.3 for some significant consequences on the structure of quotients of absolute Galois groups.

The structure of our paper is as follows. In Section 2 we recall basic materials on the cohomology of bicyclic groups. In Section 3 we discuss Heisenberg extensions. In Section 4, by using the materials developed in Sections 2 and 3, we provide an alternative cohomological proof of Matzri's theorem on the vanishing of triple Massey products with respect to $\mathbb{F}_p$ when F contains a primitive p-th root of unity. Before we received a very nice preprint [Ma] from E. Matzri, we planned to make such a proof but we completed this proof only after we received his preprint. We also want to notice that by referring directly to some results in [Ti] (see Remark 4.6 for a brief explanation), one can avoid using materials in Section 2. However we think that Section 2 might be of independent interest. E.Matzri used in his work tools from the theory of central simple algebras. In our paper we use cohomological techniques instead. In Remark 4.11 we provide yet another short direct variant of the key part of the proof of Theorem 4.10. Considering the details of our proof makes it possible to prove the vanishing of triple Massey products in a more general setting. Consider a formation $\{G,\{G(K)\},N\}$, where G is a profinite group, $\{G(K)\}$ is a collection of open subgroups of G indexed by a set $\Sigma=\{K\}$, and N is a discrete G-module. (See [Se1, Chapter XI, §1] or [We, Chapter VI, Section 6.1] for a definition of a formation.) We shall call such a formation $\{G,\{G(K)\},N\}$ a *p-Kummer field formation* if it satisfies two axioms:

(1) For each open normal subgroup $G(K)$ of G, $H^1(G/G(K),N^{G(K)})=\{1\}$. (Here $N^{G(K)}$ is the set of elements of N which are fixed under the action of every element σ in $G(K)$.)
(2) There is a short exact sequence of G-module
$$1\longrightarrow \mathbb{Z}/p\mathbb{Z}\longrightarrow N \stackrel{x\mapsto x^p}{\longrightarrow} N\longrightarrow 1,$$
where G acts trivially on $\mathbb{Z}/p\mathbb{Z}$, and N is written in a multiplicative way.

Recall that axiom (1) above guarantees that each p-Kummer field formation is also a field formation. (See [We, Chapter 6, Section 6.2].) Our main interest is when $G=G_F$, the absolute Galois group of F, and Σ is the set of all finite separable extensions of F, and $N=F_s^\times$. But our approach is valid in this more general setting which may have applications in anabelian geometry. Also this approach clarifies the key properties of G which are sufficient for our proofs to go through. Nearly simultaneously with our arXiv posting of the first version of our paper, I. Efrat and E. Matzri posted [EMa2] on arXiv. The paper [EMa2] is a replacement of [Ma]. In [EMa2], I. Efrat and E. Matzri also provide a cohomological approach to Theorem 4.10. Their approach has a similar flavor to our proofs in this paper, but it is still different. We feel that both papers taken together provide a definite complementary insight to the new fundamental property of absolute Galois groups. As we mentioned above, in Remark 4.11 we provide the second alternative proof of the vanishing of triple Massey products. In this proof we are able to show a specific element of the triple Massey product which vanishes. In [MT4] we succeeded in extending the crucial ideas in this paper together with further ideas in Galois theory to find explicit constructions of Galois extensions L/F with $\mathrm{Gal}(L/F) \simeq \mathbb{U}_4(\mathbb{F}_p)$, for all fields F and all primes p. In Section 5 we prove the vanishing of $(k+1)$-fold Massey products of the form $\langle \chi_b, \chi_a, \ldots, \chi_a \rangle$ (k copies of χ_a) and the vanishing of $(k+2)$-fold Massey products of the form $\langle \chi_a, \chi_b, \chi_a, \ldots, \chi_a \rangle$ ($k+1$ copies of χ_a), where $k < p$. (See Theorem 5.10.) The first vanishing can be deduced also from the results in [Sha2], but the second vanishing appears to be new.

Acknowledgements: We are grateful to Jochen Gärtner and Adam Topaz with whom we initially began correspondence on the vanishing triple Massey products pursuing a different strategy. We are also grateful to Eliyahu Matzri for sending us his beautiful preprint [Ma] shortly before his arXiv posting. Although we did not yet discuss details of our paper with Ido Efrat, Eliyahu Matzri, Danny Neftin and Kirsten Wickelgren, we thank them for their interest and great encouragement.

2. COHOMOLOGY OF BICYCLIC GROUPS

In this section we study the cohomology of cyclic and bicyclic groups. A number of basic results which we will need subsequently in this paper, are recalled here. Our main references are [CKM, pages 16-19] and [Me, pages 694-697].

2.1. **Cohomology of cylic groups.** If G is abelian group and $g \in G$ is an element of order n, we denote

$$D_g := g - 1 \text{ and } N_g := 1 + g + \cdots + g^{n-1} \in \mathbb{Z}[G].$$

Let G be a cyclic group of order n. We choose a generator s of G. Recall that $\epsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ is the augmentation homomorphism with $\epsilon(g) = 1$ for all $g \in G$. Then we have the following resolution of the trivial G-module $\mathbb{Z}$:

$$\cdots \longrightarrow \mathbb{Z}[G] \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

where d_i is multiplication by D_s (resp. N_s) if i is even (resp. odd). For any G-module M, the above resolution determines a complex

$$\mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{d_0^*} \mathrm{Hom}_G(\mathbb{Z}[G]^2, M) \xrightarrow{d_1^*} \mathrm{Hom}_G(\mathbb{Z}[G]^3, M) \longrightarrow \cdots$$

We make the natural identifications $\mathrm{Hom}_G(\mathbb{Z}[G]^i, M) = M^i$. Then the above complex becomes

$$M \xrightarrow{d_0^*} M^2 \xrightarrow{d_1^*} M^3 \xrightarrow{d_2^*} M^4 \longrightarrow \cdots$$

This implies in particularly that

$$H^2(G, M) \simeq \hat{H}^0(G, M) := \ker D_s/\mathrm{im} N_s = M^s/M_s A$$

As explained in [Se1, Chapter VIII, §4], the above isomorphism does depend on the choice of generator s and can be described as below. The choice of s defines a homomorphism $\chi^s\colon G \to \mathbb{Q}/\mathbb{Z}$ such that $\chi^s(s) = 1/n$. The coboundary $\delta\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \to$

$H^2(G,\mathbb{Z})$ associated to the short exact sequence of trivial G-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

sends χ^s to an element $\theta_s = \delta\chi^s \in H^2(G,\mathbb{Z})$. Then the isomorphism

$$M^s/N_sM \simeq H^2(G,M),$$

is the map which sends $x \in M$ to $x \cup \delta\chi^s$.

2.2. **Cohomology of bicyclic groups.** Let G be a bicyclic group. We choose two generators s, of order m, and t, of order n.

We define a chain complex $L_\bullet = (L_i)$ as follows: $L_i = \mathbb{Z}[G]^{i+1}$ for all $i \geq 0$, and $d_i \colon L_{i+1} \to L_i$ are defined by the following conditions

$$\begin{aligned}
d_{2i}e_{2j} &= N_se_{2j-1} + D_te_{2j},\\
d_{2i}e_{2j+1} &= D_se_{2j} - N_te_{2j+1},\\
d_{2i+1}e_{2j} &= N_se_{2j-1} + N_te_{2j},\\
d_{2i+1}e_{2j+1} &= D_se_{2j} - D_te_{2j+1},
\end{aligned}$$

here, for convenience, we put $e_{-1} = 0$ and $(e_0,\ldots,e_i)$ is the canonical basis of $L_i = \mathbb{Z}[G]^{i+1}$. Then we obtain a free resolution of the trivial G-module $\mathbb{Z}$:

$$\cdots \longrightarrow \mathbb{Z}[G]^4 \xrightarrow{d_2} \mathbb{Z}[G]^3 \xrightarrow{d_1} \mathbb{Z}[G]^2 \xrightarrow{d_0} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0. \tag{1}$$

We define $I := \ker\epsilon$, the augmentation ideal of $\mathbb{Z}[G]$; and $J := \ker d_0$. Then we obtain the following exact sequence of $\mathbb{Z}[G]$-modules

$$0 \longrightarrow J \longrightarrow \mathbb{Z}[G]^2 \xrightarrow{f} I \longrightarrow 0, \tag{2}$$

where $f(x,y) = d_0(x,y) = D_tx + D_sy$. We also consider the following exact sequence

$$0 \longrightarrow \mathbb{Z}[G]/\mathbb{Z}N_G \xrightarrow{g} J \xrightarrow{h} \mathbb{Z}^2 \longrightarrow 0, \tag{3}$$

where $N_G = \sum_{\sigma\in G}\sigma$, $g(x+\mathbb{Z}N_G) = (D_tx, -D_sx)$ and $h(x,y) = (\epsilon(x)/n, \epsilon(y)/m)$.

Now let M be any G-module. The resolution (1) yields the following complex

$$\mathrm{Hom}_G(\mathbb{Z}[G],M) \xrightarrow{d_0^*} \mathrm{Hom}_G(\mathbb{Z}[G]^2,M) \xrightarrow{d_1^*} \mathrm{Hom}_G(\mathbb{Z}[G]^3,M) \xrightarrow{d_2^*} \mathrm{Hom}_G(\mathbb{Z}[G],M) \to \cdots$$

We make the natural identifications $\mathrm{Hom}_G(\mathbb{Z}[G]^i,M) = M^i$. Then the above complex becomes

$$M \xrightarrow{d_0^*} M^2 \xrightarrow{d_1^*} M^3 \xrightarrow{d_2^*} M^4 \longrightarrow \cdots$$

The explicit descriptions of some maps d_i^* in matrix form are given below:

$$d_0^* = \begin{bmatrix} D_t \\ D_s \end{bmatrix}, d_1^* = \begin{bmatrix} N_t & 0 \\ D_s & -D_t \\ 0 & N_s \end{bmatrix}, d_2^* = \begin{bmatrix} D_t & 0 & 0 \\ D_s & -N_t & 0 \\ 0 & N_s & D_t \\ 0 & 0 & D_s \end{bmatrix}.$$

In particular we have

$$\begin{aligned}
Z^2(G,M) &:= \ker d_2^* = \{(x,y,z)\in M^3 \mid D_t(x)=0, D_s(z)=0, D_s(x)=N_t(y), D_t(z)=-N_s(z)\},\\
B^2(G,M) &:= \mathrm{im} d_1^* = \{(x,y,z)\in A^3 \mid \exists (c,d)\in A^2 : x=N_t(c), y=D_s(c)-D_t(d), z=N_s(d)\},\\
H^2(G,M) &\simeq Z^2(G,M)/B^2(G,M).
\end{aligned}$$

The exact sequences (2) and (3) yield the following commutative diagram
(*)

$$\begin{array}{ccccccc}
 & & \mathrm{Hom}_G(\mathbb{Z}^2,M) & \overset{u}{\searrow} & & & \\
 & & \downarrow & & & & \\
\mathrm{Hom}_G(\mathbb{Z}[G]^2,M) & \longrightarrow & \mathrm{Hom}_G(J,M) & \longrightarrow & \mathrm{Ext}^1_G(I,M) & \longrightarrow & 0=\mathrm{Ext}^1_G(\mathbb{Z}[G]^2,M)\\
 & \overset{v}{\searrow} & \downarrow & & & & \\
 & & \mathrm{Hom}_G(\mathbb{Z}[G]/\mathbb{Z}N_G,M) & & & & \\
 & & \downarrow & & & & \\
 & & \mathrm{Ext}^1_G(\mathbb{Z}^2,M) & & & &
\end{array}.$$

This diagram implies that we have a natural injection

$$\eta\colon \mathrm{coker}(u)\hookrightarrow \mathrm{coker}(v).$$

Note that η is an isomorphism if and only if $H^1(G,M)=0$ since $\mathrm{Ext}^1_G(\mathbb{Z}^2,M)=H^1(G,M)^2$. Under the natural identifications

$$\mathrm{Hom}_G(\mathbb{Z}^2,M)=(M^G)^2 \text{ and } \mathrm{Hom}_G(\mathbb{Z}[G]^i,M)=M^i,$$

we shall describe explicitly all objects and maps in the diagram.

First we have

$$\mathrm{Hom}_G(\mathbb{Z}[G]/\mathbb{Z}N_G,M)=\{x\in M\mid N_Gx=0\}=:{}_{N_G}M.$$

The map v becomes $v\colon M^2\longrightarrow {}_{N_G}M$, which sends (x,y) to D_tx-D_sy. This follows from the observation that the map v is obtained by applying the functor $\mathrm{Hom}_G(\cdot,M)$ to the composite $\mathbb{Z}[G]/\mathbb{Z}N_G\to J\to\mathbb{Z}[G]^2$, which maps $x \mod \mathbb{Z}N_G$ to $(D_tx,-D_sx)$.

On the other hand, the surjection $d_1\colon\mathbb{Z}[G]^3\twoheadrightarrow J$ yields an injection $\mathrm{Hom}_G(J,M)\hookrightarrow \mathrm{Hom}_G(\mathbb{Z}[G]^3,M)=M^3$. If we identify $\mathrm{Hom}_G(J,M)$ with its image in M^3, then

$$\mathrm{Hom}_G(J,M)=\ker d_2^*=:Z^2(G,M), \text{ and } \mathrm{Ext}^1_G(I,M)=\ker d_2^*/\mathrm{im} d_1^*=H^2(G,M).$$

The map u becomes $u\colon (M^G)^2\longrightarrow H^2(G,M)$, which can be described explicitly as follows. We consider the composite

$$\varphi\colon \mathbb{Z}[G]^3\xrightarrow{d_1} J\xrightarrow{h}\mathbb{Z}^2.$$

Then

$$\begin{aligned}\varphi(x,y,z) &= h(N_t x + D_s y, -D_t y + N_s z)\\ &= (\epsilon(N_t x + D_s y)/n, \epsilon(-D_t y + N_s z)/m)\\ &= (\epsilon(x), \epsilon(z)).\end{aligned}$$

The Hom-dual of φ is the map

$$\varphi^*\colon (M^G)^2 = \mathrm{Hom}_G(\mathbb{Z}^2, M) \longrightarrow \mathrm{Hom}_G(J, M) \hookrightarrow \mathrm{Hom}_G(\mathbb{Z}[G]^3, M) = M^3,$$

which is given by $\varphi^*(x,z) = (x,0,z)$. The map u is then given by

$$u(x,z) = [(x,0,z)],$$

where $[(x,0,z)]$ is the class of $(x,0,z)$ in $H^2(G,M)$.

Let $\sigma \in G/\langle t\rangle$ denote the class of s modulo $\langle t\rangle$. Then $G/\langle t\rangle = \langle\sigma\rangle$ is of order m. We have the natural identification $\hat{H}^0(G/\langle t\rangle, M^t) = M^G/N_\sigma(M^t) = H^2(G/\langle t\rangle, M)$ by identifying a with the cup product $a \cup \theta_\sigma$. (See Subsection 2.1.) Let $\chi^s\colon G \to \mathbb{Q}/\mathbb{Z}$ be a homomorphism such that $\chi^s(s) = 1/n$, $\chi^s(t) = 0$, and set $\theta_s := \delta\chi^s \in H^2(G,\mathbb{Z})$. Then we have

$$[(0,0,z)] = z \cup \theta_s = z \cup \delta\chi^s \in H^2(G,M).$$

This follows from an observation in [CKM, page 18] that the inflation map

$$\mathrm{inf}_{G/\langle t\rangle}\colon H^2(G/\langle t\rangle, M) \hookrightarrow H^2(G,M),$$

is given by

$$\mathrm{inf}_{G/\langle t\rangle}(z) = [(0,0,z)].$$

(Note also that $\chi^s = \mathrm{inf}_{G/\langle t\rangle}(\chi^\sigma)$ and $\theta_s = \mathrm{inf}_{G/\langle t\rangle}\theta_\sigma$.)

Similarly, we have

$$[(x,0,0)] = x \cup \theta_t = x \cup \delta\chi^t \in H^2(G,M).$$

Here $\chi^t\colon G \to \mathbb{Q}/\mathbb{Z}$ is a homomorphism such that $\chi^t(t) = 1/n$, $\chi^t(s) = 0$, and $\theta_t := \delta\chi^t \in H^2(G,\mathbb{Z})$. Therefore

$$u(x,z) = x \cup \delta\chi^t + z \cup \delta\chi^s.$$

Observe that we have the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z}[G] & \xrightarrow{x\mapsto(0,x,0)} & \mathbb{Z}[G]^3 \\ \downarrow & & \downarrow d_1 \\ \mathbb{Z}[G]/\mathbb{Z}[G]N_G & \xrightarrow{g} & J. \end{array}$$

This induces the following commutative diagram

$$\begin{array}{ccc}
\mathrm{Hom}_G(\mathbb{Z}[G]^3, M) = M^3 & \xrightarrow{(x,y,z)\mapsto y} & \mathrm{Hom}_G(\mathbb{Z}[G], M) = M \\
\uparrow & & \uparrow \\
\mathrm{Hom}_G(J, M) = Z^2(G,M) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G]/\mathbb{Z}N_G, M) = {}_{N_G}M
\end{array}$$

In summary, under the identifications $\mathrm{Hom}_G(\mathbb{Z}[G]^i, M) = M^i$, $\mathrm{Hom}_G(J, M) = Z^2(G,M)$, $\mathrm{Ext}^1_G(I, M) = Z^2(G,M)/B^2(G,M) = H^2(G,M)$, etc., the diagram (*) becomes

(**)
$$\begin{array}{ccccccc}
 & & (M^G)^2 & \overset{u}{\searrow} & & & \\
 & & \downarrow & & & & \\
M^2 & \longrightarrow & Z^2(G,M) & \longrightarrow & H^2(G,M) & \longrightarrow & 0 \\
 & \underset{v}{\searrow} & \downarrow & & & & \\
 & & {}_{N_G}M & & & & \\
 & & \downarrow & & & & \\
 & & H^1(G,M)^2 & & & &
\end{array}$$

Here

$$v(x,y) = D_t x - D_s y.$$
$$u(x,z) = x \cup \delta\chi^t + z \cup \delta\chi^s.$$

The natural injection $\eta\colon \mathrm{coker}(u) \hookrightarrow \mathrm{coker}(v)$ is given by

$$\eta([(x,y,z)]) = [y].$$

3. Heisenberg extensions

3.1. **Norm residue symbols.** Let F be a field containing a primitive p-th root of unity ξ. For any element a in $F^\times$, we shall write χ_a for the character corresponding to a via the Kummer map $F^\times \to H^1(G_F, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G_F, \mathbb{Z}/pZ)$. From now on we assume that a is not in $(F^\times)^p$. The extension $F(\sqrt[p]{a})/F$ is a Galois extension with Galois group $\langle\sigma_a\rangle \simeq \mathbb{Z}/p\mathbb{Z}$, where σ_a satisfies $\sigma_a(\sqrt[p]{a}) = \xi\sqrt[p]{a}$.

The character χ_a defines a homomorphism $\chi^a \in \mathrm{Hom}(G_F, \frac{1}{p}\mathbb{Z}/\mathbb{Z}) \subseteq \mathrm{Hom}(G_F, \mathbb{Q}/\mathbb{Z})$ by the formula

$$\chi^a = \frac{1}{p}\chi_a.$$

Let b be any element in $F^\times$. Then the norm residue symbol can be defined to be

$$(a,b) := (\chi^a, b) := b \cup \delta\chi^a.$$

The cup product $\chi_a \cup \chi_b \in H^2(G_F, \mathbb{Z}/p\mathbb{Z})$ can be interpreted as the norm residue symbol (a,b). More precisely, we consider the exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow F_s^\times \stackrel{x\mapsto x^p}{\longrightarrow} F_s^\times \longrightarrow 1,$$

where $\mathbb{Z}/p\mathbb{Z}$ has been identified with the group of p-th roots of unity μ_p via the choice of ξ. As $H^1(G_F, F_s^\times) = 0$, we obtain

$$0 \longrightarrow H^2(G_F, \mathbb{Z}/p\mathbb{Z}) \stackrel{i}{\longrightarrow} H^2(G_F, F_s^\times) \stackrel{\times p}{\longrightarrow} H^2(G_F, F_s^\times).$$

Then one has $i(\chi_a \cup \chi_b) = (a,b) \in H^2(G_F, F_s^\times)$. (See [Se1, Chapter XIV, Proposition 5].) The following fact ([Se1, Chapter XIV, Proposition 2]) will also be used frequently in the sequel.

Proposition 3.1. *We have*

$$\ker\left(H^2(G_F, F_s^\times) \stackrel{\mathrm{res}_{\ker \chi_a}}{\longrightarrow} H^2(G_{F(\sqrt[p]{a})}, F_s^\times)\right) = \{(a,b) \mid b \in F^\times\}.$$

3.2. **Heisenberg extensions.** In this subsection we provide a short alternative version of some materials in [Ma, Section 5]. (See also [Sha1, Chapter 2, Section 2.4].)

Assume that a, b are elements in $F^\times$, which are linearly independent modulo $(F^\times)^p$. Let $K = F(\sqrt[p]{a}, \sqrt[p]{b})$. Then K/F is a Galois extension whose Galois group is generated by σ_a and σ_b. Here $\sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}$, $\sigma_a(\sqrt[p]{a}) = \xi\sqrt[p]{a}$; $\sigma_b(\sqrt[p]{a}) = \sqrt[p]{a}$, $\sigma_b(\sqrt[p]{b}) = \xi\sqrt[p]{b}$.

Let $\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ be the group of all upper-triangular unipotent 3×3-matrix with entries in $\mathbb{Z}/p\mathbb{Z}$. We consider a map $\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^2$ which sends $\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}$ to (x,y). Then we have the following embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_F & & \\ & & & & & & \big\downarrow{\scriptstyle \bar\rho} & & \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & 1, \end{array}$$

where $\bar\rho$ is the map $(\chi_a, \chi_b)\colon G_F \to \mathrm{Gal}(K/F) \simeq (\mathbb{Z}/p\mathbb{Z})^2$. (The last isomorphism $\mathrm{Gal}(K/F) \simeq (\mathbb{Z}/p\mathbb{Z})^2$ is the one which sends σ_a to $(1,0)$ and σ_b to $(0,1)$.)

Assume that $\chi_a \cup \chi_b = 0$. Then the norm residue symbol (a,b) is trivial. Hence there exists α in $F(\sqrt[p]{a})$ such that $N_{F(\sqrt[p]{a})/F}(\alpha) = b$ (see [Se1, Chapter XIV, Proposition 4 (iii)]). We set

$$A_0 = \alpha^{p-1}\sigma_a(\alpha^{p-2})\cdots\sigma_a^{p-2}(\alpha) = \prod_{i=0}^{p-2}\sigma_a^i(\alpha^{p-i-1}) \in F(\sqrt[p]{a}).$$

Lemma 3.2. *Let f_a be an element in $F^\times$. Let $A = f_aA_0$. Then we have*

$$\frac{\sigma_a(A)}{A} = \frac{N_{F(\sqrt[p]{a})/F}(\alpha)}{\alpha^p} = \frac{b}{\alpha^p}.$$

Proof. Observe that $\dfrac{\sigma_a(A)}{A}=\dfrac{\sigma_a(A_0)}{A_0}$. The lemma then follows from the identity

$$(s-1)\sum_{i=0}^{p-2}(p-i-1)s^i=\sum_{i=0}^{p-1}s^i-ps^0. \qquad \square$$

For any representation $\rho\colon G_F\to \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ and $1\leq i<j\leq 3$, let $\rho_{ij}\colon G_F\to \mathbb{Z}/p\mathbb{Z}$ be the composition of ρ with the projection from $\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ to its (i,j)-coordinate.

Proposition 3.3. *Assume that $\chi_a\cup\chi_b=0$. Let f_a be an element in $F^\times$. Let $A=f_aA_0$ be defined as above. Then the homomorphism $\bar\rho:=(\chi_a,\chi_b)\colon G_F\to\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ lifts to a Heisenberg extension $\rho\colon G_F\to\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ with $\mathrm{res}_{\ker\chi_a}(\rho_{13})=\chi_A$.*

Proof. From $\sigma_a(A)/A=b/\alpha^p\in(K^\times)^p$, and $\sigma_b(A)=A$, we see that $\sigma(A)/A\in(K^\times)^p$ for every $\sigma\in\mathrm{Gal}(K/F)$. This implies that the extension $L:=K(\sqrt[p]{A})/F$ is Galois. Let $\tilde\sigma_a\in\mathrm{Gal}(L/F)$ (resp. $\tilde\sigma_b\in\mathrm{Gal}(L/F)$) be an extension of σ_a (resp. σ_b). Since $\sigma_b(A)=A$, we have $\tilde\sigma_b(\sqrt[p]{A})=\xi^j\sqrt[p]{A}$, for some $j\in\mathbb{Z}$. Hence $\tilde\sigma_b^p(\sqrt[p]{A})=\sqrt[p]{A}$. This implies that $\tilde\sigma_b$ is of order p.

On the other hand, we have

$$\tilde\sigma_a(\sqrt[p]{A})^p=\sigma_a(A)=A\frac{b}{\alpha^p}.$$

Hence $\tilde\sigma_a(\sqrt[p]{A})=\xi^i\sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}$, for some $i\in\mathbb{Z}$. Then

$$\tilde\sigma_a^p(\sqrt[p]{A})=\sqrt[p]{A}\frac{b}{N_{F(\sqrt[p]{a})/F}(\alpha)}=\sqrt[p]{A}.$$

This implies that $\tilde\sigma_a$ is also of order p. We have

$$\tilde\sigma_a\tilde\sigma_b(\sqrt[p]{A})=\tilde\sigma_a(\xi^j\sqrt[p]{A})=\xi^{i+j}\sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha},$$

$$\tilde\sigma_b\tilde\sigma_a(\sqrt[p]{A})=\tilde\sigma_b(\xi^i\sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha})=\xi^{i+j}\sqrt[p]{A}\frac{\xi\sqrt[p]{b}}{\alpha}.$$

We set $\tilde\sigma_A:=\tilde\sigma_a\tilde\sigma_b\tilde\sigma_a^{-1}\tilde\sigma_b^{-1}$. Then

$$\tilde\sigma_A(\sqrt[p]{A})=\xi\sqrt[p]{A}.$$

This implies that $\tilde\sigma_A$ is of order p and that $\mathrm{Gal}(L/F)$ is generated by $\tilde\sigma_a$ and $\tilde\sigma_b$. We also have

$$\tilde\sigma_a\tilde\sigma_A=\tilde\sigma_A\tilde\sigma_a,\ \text{ and }\tilde\sigma_b\tilde\sigma_A=\tilde\sigma_A\tilde\sigma_b.$$

We can define an isomorphism $\varphi\colon\mathrm{Gal}(L/F)\to\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ by letting

$$\tilde\sigma_a\mapsto x:=\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix},\tilde\sigma_b\mapsto y:=\begin{bmatrix}1&0&0\\0&1&1\\0&0&1\end{bmatrix},\tilde\sigma_A\mapsto z:=\begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix}.$$

Then the composition $\rho\colon G_F\to\mathrm{Gal}(L/F)\stackrel{\varphi}{\to}\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ is the desired lifting of $\bar\rho$. $\square$

Corollary 3.4. *Let the notation be as in Proposition 3.3. Let φ_{ab} be the map $-\rho_{13}\colon G_F \to \mathbb{Z}/p\mathbb{Z}$. Then*

$$d\varphi_{ab} = \chi_a \cup \chi_b \text{ and } \mathrm{res}_{\ker \chi_a}(\varphi_{ab}) = -\chi_A.$$

Proof. Since $\rho\colon G_F \to \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ is a homomorphism, we obtain

$$d\varphi_{ab}(\sigma,\tau) = \rho_{13}(\sigma\tau) - \rho_{13}(\sigma) - \rho_{13}(\tau) = \rho_{12}(\sigma)\rho_{23}(\tau) = (\chi_a \cup \chi_b)(\sigma,\tau).$$

Therefore $d\varphi_{ab} = \chi_a \cup \chi_b$, as desired. □

4. Triple Massey products

4.1. **Triple Massey products over fields containing primitive p-th roots of unity.** In this subsection we assume that F is a field containing a primitive p-th root of unity. Let a, b and c be elements in $F^\times$. Assume further that the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ is defined, i.e., we have $\chi_a \cup \chi_b = 0 = \chi_b \cup \chi_c$. Until Theorem 4.10, we always assume further that a and c are linearly independent modulo $(F^\times)^p$, and that a and b are linearly independent modulo $(F^\times)^p$. We also fix two elements f_a and f_c in $F^\times$. Let A_0 be the element defined right before Lemma 3.2. Let $A = f_a A_0$.

By Corollary 3.4, there is a map $\varphi_{ab}\colon G_F \to \mathbb{Z}/p\mathbb{Z}$ such that

$$d\varphi_{ab} = \chi_a \cup \chi_b \in C^2(G_F, \mathbb{Z}/p\mathbb{Z}) \text{ and } \mathrm{res}_{\ker \chi_a}(\varphi_{ab}) = -\chi_A.$$

Since $\chi_b \cup \chi_c = 0$ in $H^2(G_F, \mathbb{Z}/p\mathbb{Z})$, there exists a map $\varphi_{bc}\colon G_F \to \mathbb{Z}/p\mathbb{Z}$ such that

$$d\varphi_{bc} = \chi_b \cup \chi_c \in C^2(G_F, \mathbb{Z}/p\mathbb{Z}).$$

Then

$$\langle \chi_a, \chi_b, \chi_c \rangle_\varphi := \chi_a \cup \varphi_{bc} + \varphi_{ab} \cup \chi_c$$

is an element in the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$.

We consider the following commutative diagram

$$\begin{array}{ccc} H^2(G_F, \mathbb{Z}/p\mathbb{Z}) & \xhookrightarrow{\ i\ } & H^2(G_F, F_s^\times) \\ \big\downarrow{\scriptstyle \mathrm{res}_{\ker \chi_a}} & & \big\downarrow{\scriptstyle \mathrm{res}_{\ker \chi_a}} \\ H^2(G_{F(\sqrt[p]{a})}, \mathbb{Z}/p\mathbb{Z}) & \xhookrightarrow{\ i\ } & H^2(G_{F(\sqrt[p]{a})}, F_s^\times). \end{array}$$

Lemma 4.1. *We have*

(1) $\mathrm{res}_{\ker \chi_a}(\langle \chi_a, \chi_b, \chi_c \rangle_\varphi) = \mathrm{res}_{\ker \chi_a}(\chi_c) \cup \chi_A \in H^2(G_{F(\sqrt[p]{a})}, \mathbb{Z}/p\mathbb{Z})$.

(2) $\mathrm{res}_{\ker \chi_a}(i(\langle \chi_a, \chi_b, \chi_c \rangle_\varphi)) = (c, A) \in H^2(G_{F(\sqrt[p]{a})}, F_s^\times)$.

Proof. (1) We have

$$\begin{aligned} \mathrm{res}_{\ker \chi_a}(\langle \chi_a, \chi_b, \chi_c \rangle_\varphi) &= \mathrm{res}_{\ker \chi_a}(\chi_a \cup \varphi_{bc} + \varphi_{ab} \cup \chi_c) \\ &= \mathrm{res}_{\ker \chi_a}(\chi_a) \cup \mathrm{res}_{\ker \chi_a}(\varphi_{bc}) + \mathrm{res}_{\ker \chi_a}(\varphi_{ab}) \cup \mathrm{res}_{\ker \chi_a}(\chi_c) \\ &= -\chi_A \cup \mathrm{res}_{\ker \chi_a}(\chi_c) \\ &= \mathrm{res}_{\ker \chi_a}(\chi_c) \cup \chi_A. \end{aligned}$$

(2) This follows from (1) and the commutativity of the above diagram. □

Let $E = F(\sqrt[p]{a}, \sqrt[p]{c})$. Since $\chi_a \cup \chi_b = 0 = \chi_b \cup \chi_c$, we have $(a,b) = (b,c) = 0$. Thus there are α in $F(\sqrt[p]{a})$ and γ in $F(\sqrt[p]{c})$ such that

$$N_{E/F(\sqrt[p]{a})}(\alpha) = b = N_{E/F(\sqrt[p]{c})}(\gamma).$$

Let G be the Galois group $\mathrm{Gal}(E/F)$. Then $G = \langle \sigma_a, \sigma_c \rangle$, where $\sigma_a \in G$ (respectively $\sigma_c \in G$) is an extension of $\sigma_a \in \mathrm{Gal}(F(\sqrt[p]{a})/F)$ (respectively $\sigma_c \in \mathrm{Gal}(F(\sqrt[p]{c})/F)$). We define

$$C_0 = \prod_{i=0}^{p-2} \sigma_c^i(\gamma^{p-i-1}) \in F(\sqrt[p]{a}),$$

$C := f_c C_0$, and define $B := \gamma/\alpha$.

Lemma 4.2. *We have*

(1) $\dfrac{\sigma_a(A)}{A} = N_{\sigma_c}(B)$.
(2) $\dfrac{\sigma_c(C)}{C} = N_{\sigma_a}(B)^{-1}$.

Proof. (1) From Lemma 3.2, we have

$$\frac{\sigma_a(A)}{A} = \frac{b}{\alpha^p} = \frac{N_{\sigma_c}(\gamma)}{N_{\sigma_c}(\alpha)} = N_{\sigma_c}(B).$$

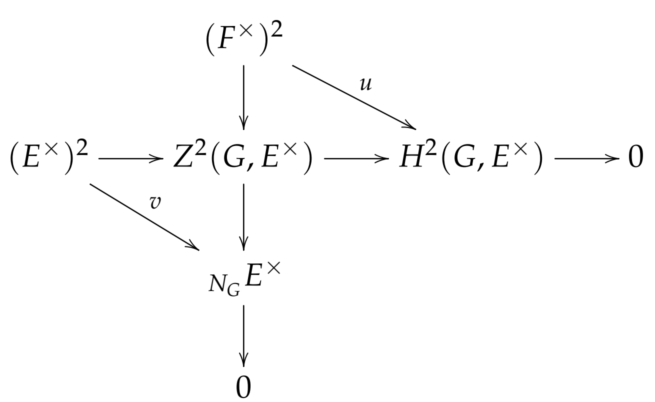
(2) From Lemma 3.2, we have

$$\frac{\sigma_c(C)}{C} = \frac{b}{\gamma^p} = \frac{N_{\sigma_a}(\alpha)}{N_{\sigma_a}(\gamma)} = N_{\sigma_a}(B)^{-1}.$$

□

We consider $E^\times$ as a G-module under the Galois action. The diagram (**) in Subsection 2.2 becomes

(***)



Here

$$v(x,y) = \frac{\sigma_c(x)}{x}\frac{y}{\sigma_a(y)},$$
$$u(x,z) = x \cup \delta\chi^{\sigma_c} + z \cup \delta\chi^{\sigma_a}.$$

The natural isomorphism $\eta\colon \mathrm{coker}(u) \hookrightarrow \mathrm{coker}(v)$ is given by

$$\eta[(x,y,z)] = [y].$$

Corollary 4.3. *The triple (A,B,C) is an element in $Z^2(G,E^\times)$.*

Proof. This follows immediately from the previous lemma. □

Lemma 4.4. *The element $[(A,B,C)]$ is in the image of u.*

Proof. Since η is an isomorphism, it suffices to show that $\eta[(A,B,C)]$ is in the image of v.

We have

$$N_{\sigma_a\sigma_c}(B) = \frac{N_{\sigma_a\sigma_c}(\alpha)}{N_{\sigma_a\sigma_c}(\gamma)} = \frac{N_{\sigma_a}(\alpha)}{N_{\sigma_c}(\gamma)} = \frac{b}{b} = 1.$$

Hence by Hilbert's Theorem 90, there exists $e \in E^\times$ such that

$$B = \frac{\sigma_a\sigma_c(e)}{e} = \frac{\sigma_c(\sigma_a(e))}{\sigma_a(e)}\frac{e^{-1}}{\sigma_a(e^{-1})}.$$

Therefore B is in $\mathrm{im} v$, as desired. □

Corollary 4.5. *There exists $x,y \in F^\times$ such that*

$$\inf([(A,B,C)]) = (a,x) + (c,y) \in H^2(G_F, F_s^\times).$$

Proof. Since $[(A,B,C)]$ is in the image of u, there exist x and y in $F^\times$ such that

$$[(A,B,C)] = x \cup \delta\chi^{\sigma_a} + y \cup \chi^{\sigma_c}.$$

This implies that

$$\begin{aligned}\inf([(A,B,C)]) &= x \cup \delta(\inf(\chi^{\sigma_a})) + y \cup \delta(\inf(\chi^{\sigma_c}))\\ &= x \cup \delta\chi^a + y \cup \delta\chi^c\\ &= (x,a) + (y,b),\end{aligned}$$

as desired. □

Remark 4.6. Observe that $\mathrm{coker}(v) = \hat{H}^{-1}(G,E^\times)$. We can identify naturally the group $\mathrm{coker}(v)$ with group $\mathrm{U}_{\mathbf{b}}(G,E^\times)$ (the notation being as in [Ti]). (See [Ti, Remark after Corollary 1.6].) Then the composition map

$$H^2(G,E^\times) \to \mathrm{coker}(u) \xrightarrow{\eta} \mathrm{coker}(v) = \mathrm{U}_{\mathbf{b}}(G,E^\times),$$

is exactly the map which was denoted by ϵ in [Ti, page 423], $\epsilon\colon H^2(G,E^\times) \to \mathrm{U}_{\mathbf{b}}(G,E^\times)$. The proof of Lemma 4.4 shows that the element $[(A,B,C)]$ is in the kernel of ϵ.

We have the following exact sequence

$$0 \longrightarrow H^2(G,E^\times) \xrightarrow{\inf} H^2(G_F,F_s^\times) \xrightarrow{\mathrm{res}} H^2(G_E,F_s^\times).$$

If we make the natural identification $H^2(G_F,F_s^\times) = \mathrm{Br(F)}$ and $H^2(G_E,F_s^\times) = \mathrm{Br}(E)$, then one can check the map

$$\inf\colon H^2(G,E^\times) \xrightarrow{\simeq} \mathrm{Br}(E/F) := \ker(\mathrm{Br}(F)\to \mathrm{Br}(E)),$$

is the natural isomorphism $\pi\colon H^2(G,E^\times) \longrightarrow \mathrm{Br}(E/F)$ mentioned in [Ti, page 427]. Then Corollary 4.5 follows from [Ti, Proposition 1.5]. □

We consider the following commutative diagram

$$\begin{array}{ccccc}
H^2(G,E^\times) & \xhookrightarrow{\inf} & H^2(G_F,F_s^\times) & \xrightarrow{\mathrm{res}} & H^2(G_E,F_s^\times)\\
\downarrow{\scriptstyle \mathrm{res}_{G/\langle\sigma_a\rangle}} & & \downarrow{\scriptstyle \mathrm{res}_{\ker\chi_a}} & & \|\\
H^2(\langle\sigma_c\rangle,E^\times) & \xhookrightarrow{\inf} & H^2(G_{F(\sqrt[p]{a})},F_s^\times) & \xrightarrow{\mathrm{res}} & H^2(G_E,F_s^\times).
\end{array}$$

Lemma 4.7. *We have*

(1) $\mathrm{res}_{G/\langle\sigma_a\rangle}([A,B,C]) = A\cup\delta\chi^{\sigma_c} \in H^2(\langle\sigma_c\rangle,E^\times)$.
(2) $\mathrm{res}_{\ker\chi_a}(\inf([A,B,C])) = (c,A)$ *in* $H^2(G_{F(\sqrt[p]{a})},F_s^\times)$.

Proof. (1) By [CKM, page 17] and under the identification $(E^\times)^{\sigma_c}/N_{\sigma_c}(E^\times) = H^2(\langle\sigma_c\rangle,E^\times)$ via identifying x with the cup product $x\cup\delta(\chi^{\sigma_c})$, we have

$$\mathrm{res}_{G/\langle\sigma_a\rangle}([A,B,C]) = [A] = A\cup\delta\chi^{\sigma_c}.$$

(2) From the commutativity of the above diagram, we obtain

$$\begin{aligned}
\mathrm{res}_{\ker\chi_a}(\inf([A,B,C])) &= \inf(\mathrm{res}_{G/\langle\sigma_a\rangle}([A,B,C]))\\
&= \inf(A\cup\delta(\chi^{\sigma_c}))\\
&= A\cup\delta(\inf(\chi^{\sigma_c}))\\
&= A\cup\delta\chi^c\\
&= (c,A),
\end{aligned}$$

as desired. □

Corollary 4.8. *There exists $x\in F^\times$ such that*

$$i(\langle\chi_a,\chi_b,\chi_c\rangle_\varphi) = \inf([A,B,C]) + (a,x) \in H^2(G_F,F_s^\times).$$

Proof. From Lemma 4.1 and Lemma 4.7 we have

$$\mathrm{res}_{\ker\chi_a}(i(\langle\chi_a,\chi_b,\chi_c\rangle_\varphi)) = \mathrm{res}_{\ker\chi_a}(\inf([A,B,C])) \in H^2(G_{F(\sqrt[p]{a})},F_s^\times)).$$

The statement then follows from Proposition 3.1. □

Corollary 4.9. *There exist x and y in $F^\times$ such that*

$$\langle \chi_a, \chi_b, \chi_c\rangle_\varphi = \chi_a \cup \chi_x + \chi_c \cup \chi_y \in H^2(G_F, \mathbb{Z}/p\mathbb{Z}).$$

Proof. By Corollaries 4.5 and 4.8, there are x_1, x_2 and y in $F^\times$ such that

$$i(\langle \chi_a, \chi_b, \chi_c\rangle_\varphi) = \inf([A, B, C]) + (a, x_2) = (a, x_1) + (c, y) + (a, x_2) \in H^2(G_F, F_s^\times).$$

Let $x := x_1x_2$. Since $i\colon H^2(G_F, \mathbb{Z}/p\mathbb{Z}) \to H^2(G_F, F_s^\times)$ is injective, we obtain

$$\langle \chi_a, \chi_b, \chi_c\rangle_\varphi = \chi_a \cup \chi_x + \chi_c \cup \chi_y,$$

as desired. □

Theorem 4.10 (E. Matzri)**.** *Let F be a field containing a primitive p-th root of unity. Let a, b, c are elements in $F^\times$. The triple Massey product $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0 whenever it is defined.*

Proof. Assume that $\langle \chi_a, \chi_b, \chi_c\rangle$ is defined. We can also assume that a, b and c are not in $(F^\times)^p$.

Case 1: Assume that a and c are linearly dependent modulo $(F^\times)^p$. Let $\varphi = \{\varphi_{ab}, \varphi_{bc}\}$ be a defining system for $\langle \chi_a, \chi_b, \chi_c\rangle$. We have

$$\begin{aligned}
\mathrm{res}_{\ker \chi_a}(\langle \chi_a, \chi_b, \chi_c\rangle_\varphi) &= \mathrm{res}_{\ker \chi_a}(\chi_a \cup \varphi_{bc} + \varphi_{ab} \cup \chi_c)\\
&= \mathrm{res}_{\ker \chi_a}(\chi_a) \cup \mathrm{res}_{\ker \chi_a}(\varphi_{bc}) + \mathrm{res}_{\ker \chi_a}(\varphi_{ab}) \cup \mathrm{res}_{\ker \chi_a}(\chi_c)\\
&= 0 \cup \mathrm{res}_{\ker \chi_a}(\varphi_{bc}) + \mathrm{res}_{\ker \chi_a}(\varphi_{ab}) \cup 0\\
&= 0.
\end{aligned}$$

By Proposition 3.1, $\langle \chi_a, \chi_b, \chi_c\rangle_\varphi = \chi_a \cup \chi_x$ for some $x \in F^\times$. This implies that $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0.

Case 2: Assume that a and b are linearly dependent modulo $(F^\times)^p$. Then $\chi_c = \lambda\chi_a$, for some $k \in \mathbb{Z}/p\mathbb{Z}$. By the linearity of Massey products, we have

$$\lambda\langle \chi_a, \chi_a, \chi_c\rangle \subseteq \langle \chi_a, \lambda\chi_a, \chi_c\rangle = \langle \chi_a, \chi_b, \chi_c\rangle.$$

(See [Fe, Lemma 6.2.4 (ii)].) So it is enough to show that $\langle \chi_a, \chi_a, \chi_c\rangle$ contains 0. If $p = 2$ then $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0 by [MT1, Theorem 1.2]. So we can assume that $p > 2$. We define

$$\varphi_{aa} := -\frac{\chi_a^2}{2}.$$

Then it is straightforward to check that

$$d\varphi_{aa}(\sigma, \tau) = \varphi_{aa}(\sigma) + \varphi_{aa}(\tau) - \varphi_{aa}(\sigma\tau) = \chi_a(\sigma)\chi_a(\tau) = \chi_a \cup \chi_a(\sigma, \tau).$$

We pick any map $\varphi_{ac}\colon G_F \to \mathbb{Z}/p\mathbb{Z}$ such that $d\varphi_{ac} = \chi_a \cup \chi_c$. Then $\{\varphi_{aa}, \varphi_{ac}\}$ is a defining system for $\langle \chi_a, \chi_a, \chi_c\rangle$. We have

$$\begin{aligned}
\mathrm{res}_{\ker\chi_a}(\langle \chi_a,\chi_a,\chi_c\rangle_\varphi) &= \mathrm{res}_{\ker\chi_a}(\chi_a\cup\varphi_{ac}+\varphi_{aa}\cup\chi_c)\\
&= \mathrm{res}_{\ker\chi_a}(\chi_a)\cup \mathrm{res}_{\ker\chi_a}(\varphi_{ac}) + \mathrm{res}_{\ker\chi_a}(\varphi_{aa})\cup\mathrm{res}_{\ker\chi_a}(\chi_c)\\
&= 0\cup \mathrm{res}_{\ker\chi_a}(\varphi_{ac}) + 0\cup \mathrm{res}_{\ker\chi_a}(\chi_c)\\
&= 0.
\end{aligned}$$

By Proposition 3.1, $\langle \chi_a,\chi_a,\chi_c\rangle_\varphi = \chi_a\cup\chi_x$ for some $x\in F^\times$. This implies that $\langle \chi_a,\chi_a,\chi_c\rangle$ contains 0, as desired. (This also follows from a more general result [Sha2, Proposition 4.2]. See also Theorem 5.10.)

Case 3: Assume that a and c are linearly independent and that a and b are linearly independent. Then Corollary 4.9 implies that the triple Massey product $\langle \chi_a,\chi_b,\chi_c\rangle$ contains 0. □

Remark 4.11. In Case 3 in the above proof, we can show that a specific element of the Massey triple product vanishes. This leads to another proof for this case and hence for Theorem 4.10, which avoids using Corollary 4.5. In a part of our proof below, we uses a similar argument to the argument in [Wa, Proof of Lemma 2.14].

Theorem 4.12. *There exists f_a, f_c in $F^\times$ such that (f_aA_0, B, f_cC_0) is a coboundary.*

Proof. As in the proof of Lemma 4.4, there exists $e\in E^\times$ such that $B = \dfrac{\sigma_a\sigma_c(e)}{e}$.

By Lemma 4.2, we have

$$\frac{\sigma_a(A_0)}{A_0} = N_{\sigma_c}(B) = N_{\sigma_c}\left(\frac{\sigma_a\sigma_c(e)}{e}\right) = \frac{\sigma_a(N_{\sigma_c}(e))}{N_{\sigma_c}(e)}.$$

This implies that

$$\frac{N_{\sigma_c}(e)}{A_0} = \sigma_a\left(\frac{N\sigma_c(e)}{A_0}\right).$$

Hence

$$\frac{N_{\sigma_c}(e)}{A_0}\in F(\sqrt[p]{c})^\times \cap F(\sqrt[p]{a})^\times = F^\times.$$

Therefore, there exists $f_a\in F^\times$ such that $N_{\sigma_c}(e) = A_0 f_a$.

Similarly, by Lemma 4.2, we have

$$\frac{\sigma_c(C_0)}{C_0} = N_{\sigma_a}(B^{-1}) = N_{\sigma_a}\left(\frac{\sigma_a\sigma_c(e^{-1})}{e^{-1}}\right) = \frac{\sigma_c(N_{\sigma_a}(e^{-1}))}{N_{\sigma_a}(e^{-1})}.$$

This implies that

$$\frac{N_{\sigma_a}(e^{-1})}{C_0} = \sigma_c\left(\frac{N\sigma_a(e^{-1})}{C_0}\right).$$

Hence

$$\frac{N_{\sigma_a}(e^{-1})}{C_0} \in F(\sqrt[p]{a})^\times \cap F(\sqrt[p]{c})^\times = F^\times.$$

Therefore, there exists $f_c \in F^\times$ such that $N_{\sigma_a}(e^{-1}) = C_0 f_c$.

Let $C_1 = \sigma_c(e)$ and $C_2 = e^{-1}$. Then we have

$$\begin{aligned} B &= \frac{\sigma_a\sigma_c(e)}{e} = \frac{\sigma_a(\sigma_c(e))}{\sigma_c(e)}\frac{e^{-1}}{\sigma_c(e^{-1})} = \frac{\sigma_a(C_1)}{C_1}\frac{C_2}{\sigma_c(C_2)}, \\ N_{\sigma_c}(C_1) &= N_{\sigma_c}(\sigma_c(e)) = N_{\sigma_c}(e) = A_0 f_a, \\ N_{\sigma_a}(C_2) &= N_{\sigma_a}(e^{-1}) = C_0 f_c. \end{aligned}$$

This implies that $(A_0 f_a, B, C_0 f_c)$ is in $B^2(G, E^\times)$. □

Observe that Corollary 4.8 says that $\inf([A_0 f_a, B, C_0 f_c])$ is in $i(\langle \chi_a, \chi_b, \chi_c\rangle)$. Hence $\langle \chi_a, \chi_b, \chi_c\rangle$ contains $i^{-1}(\inf([A_0 f_a, B, C_0 f_c])) = 0$. □

4.2. **Embedding problems and triple Massey products over an arbitrary field.** A *weak embedding problem* $\mathcal{E}$ for a profinite group Π is a diagram

$$\mathcal{E} := \quad \begin{array}{ccc} & & \Pi \\ & & \downarrow{\scriptstyle \alpha} \\ U & \xrightarrow{f} & \bar{U} \end{array}$$

which consists of profinite groups U and $\bar{U}$ and homomorphisms $\alpha\colon \Pi \to \bar{U}$, $f\colon U \to \bar{U}$ with f being surjective. (All homomorphisms of profinite groups considered in this paper are assumed to be continuous.) If in addition α is also surjective, we call $\mathcal{E}$ an *embedding problem*.

A *weak solution* of $\mathcal{E}$ is a homomorphism $\beta\colon \Pi \to U$ such that $f\beta = \alpha$. We call $\mathcal{E}$ a *finite* weak embedding problem if group U is finite. The *kernel* of $\mathcal{E}$ is defined to be $N := \ker(f)$.

Let $\mathbb{U}_4(\mathbb{F}_p)$ be the group of all upper-triangular unipotent 4×4-matrices with entries in $\mathbb{F}_p$. Let Z be the subgroup of all such matrices with all off-diagonal entries being 0 except at position $(1,4)$. We may identify $\mathbb{U}_4(\mathbb{F}_p)/Z$ with the group $\bar{\mathbb{U}}_4(\mathbb{F}_p)$ of all upper-triangular unipotent 4×4-matrices with entries over $\mathbb{F}_p$ with the $(1,4)$-entry omitted. For any representation $\rho\colon G \to \mathbb{U}_4(\mathbb{F}_p)$ and $1 \le i < j \le 4$, let $\rho_{ij}\colon G \to \mathbb{F}_p$ be the composition of ρ with the projection from $\mathbb{U}_4(\mathbb{F}_p)$ to its (i,j)-coordinate. We use similar notation for representations $\bar{\rho}\colon G \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$. Note that for each $i = 1,2,3$, $\rho_{i,i+1}$ (resp., $\bar{\rho}_{i,i+1}$) is a group homomorphism.

Recall that we have the following result ([MT2, Lemma 3.1]), which is a direct consequence of [Dwy, Theorem 2.4].

Lemma 4.13. *Let G be a profinite group, and p a prime number. Then the following statements are equivalent:*

(1) *G has the vanishing triple Massey product property with respect to $\mathbb{F}_p$.*

(2) *For every homomorphism $\bar{\rho}\colon G \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$, the finite weak embedding problem*

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & \swarrow & \downarrow{\scriptstyle (\bar{\rho}_{12},\bar{\rho}_{23},\bar{\rho}_{34})} & & \\ 0 & \longrightarrow & M & \longrightarrow & \mathbb{U}_4(\mathbb{F}_p) & \longrightarrow & (\mathbb{F}_p)^3 & \longrightarrow & 1, \end{array}$$

has a weak solution, i.e., $(\bar{\rho}_{12}, \bar{\rho}_{23}, \bar{\rho}_{34})$ can be lifted to a homomorphism $\rho\colon G \to \mathbb{U}_4(\mathbb{F}_p)$.

Proposition 4.14. *Let G be a profinite group, and p a prime number. Let H be a open subgroup of G whose index is coprime to p. Assume that H has the vanishing triple Massey product property with respect to $\mathbb{F}_p$, then G also has the vanishing triple Massey product property with respect to $\mathbb{F}_p$.*

Proof. We shall prove the condition (2) in Lemma 4.13 for the group G.

Let $\bar{\rho}\colon G \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$ be any homomorphism. We consider the weak embedding problem

$$(\mathcal{E}) \qquad \begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & & \downarrow{\scriptstyle (\bar{\rho}_{12},\bar{\rho}_{23},\bar{\rho}_{34})=:\phi} & & \\ 0 & \longrightarrow & M & \longrightarrow & \mathbb{U}_4(\mathbb{F}_p) & \longrightarrow & (\mathbb{F}_p)^3 & \longrightarrow & 1. \end{array}$$

Then by the assumption and by Lemma 4.13, the weak embedding problem $(\mathcal{E} \mid_H)$

$$(\mathcal{E} \mid_H) \qquad \begin{array}{ccccccccc} & & & & & & H & & \\ & & & & & \swarrow & \downarrow{\scriptstyle \phi|_H} & & \\ 0 & \longrightarrow & M & \longrightarrow & \mathbb{U}_4(\mathbb{F}_p) & \longrightarrow & (\mathbb{F}_p)^3 & \longrightarrow & 1, \end{array}$$

which is induced from $(\mathcal{E})$, has a weak solution. Let ϵ be the cohomology class in $H^2((\mathbb{F}_p)^3, M)$ which corresponds to the extension

$$1 \longrightarrow M \longrightarrow \mathbb{U}_4(\mathbb{F}_p) \xrightarrow{(a_{12},a_{23},a_{34})} (\mathbb{F}_p)^3 \longrightarrow 1.$$

We have the following commutative diagram

$$\begin{array}{ccc} H^2((\mathbb{F}_p)^3, M) & \xrightarrow{\phi^*} & H^2(G, M) \\ \| & & \downarrow{\scriptstyle \mathrm{res}} \\ H^2((\mathbb{F}_p)^3, M) & \xrightarrow{(\phi|_H)^*} & H^2(H, M). \end{array}$$

In particular, $(\phi \mid_H)^*(\epsilon) = \mathrm{res}(\phi^*(\epsilon))$. Since the weak embedding problem $(\mathcal{E} \mid_H)$ has a weak solution, we see that $(\phi \mid_H)^*(\epsilon) = 0$ by Hoechsmann's lemma ([NSW, Chapter 3, §5, Proposition 3.5.9]). (Note that the statement of Hoechsmann's lemma in [NSW] deals with embedding problems, but its proof goes well with weak embedding problems.) Since $[G : H]$ is coprime to p and the order of M is a p-power, we see that the restriction map res: $H^2(G,M) \longrightarrow H^2(H,M)$ is injective by [Se2, Chapter I, §2, Corollary to Proposition 9]. Hence $\phi^*(\epsilon)=0$. Hoechsmann's lemma implies that the weak embedding problem $(\mathcal{E})$ has a weak solution, and we are done. □

Theorem 4.15. *Let F be any field and p a prime number. Then the absolute Galois group G_F of F has the vanishing triple Massey product property with respect to $\mathbb{F}_p$*

Proof. If $\mathrm{char}F=p$, then the maximal pro-p-quotient $G_F(p)$ of G_F is a free pro-p-group. Therefore $G_F(p)$ and G_F has the vanishing triple Massey product property with respect to $\mathbb{F}_p$.

Now we assume that $\mathrm{char}F\neq p$. Let ξ be a primitive p-th root of unity, and let $K=F(\xi)$. Then K/F is a finite extension of degree d, and d divides $p-1$. This implies that $[G_F:G_K]=d$ is coprime to p. Since G_K has the vanishing triple Massey product property by Theorem 4.10, it follows that G_F also has the vanishing triple Massey product property by Proposition 4.14. □

4.3. **Some consequences.** In this subsection we assume that p is an odd prime number. The case when $p=2$ is treated in [MT1, Theorem 1.3 and Theorem 1.4].

Recall that for a profinite group G and a prime number p, the Zassenhaus (p-)filtration $(G_{(n)})$ of G is defined inductively by

$$G_{(1)}=G,\quad G_{(n)}=G^p_{(\lceil n/p\rceil)}\prod_{i+j=n}[G_{(i)},G_{(j)}],$$

where $\lceil n/p\rceil$ is the least integer which is greater than or equal to n/p. (Here for two closed subgroups H and K of G, $[H,K]$ means the smallest closed subgroup of G containing the commutators $[x,y]=x^{-1}y^{-1}xy$, $x\in H, y\in K$. Similarly, H^p means the smallest closed subgroup of G containing the p-th powers x^p, $x\in H$.)

Let $(I,<)$ be a well-ordered set. Let S be a free pro-p-group on a set of generators $x_i, i\in I$ (see [NSW, Definition 3.5.14]). Let $S_{(i)}, i=1,2,\ldots$ be the p-Zassenhaus filtration of S. Then any element r in $S_{(2)}$ may be written uniquely as

$$r=\begin{cases}\prod_{i<j}[x_i,x_j]^{b_{ij}}\prod_{i\in I}x_i^{3a_i}\prod_{i<j,k\leq j}[[x_i,x_j],x_k]^{c_{ijk}}\cdot r', \text{ if } p=3,\\ \prod_{i<j}[x_i,x_j]^{b_{ij}}\prod_{i<j,k\leq j}[[x_i,x_j],x_k]^{c_{ijk}}\cdot r', \text{ if } p\neq 3,\end{cases}\tag{1}$$

where $a_i, b_{ij}, c_{ijk}\in\{0,1,\ldots,p-1\}$ and $r'\in S_{(4)}$. For convenience we call (1) the canonical decomposition modulo $S_{(4)}$ of r (with respect to the basis (x_i)) and we also set $u_{ij}=b_{ij}$ if $i<j$, and $u_{ij}=b_{ji}$ if $j<i$.

We denote by $G_F(p)$ the maximal pro-p-quotient of an absolute Galois group G_F of a given field F.

Theorem 4.16. *Let $\mathcal{R}$ be a set of elements in $S_{(2)}$. Assume that there exists an element r in $\mathcal{R}$ and distinct indices i,j,k with $i<j, k<j$ such that:*

(i) *In (1) the canonical decomposition modulo $S_{(4)}$ of r, $u_{ij} = u_{kj} = u_{ki} = u_{kl} = u_{jl} = 0$ for all $l \neq i, j, k$, and $c_{ijk} \neq 0$; and*

(ii) *for every $s \in \mathcal{R}$ which is different from r, the factors $[x_k, x_i]$, $[x_i, x_k]$ and $[x_i, x_j]$ do not occur in the canonical decomposition modulo $S_{(4)}$ of s.*

Then $G = S/\langle \mathcal{R} \rangle$ is not realizable as $G_F(p)$ for any field F.

Proof. This follows immediately from Theorem 4.15, [MT1, Theorem 7.8] and [MT1, Corollary 3.5]. □

Theorem 4.17. *Let $\mathcal{R}$ be a set of elements in $S_{(2)}$. Assume that there exists an element r in $\mathcal{R}$ and distinct indices $i < j$ such that:*

(i) *In (1) the canonical decomposition modulo $S_{(4)}$ of r, $u_{ij} = u_{il} = u_{jl} = 0$, for all $l \neq i, j$ and $c_{iji} \neq 0$ (respectively, $c_{ijj} \neq 0$); and*

(ii) *for every $s \in \mathcal{R}$ which is different from r, the factors $[x_i, x_j]$ does not occur in the canonical decomposition modulo $S_{(4)}$ of s.*

Then $G = S/\langle \mathcal{R} \rangle$ is not realizable as $G_F(p)$ for any field F.

Proof. This follows immediately from Theorem 4.15, [MT1, Theorem 7.12] and [MT1, Corollary 3.5]. □

5. Vanishing of some higher Massey products

5.1. **Massey products.** Let G be a profinite group and p a prime number. We consider the finite field $\mathbb{F}_p$ as a trivial discrete G-module. Let $\mathcal{C}^\bullet = (C^\bullet(G, \mathbb{F}_p), \partial, \cup)$ be the differential graded algebra of inhomogeneous continuous cochains of G with coefficients in $\mathbb{F}_p$ [NSW, Ch. I, §2]. We write $H^i(G, \mathbb{F}_p)$ for the corresponding cohomology groups. We denote by $Z^1(G, \mathbb{F}_p)$ the subgroup of $C^1(G, \mathbb{F}_p)$ consisting of all 1-cocycles. Because we use trivial action on the coefficients $\mathbb{F}_p$, $Z^1(G, \mathbb{F}_p) = H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p)$. (See [MT1, MT2] and references therein for more general setups.)

Let $n \geq 3$ be an integer. Let $a_1, \ldots, a_n$ be elements in $H^1(G, \mathbb{F}_p) = Z^1(G, \mathbb{F}_p) \subseteq C^1(G, \mathbb{F}_p)$.

Definition 5.1. A collection $\mathcal{M} = \{a_{ij} \mid 1 \leq i < j \leq n+1, (i,j) \neq (1, n+1)\}$ of elements a_{ij} of $\mathcal{C}^1(G, \mathbb{F}_p)$ is called a *defining system* for the *n-fold Massey product* $\langle a_1, \ldots, a_n \rangle$ if the following conditions are fulfilled:

(1) $a_{i,i+1} = a_i$ for all $i = 1, 2 \ldots, n$.

(2) $\partial a_{ij} = \sum_{l=i+1}^{j-1} a_{il} \cup a_{lj}$ for all $i + 1 < j$.

Then $\sum_{k=2}^{n} a_{1k} \cup a_{k,n+1}$ is a 2-cocycle. Its cohomology class in H^2 is called the *value* of the product relative to the defining system $\mathcal{M}$, and is denoted by $\langle a_1, \ldots, a_n \rangle_{\mathcal{M}}$. The product $\langle a_1, \ldots, a_n \rangle$ itself is the subset of $H^2(G, \mathbb{F}_p)$ consisting of all elements which can be written in the form $\langle a_1, \ldots, a_n \rangle_{\mathcal{M}}$ for some defining system $\mathcal{M}$.

When $n = 3$ we will speak about a *triple* Massey product. Note that in this case the triple Massey product $\langle a_1, a_2, a_3\rangle$ is defined if and only if $a_1 \cup a_2 = a_2 \cup a_3 = 0$ in $H^2(G, \mathbb{F}_p)$.

Definition 5.2. We say that G has the *vanishing triple Massey product property (with respect to $\mathbb{F}_p$)* if every defined triple Massey product $\langle a_1, a_2, a_3\rangle$, where $a_1, a_2, a_3 \in H^1(G, \mathbb{F}_p)$, necessarily contains 0.

For some convenience, we introduce the following definition.

Definition 5.3. Let $n \geq 1$ be an integer. Let $a_1, \ldots, a_n$ be elements in $H^1(G, \mathbb{F}_p)$. A collection $\mathcal{M} = \{a_{ij} \mid 1 \leq i < j \leq n+1\}$ of elements a_{ij} of $\mathcal{C}^1(G, \mathbb{F}_p)$ is called a *complete defining system* for the n-tuple $(a_1, \ldots, a_n)$ if the following conditions are fulfilled:

(1) $a_{i,i+1} = a_i$ for all $i = 1, 2 \ldots, n$.
(2) $\partial a_{ij} = \sum_{l=i+1}^{j-1} a_{il} \cup a_{lj}$ for all $i + 1 < j$.

Note that for $n = 1$, $\mathcal{M} = \{a_{12} := a_1\}$ is a complete defining system for (a_1). For $n = 2$, (a_1, a_2) has a complete defining system if and only if $a_1 \cup a_2 = 0$. For $n \geq 3$, $(a_1, \ldots, a_n)$ has a complete defining system if and only if the n-fold Massey product $\langle a_1, \ldots, a_n\rangle$ is defined and contains 0.

5.2. **Vanishing of some higher Massey products.** Assume R be a unital commutative ring. Let n be a positive integer. Assume that every integer $1 \leq k \leq n$ is invertible in R. We have the following binomial polynomials in the ring $A[X]$ of polynomials in one variable X and with coefficients in A:

$$\binom{X}{0} = 1 \text{ and } \binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}, 1 \leq k \leq n.$$

We have the following elemenatary lemma.

Lemma 5.4. *Let the notation be as above. For $1 \leq k \leq n$, one has*

$$\binom{X+Y}{k} = \sum_{l=0}^{k} \binom{X}{l}\binom{Y}{k-l} \in A[X,Y].$$

Here $A[X,Y]$ is the ring of polynomials with coefficients A in two variables X and Y. □

Remark 5.5. Let the notation be as above. Then for $1 \leq k \leq n$, one also has

$$\frac{(X+Y)^k}{k!} = \sum_{l=0}^{k} \frac{X^l}{l!}\frac{Y^{k-l}}{(k-l)!} \in A[X,Y].$$

And all results presented below can be stated and proved by using $\frac{X^k}{k!}$ (with some obvious modifications) instead of using $\binom{X}{k}$. □

For any element χ in $H^1(G,\mathbb{F}_p) = Z^1(G,\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p)$ and for each $k = 0,\ldots,p-1$, we define $\binom{\chi}{k} \in C^1(G,\mathbb{F}_p)$ by

$$\binom{\chi}{k}(\sigma) = \binom{\chi(\sigma)}{k},\ \forall \sigma \in G.$$

Corollary 5.6. *Let χ be an element in $\mathrm{Hom}(G,\mathbb{F}_p)$. Let k be an integer with $1 \le k < p$. Then*

$$d\binom{\chi}{k} = -\sum_{l=1}^{k-1}\binom{\chi}{l}\cup\binom{\chi}{k-l} \in C^2(G,\mathbb{F}_p).$$

Proof. By Lemma 5.4, we have

$$\begin{aligned} d\binom{\chi}{k}(\sigma,\tau) &= \binom{\chi}{k}(\sigma) + \binom{\chi}{k}(\tau) - \binom{\chi}{k}(\sigma\tau) \\ &= \binom{\chi(\sigma)}{k} + \binom{\chi(\tau)}{k} - \binom{\chi(\sigma\tau)}{k} \\ &= \binom{\chi(\sigma)}{k} + \binom{\chi(\tau)}{k} - \binom{\chi(\sigma)+\chi(\tau)}{k} \\ &= \binom{\chi(\sigma)}{k} + \binom{\chi(\tau)}{k} - \sum_{l=0}^{k}\binom{\chi(\sigma)}{l}\binom{\chi(\tau)}{k-l} \\ &= -\sum_{l=1}^{k-1}\binom{\chi}{l}\cup\binom{\chi}{k-l}(\sigma,\tau),\ \forall \sigma,\tau \in G, \end{aligned}$$

as desired. □

Corollary 5.7. *Let χ be an element in $H^1(G,\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p)$. Let $k < p$ be a positive integer. Then the system*

$$\mathcal{M} = \left\{-\binom{\chi}{j-i} \mid 1 \le i < j \le k+1\right\}$$

is a complete defining system for the n-tuple $(-\chi,-\chi,\ldots,-\chi)$ (k copies of $-\chi$).

Proof. This follows immediately from Corollary 5.6. □

Proposition 5.8. *Let F be a field containing a primitive p-th root of unity. Let a and b be elements which are linearly independent modulo $(F^\times)^p$. Let $k < p$ be a positive integer. Assume that $\chi_a \cup \chi_b = 0$. Then the $(k+1)$-fold Massey product $\langle -\chi_b, -\chi_a, \ldots, -\chi_a\rangle$ (k copies of $-\chi_a$) is defined and has a complete defining system of the form $\mathcal{M} = \{a_{ij} \in C^1(G,\mathbb{F}_p) \mid 1 \le i < j \le k+2\}$, where*

$$a_{ij} = -\binom{\chi_a}{j-i},\ \text{for all } 2 \le i < j \le k+2.$$

Proof. By Corollary 5.7, the system $\{a_{ij} := -\binom{\chi_a}{j-i} \mid 2 \leq i < j \leq k+2\}$ is a complete defining system for the k-tuple $(-\chi_a, \ldots, -\chi_a)$. We set $a_{1,2} = -\chi_b$. We shall prove by induction on $j = 3, 4, \ldots, k+2$ that there exist $a_{13}, a_{14}, \ldots, a_{1j} \in C^1(G_F, \mathbb{F}_p)$ such that

$$da_{1r} = \sum_{l=2}^{r-1} a_{2l} \cup a_{lr}, \forall r = 3, 4, \ldots, j.$$

Then this will imply immediately that the system $\{a_{ij} \mid 1 \leq i < j \leq k+2\}$ is a complete defining sytem for the $(k+1)$-tuple $(-\chi_b, -\chi_a, \ldots, -\chi_a)$.

If $j = 3$, then since $\chi_a \cup \chi_b = 0$, there exists $\varphi_{ba} \in C^1(G_F, \mathbb{F}_p)$ such that $d\varphi_{ba} = \chi_b \cup \chi_a$. We set $a_{1,3} := \varphi_{ba}$. Then

$$da_{1,3} = \chi_b \cup \chi_a = a_{1,2} \cup a_{2,3}.$$

Now assume that $j > 3$. By induction hypothesis there exist $b_{13}, b_{14}, \ldots, b_{1j} \in C^1(G_F, \mathbb{F}_p)$ such that

$$db_{1r} = \sum_{l=2}^{r-1} a_{1l} \cup a_{lr}, \forall r = 3, 4, \ldots, j.$$

Then the system

$$\mathcal{N} := \{a_{12}, b_{13}, \ldots, b_{1j}, \text{ and } a_{\mu\nu} \text{ with } 2 \leq \mu < \nu \leq j+1\}$$

is a defining system for the j-fold Massey product $\langle -\chi_b, -\chi_a, \ldots, -\chi_a \rangle$. Then the value of this Massey product with respect to $\mathcal{N}$ is

$$\begin{aligned}\langle \chi_b, \chi_a, \ldots, \chi_a \rangle_{\mathcal{N}} &= a_{12} \cup a_{2,j+1} + b_{13} \cup a_{3,j+1} + \cdots + b_{1j} \cup a_{j,j+1} \\ &= -\chi_b \cup -\binom{\chi_a}{j-1} + b_{13} \cup -\binom{\chi_a}{j-2} + \cdots + b_{1j} \cup -\binom{\chi_a}{1}.\end{aligned}$$

For the ease of notation, we denote $\mathrm{res}_{\ker \chi_a}$ just by res_a. Then we have

$$\begin{aligned}&\mathrm{res}_a(\langle -\chi_b, -\chi_a, \ldots, -\chi_a \rangle_{\mathcal{N}}) \\ &= \mathrm{res}_a(-\chi_b) \cup \mathrm{res}_a(-\binom{\chi_a}{j-1}) + \mathrm{res}_a(b_{13}) \cup \mathrm{res}_a(-\binom{\chi_a}{j-2}) + \cdots + \mathrm{res}_a(b_{1j}) \cup \mathrm{res}_a(-\binom{\chi_a}{1}) \\ &= \mathrm{res}_a(-\chi_b) \cup 0 + \mathrm{res}_a(b_{13}) \cup 0 + \cdots + \mathrm{res}_a(b_{1j}) \cup 0 = 0.\end{aligned}$$

Then by Proposition 3.1, there exists $x \in F^\times$ such that

$$-\chi_b \cup -\binom{\chi_a}{j-1} + b_{13} \cup -\binom{\chi_a}{j-2} + \cdots + b_{1j} \cup -\binom{\chi_a}{1} = -\chi_x \cup -\binom{\chi_a}{1} \in H^2(G, \mathbb{F}_p).$$

Hence there exists $a_{1,j+1}$ in $C^1(G, \mathbb{F}_p)$ such that

$$\chi_b \cup -\binom{\chi_a}{j-1} + b_{13} \cup -\binom{\chi_a}{j-2} + \cdots + b_{1,j-1} \cup -\binom{\chi_a}{2} + (b_{1j} + \chi_x) \cup -\binom{\chi_a}{1} = da_{1,j+1}.$$

We set $a_{1r} := b_{1r}$ for $r = 3, 4, \ldots, j-1$, and $a_{1j} := b_{1j} + \chi_x$. Then we have

$$da_{1r} = db_{1r} = \sum_{l=2}^{r-1} a_{1l} \cup a_{lr}, \forall r = 3, 4, \ldots, j,$$

and

$$da_{1,j+1} = \sum_{l=2}^{j} a_{1l} \cup a_{l,j+1},$$

as desired. □

Proposition 5.9. *Let F be a field containing a primitive p-th root of unity. Let a and b be elements which are linearly independent modulo $(F^\times)^p$. Let $k < p$ be a positive integer. Assume that $\chi_a \cup \chi_b = 0$. Then the $(k+2)$-fold Massey product $\langle -\chi_a, -\chi_b, -\chi_a, \ldots, -\chi_a \rangle$ ($k+1$ copies of $-\chi_a$) is defined and has a complete defining system of the form $\mathcal{M} = \{a_{ij} \in C^1(G, \mathbb{F}_p) \mid 1 \le i < j \le k+3\}$, where*

$$a_{ij} = -\binom{\chi_a}{j-i}, \text{ for all } 3 \le i < j \le k+3.$$

Proof. By Proposition 5.8, there exists a system $\{a_{ij} \in C^1(G, \mathbb{F}_p) \mid 2 \le i < j \le k+3\}$ such that it is a complete defining system for the $k+1$-tuple $(-\chi_b, -\chi_a, \ldots, -\chi_a)$ and that

$$a_{ij} = -\binom{\chi_a}{j-i}, \text{ for all } 3 \le i < j \le k+3.$$

We set $a_{1,2} = -\chi_a$. We shall prove by induction on $j = 3, 4, \ldots, k+3$ that there exist $a_{13}, a_{14}, \ldots, a_{1j} \in C^1(G_F, \mathbb{F}_p)$ such that

$$da_{1r} = \sum_{l=2}^{r-1} a_{2l} \cup a_{lr}, \forall r = 3, 4, \ldots, j.$$

Then this will imply immediately that the system $\{a_{ij} \mid 1 \le i < j \le k+3\}$ is a complete defining system for the $(k+2)$-tuple $(-\chi_a, -\chi_b, -\chi_a, \ldots, -\chi_a)$.

If $j = 3$, then since $\chi_a \cup \chi_b = 0$, there exists $\varphi_{ab} \in C^1(G_F, \mathbb{F}_p)$ such that $d\varphi_{ab} = \chi_a \cup \chi_b$. We set $a_{1,3} := \varphi_{ab}$. Then

$$da_{1,3} = \chi_a \cup \chi_b = a_{1,2} \cup a_{2,3}.$$

Now assume that $j > 3$. By induction hypothesis there exist $b_{13}, b_{14}, \ldots, b_{1j} \in C^1(G_F, \mathbb{F}_p)$ such that

$$db_{1r} = \sum_{l=2}^{r-1} a_{1l} \cup a_{lr}, \forall r = 3, 4, \ldots, j.$$

Then the system

$$\mathcal{N} := \{a_{12}, b_{13}, \ldots, b_{1j}, \text{ and } a_{\mu\nu} \text{ with } 2 \le \mu < \nu \le j+1\}$$

is a defining system for the j-fold Massey product $\langle -\chi_b, -\chi_a, \ldots, -\chi_a\rangle$. Then the value of this Massey product with respect to $\mathcal{N}$ is

$$\begin{aligned}&\langle -\chi_a, -\chi_b, -\chi_a, \ldots, -\chi_a\rangle_{\mathcal{N}}\\ &= a_{12}\cup a_{2,j+1} + b_{13}\cup a_{3,j+1} + \cdots + b_{1j}\cup a_{j,j+1}\\ &= -\chi_a\cup a_{2,j+1} + b_{13}\cup -\binom{\chi_a}{j-1} + b_{13}\cup -\binom{\chi_a}{j-2} + \cdots + b_{1j}\cup -\binom{\chi_a}{1}.\end{aligned}$$

For the ease of notation, we denote $\mathrm{res}_{\ker\chi_a}$ just by res_a. Then we have

$$\begin{aligned}&\mathrm{res}_a(\langle -\chi_a, -\chi_b, -\chi_a, \ldots, -\chi_a\rangle_{\mathcal{N}})\\ &= \mathrm{res}_a(-\chi_a)\cup \mathrm{res}_a(a_{2,j+1}) + \mathrm{res}_a(b_{13})\cup \mathrm{res}_a(-\binom{\chi_a}{j-2}) + \cdots + \mathrm{res}_a(b_{1j})\cup \mathrm{res}_a(-\binom{\chi_a}{1})\\ &= 0\cup \mathrm{res}_a(a_{2,j+1}) + \mathrm{res}_a(b_{13})\cup 0 + \cdots + \mathrm{res}_a(b_{1j})\cup 0 = 0.\end{aligned}$$

By Proposition 3.1, there exists $x\in F^\times$ such that

$$-\chi_a\cup a_{2,j+1} + b_{13}\cup -\binom{\chi_a}{j-2} + \cdots + b_{1j}\cup -\binom{\chi_a}{1} = -\chi_x\cup -\binom{\chi_a}{1} \in H^2(G,\mathbb{F}_p).$$

Hence there exists $a_{1,j+1}$ in $C^1(G,\mathbb{F}_p)$ such that

$$-\chi_a\cup a_{2,j+1} + b_{13}\cup -\binom{\chi_a}{j-2} + \cdots + b_{1,j-1}\cup -\binom{\chi_a}{2} + (b_{1j}+\chi_x)\cup -\binom{\chi_a}{1} = da_{1,j+1}.$$

We set $a_{1r} := b_{1r}$ for $r = 3, 4, \ldots, j-1$, and $a_{1j} := b_{1j} + \chi_x$. Then we have

$$da_{1r} = db_{1r} = \sum_{l=2}^{r-1} a_{1l}\cup a_{lr}, \forall r = 3, 4, \ldots, j,$$

and

$$da_{1,j+1} = \sum_{l=2}^{j} a_{1l}\cup a_{l,j+1},$$

as desired. □

Theorem 5.10. *Let F be a field containing a primitive p-th root of unity. Let a and b be elements which are linearly independent modulo $(F^\times)^p$. Let $k < p$ be a positive integer. Assume that $\chi_a\cup\chi_b = 0$. Then we have*

1. *The $(k+1)$-fold Massey products $\langle \chi_b, \chi_a, \ldots, \chi_a\rangle$ and $\langle \chi_a, \ldots, \chi_a, \chi_b\rangle$ (k copies of χ_a) are defined and contain 0.*
2. *The $(k+2)$-fold Massey products $\langle \chi_a, \chi_b, \chi_a, \ldots, \chi_a\rangle$ and $\langle \chi_a, \ldots, \chi_a, \chi_b, \chi_a\rangle$ ($k+1$ copies of χ_a) are defined and contain 0.*

Proof. We recall the following formal property of Massey products. If $\langle a_1, a_2, \ldots, a_n\rangle$ is defined, then $\langle a_n, a_{n-1}, \ldots, a_1\rangle$ is defined and

$$\langle a_1, a_2, \ldots, a_n\rangle = \pm\langle a_n, a_{n-1}, \ldots, a_1\rangle.$$

(See [Kra, Theorem 8].) Observe also that $-\chi_a = \chi_{a^{-1}}$ for every $a \in F^\times$. The statement then follows from the two previous propositions. □

References

[AS1] E. Artin and O. Schreier, *Algebraische Konstruktion reeller Körper*, Abh. Math. Sem. Univ. Hamburg 5 (1927) pp. 85-99. Reprinted in: Artin's Collected Papers (Eds. S. Lang and J. Tate), Springer-Verlag, New York, 1965, pp. 258-272.

[AS2] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Abh. Math. Sem. Univ. Hamburg 5 (1927) pp. 225-231. Reprinted in: Artin's Collected Papers (Eds. S. Lang and J. Tate), Springer-Verlag, New York, 1965, pp. 289-295.

[CKM] J.-P. Colliot-Thélène, D. Kanevsky, J.P. Sansuc, *Arithmétique des surfaces cubiques diagonales,* Diophantine approximation and transcendence theory (Bonn, 1985), 1-108, Lecture Notes in Math., 1290, Springer, Berlin, 1987.

[Dwy] W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra 6 (1975), no. 2, 177-190.

[Ef] I. Efrat, *The Zassenhaus filtration, Massey products, and representations of profinite groups*, Adv. Math. 263 (2014), 389-411.

[EMa1] I. Efrat and E. Matzri, *Vanishing of Massey products and Brauer groups*, to appear in Can. Math. Bull., arXiv:1410.0502.

[EMa2] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, preprint (2014), arXiv:1412.7265.

[EM1] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. 133 (2011), no. 6, 1503-1532.

[EM2] I. Efrat and J. Mináč, *Galois groups and cohomological functors* preprint (2011), available at arXiv:1103.1508v1.

[Fe] R. Fenn, *Techniques of Geometric Topology*, London Math. Soc. Lect. Notes 57 Cambridge 1983.

[DGMS] P. Deligne, P. Griffiths, J. Morgan and D. Sullivan, *Real homotopy theory of Kähler manifolds,* Invent. Math. 29 (1975), 245-274.

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

[Kra] D. Kraines, *Massey higher products*, Trans. Amer. Math. Soc. 124 (1996), 431-449.

[Ma] E. Matzri, *Triple Massey products in Galois cohomology*, preprint (2014), arXiv:1411.4146.

[Me] A. Merkurjev, *Essential p-dimension of* $\mathrm{PGL}(p^2)$, J. Amer. Math. Soc. 23 (2010), no. 3, 693-712.

[MSp] J. Mináč and M. Spira, *Witt rings and Galois groups*, Ann. of Math. (2) 144 (1996), no. 1, 35-60.

[MT1] J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, to appear in J. Eur. Math. Soc., arXiv:1307.6624.

[MT2] J. Mináč and N. D. Tân, *The Kernel Unipotent Conjecture and Massey products on an odd rigid field* (with an appendix by I. Efrat, J. Mináč and N. D. Tân), Adv. Math. 273 (2015), 242-270.

[MT3] J. Mináč and N. D. Tân, *Triple Massey products over global fields*, preprint (2014), arXiv:1403.4586.

[MT4] J. Mináč and N. D. Tân, *Construction of unipotent Galois extensions and Massey products*, preprint (2015) arXiv:1501.01346.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323, Springer-Verlag, Berlin, 2000.

[Se1] J.-P. Serre, *Local fields*, translated from the French by M. J. Greenberg, Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.

[Se2] J.-P. Serre, *Galois cohomology*, translated from the French by P. Ion and revised by the author, corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[Sha1] R. Sharifi, *Twisted Heisenberg representations and local conductors*, Ph.D. thesis, The University of Chicago (1999).

[Sha2] R. Sharifi, *Massey products and ideal class groups*, J. Reine Angew. Math. 603 (2007), 1-33.

[Ti] J.-P. Tignol, *Produits croisés abéliens*, J. Algebra 70 (1981), no. 2, 420-436.

[Vi] F. R. Villegas, *Relations between quadratic forms and certain Galois extensions*, a manuscript, Ohio State University, 1988, http://www.math.utexas.edu/users/villegas/osu.pdf.

[Wa] A. R. Wadsworth, *Merkurjev's elementary proof of Merkurjev's theorem*, Applications of algebraic K-theory to algebraic geometry and number theory, Parts I, II (Boulder, Colo., 1983), 741-776, Contemp. Math., 55, Amer. Math. Soc., Providence, RI, 1986.

[We] E. Weiss, *Cohomology of groups*, Pure and Applied Mathematics, Vol. 34 Academic Press, New York-London, 1969.

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
E-mail address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7 AND INSTITUTE OF MATHEMATICS, VIETNAM ACADEMY OF SCIENCE AND TECHNOLOGY, 18 HOANG QUOC VIET, 10307, HANOI - VIETNAM
E-mail address: dnguy25@uwo.ca