TRIPLE MASSEY PRODUCTS OVER GLOBAL FIELDS

JÁN MINÁČ AND NGUYỄN DUY TÂN

ABSTRACT. Let K be a global field which contains a primitive p-th root of unity, where p is a prime number. M. J. Hopkins and K. G. Wickelgren showed that for $p = 2$, any triple Massey product over K with respect to $\mathbb{F}_p$, contains 0 whenever it is defined. We show that this is true for all primes p.

1. INTRODUCTION

Massey products were introduced by W. S. Massey in [Ma]. (We review the definition and some basic properties in Section 2.) Massey products were first used in topology where usual cohomology cup products would not detect some linking properties of knots but Massey products would. (See for example [Mo, page 98] or [GM, pages 154-158].) Further interest in Massey products arises as an obstruction to the "formality" of manifolds over real numbers. In the case of compact Kähler manifolds, formality formalizes the property that their homotopy type is a formal consequence of their real cohomology ring. (See [DGMS].) We treat Massey products also as obstructions to solving certain Galois embedding problems.

Let p be a prime number. Let K be a field which we assume contains a fixed primitive p-th root of unity ζ_p. Let G_K be the absolute Galois group of K. Let $\mathcal{C}^\bullet = \mathcal{C}^\bullet(G_K, \mathbb{F}_p)$ denote the differential graded algebra of $\mathbb{F}_p$-inhomogeneous cochains in continuous group cohomology of G_K (see e.g., [NSW, Chapter I, §2]). For any $a \in K^\times = K \setminus \{0\}$, let χ_a denote the corresponding character via the Kummer map $K^\times \to H^1(G_K, \mathbb{F}_p)$, i.e., χ_a is defined by $\sigma(\sqrt[p]{a}) = \zeta_p^{\chi_a(\sigma)} \sqrt[p]{a}$, for all $\sigma \in G_K$. In the work of M. J. Hopkins and K. G. Wickelgren [HW], the following fundamental result was proved. (By a global field we mean a finite extension of $\mathbb{Q}$, or a function field in one variable over a finite field.)

Theorem 1.1 ([HW, Theorem 1.2]). *Let the notation be as above. Assume that $p = 2$ and K is a global field of characteristic $\neq 2$. Let $a, b, c \in K^\times$. The triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ contains 0 whenever it is defined.*

In [MT] we extend the result of Hopkins-Wickelgren to an arbitrary field K of characteristic $\neq 2$, still assuming that $p = 2$.

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

Theorem 1.2 ([MT, Theorem 1.2]). *Let the notation be as above. Assume that $p = 2$ and K is an arbitrary field of characteristic $\neq 2$. Let $a, b, c \in K^\times$. The triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ contains 0 whenever it is defined.*

In this paper we extend the result of Hopkins-Wickelgren in Theorem 1.1 in another direction. We still consider a global field K but we let prime p be arbitrary.

Theorem 1.3 (Theorem 4.3). *Let p be an arbitrary prime. Let K be a global field containing a primitive p-th root of unity and $a, b, c \in K^\times$. Then the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ contains 0 whenever it is defined.*

Let us denote by $\mathbb{U}_4(\mathbb{F}_p)$ the group of all upper-triangular unipotent 4-by-4-matrices with entries in $\mathbb{F}_p$. For a finite group G, by a G-Galois extension L/K, we mean a Galois extension with Galois group isomorphic to G. It is a classical problem to describe extensions M/K which can be embedded into a G-Galois extension L/K with a prescribed Galois group G. From Theorem 1.3 and its local version we can deduce the following contribution to this problem when $G = \mathbb{U}_4(\mathbb{F}_p)$.

Corollary 1.4. *Let p be an arbitrary prime. Let K be a local or global field containing a primitive p-th root of unity. Let $a, b, c \in K^\times$ and assume that the classes $[a], [b], [c]$ in the $\mathbb{F}_p$-vector space $K^\times/(K^\times)^p$ are linearly independent. Assume further that $\chi_a \cup \chi_b = \chi_b \cup \chi_c = 0$ in $H^2(G_K, \mathbb{F}_p)$. Then the Galois extension $K(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/K$ can be embedded in a $\mathbb{U}_4(\mathbb{F}_p)$-Galois extension L/K.*

In fact for each $\mathbb{U}_4(\mathbb{F}_p)$-extension L/K, there exist $a, b, c \in K^\times \cap L^p$ such that that the classes $[a], [b], [c]$ in the $\mathbb{F}_p$-vector space $K^\times/(K^\times)^p$ are linearly independent, and that $\chi_a \cup \chi_b = \chi_b \cup \chi_c = 0$ in $H^2(G_K, \mathbb{F}_p)$. Thus we see that this hypothesis is both necessary and sufficient for embedding abelian extensions of degree p^3 and exponent p into a $\mathbb{U}_4(\mathbb{F}_p)$-extension. (See Section 3 for more detail.)

In the case when $p = 2$, Corollary 1.4 was also proved in [GLMS, Section 4] for all fields K of characteristic not 2. (See also [MT, Section 6].)

Let us now recall briefly how Theorem 1.1 is established in [HW].

Let $p = 2$ and K be a field of characteristic not 2. In [HW], the authors construct for each $a, b, c \in K^\times$, a K-variety $X_{a,b,c}$, which detects when a triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ is defined and contains 0. More precisely, the variety $X_{a,b,c}$ has a K-rational point if and only if the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ is defined and contains 0 (see [HW, Theorem 1.1]). The authors then establish a local version of Theorem 1.1 by using the non-degenerate property of the cup products and the indeterminacy of Massey products. Now assume that K is a global field and consider $a, b, c \in K^\times$ such that $\langle \chi_a, \chi_b, \chi_c \rangle$ is defined. By applying a result of D. B. Leep and A. R. Wadsworth in [LW], the authors show that the splitting variety $X_{a.b,c}$ satisfies the Hasse local-global principle (see [HW, Theorem 3.4]), and then the result follows from the local case.

In our paper we also use the local-global principle but our method is different from the method used in the paper [HW]. Let p be any prime, and let K be a field containing a primitive p-th root of unity. Let $a, b, c \in K^\times$ such that the triple Massey product

$\langle \chi_a, \chi_b, \chi_c \rangle$ is defined. Now instead of constructing a splitting variety for $\langle \chi_a, \chi_b, \chi_c \rangle$, we use the technique of Galois embedding problems to detect the vanishing property of triple Massey products. Namely, $\langle \chi_a, \chi_b, \chi_c \rangle$ vanishes if certain kinds of embedding problems are solvable. This is true because of a result of W. G. Dwyer. We then use Hoechsmann's lemma to translate the problem of showing the solvability of embedding problems to the problem of showing some degree 2 cohomological classes vanish. Then we establish a local-global principle for the vanishing of the cohomogical classes (see Lemma 4.1). Theorem 1.3 then follows from its local version. This being said, our proof also provides another proof for Theorem 1.1 in the case $p = 2$.

The structure of our paper is as follows. In Section 2 we review some basic facts on Massey products. In Section 3 we discuss embedding problems. In Section 4 we provide a proof of Theorem 1.3 assuming Lemma 4.1. In Section 5 we use Poitou-Tate duality as one of the main tools to establish the technical Lemma 4.1.

Acknowledgments: We would like to thank Stefan Gille, Thong Nguyen Quang Do and Kirsten Wickelgren for their interest and correspondence.

2. Review of Massey products

In this section, we review some basic facts about Massey products, see [MT] and references therein for more detail.

Let A be a unital commutative ring. Recall that a differential graded algebra (DGA) over A is a graded associative A-algebra

$$\mathcal{C}^\bullet = \oplus_{k\geq 0}\mathcal{C}^k = \mathcal{C}^0 \oplus \mathcal{C}^1 \oplus \mathcal{C}^2 \oplus \cdots$$

with product $\cup$ and equipped with a differential $\delta\colon \mathcal{C}^\bullet \to \mathcal{C}^{\bullet+1}$ such that

(1) δ is a derivation, i.e.,

$$\delta(a\cup b) = \delta a \cup b + (-1)^k a \cup \delta b \quad (a \in \mathcal{C}^k);$$

(2) $\delta^2 = 0$.

Then as usual the cohomology $H^\bullet = \ker\delta/\mathrm{im}\delta$. We shall assume that $a_1, \ldots, a_n$ are elements in H^1.

Definition 2.1. A collection $M = (a_{ij})$, $1 \leq i < j \leq n+1$, $(i,j) \neq (1, n+1)$ of elements of $\mathcal{C}^1$ is called a *defining system* for the *nth order Massey product* $\langle a_1, \ldots, a_n\rangle$ if the following conditions are fulfilled:

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

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 M, and is denoted by $\langle a_1, \ldots, a_n\rangle_M$.

The product $\langle a_1, \ldots, a_n\rangle$ itself is the subset of H^2 consisting of all elements which can be written in the form $\langle a_1, \ldots, a_n\rangle_M$ for some defining system M.

When $n = 3$ we will speak about a *triple* Massey product.

For $n \geq 2$ we say that $\mathcal{C}^\bullet$ has the *vanishing n-fold Massey product property* if every defined Massey product $\langle a_1, \ldots, a_n \rangle$, where $a_1, \ldots, a_n \in \mathcal{C}^1$, necessarily contains 0.

Now let G be a profinite group and let A be a finite commutative ring considered as a trivial discrete G-module. Let $\mathcal{C}^\bullet = \mathcal{C}^\bullet(G, A)$ be the DGA of inhomogeneous continuous cochains of G with coefficients in A [NSW, Ch. I, §2]. We write $H^i(G, A)$ for the corresponding cohomology groups.

Definition 2.2. We say that G has the *vanishing n-fold Massey product property (with respect to A)* if the DGA $\mathcal{C}^\bullet(G, A)$ has the vanishing n-fold Massey product property.

Let K be a field. We say that K has the *vanishing n-fold Massey product property (with respect to A)* if its absolute Galois group G_K has the vanishing n-fold Massey product property (with respect to A).

As observed by Dwyer [Dwy] in the discrete context (see also [Ef, §8] in the profinite case), defining systems for the DGA $\mathcal{C}^\bullet(G, A)$ can be interpreted in terms of upper-triangular unipotent representations of G, as follows.

Let $\mathbb{U}_{n+1}(A)$ be the group of all upper-triangular unipotent $(n+1) \times (n+1)$-matrices with entries in A. Let $Z_{n+1}(A)$ be the subgroup of all such matrices with all off-diagonal entries being 0 except at position $(1, n+1)$. We may identify $\mathbb{U}_{n+1}(A)/Z_{n+1}(A)$ with the group $\bar{\mathbb{U}}_{n+1}(A)$ of all upper-triangular unipotent $(n+1) \times (n+1)$-matrices with entries over A with the $(1, n+1)$-entry omitted.

For a representation $\rho\colon G \to \mathbb{U}_{n+1}(A)$ and $1 \leq i < j \leq n+1$, let $\rho_{ij}\colon G \to A$ be the composition of ρ with the projection from $\mathbb{U}_{n+1}(A)$ to its (i, j)-coordinate. We use similar notation for representations $\bar{\rho}\colon G \to \bar{\mathbb{U}}_{n+1}(A)$. Note that $\rho_{i,i+1}$ (resp., $\bar{\rho}_{i,i+1}$) is a group homomorphism.

Theorem 2.3 ([Dwy, Theorem 2.4]). *Let $\alpha_1, \ldots, \alpha_n$ be elements of $H^1(G, A)$. There is a one-one correspondence $M \leftrightarrow \bar{\rho}_M$ between defining systems M for $\langle \alpha_1, \ldots, \alpha_n \rangle$ and group homomorphisms $\bar{\rho}_M\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ with $(\bar{\rho}_M)_{i,i+1} = -\alpha_i$, for $1 \leq i \leq n$.*

Moreover $\langle \alpha_1, \ldots, \alpha_n \rangle_M = 0$ in $H^2(G, A)$ if and only if the dotted arrow exists in the following commutative diagram

$$\begin{tikzcd}
& & & G \arrow[dl, dashed] \arrow[d, "\bar{\rho}_M"] & \\
0 \arrow[r] & A \arrow[r] & \mathbb{U}_{n+1}(A) \arrow[r] & \bar{\mathbb{U}}_{n+1}(A) \arrow[r] & 1.
\end{tikzcd}$$

Explicitly, the one-one correspondence in Theorem 2.3 is given by: For a defining system $M = (a_{ij})$ for $\langle \alpha_1, \ldots, \alpha_n \rangle$, $\bar{\rho}_M\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ is given by letting $(\bar{\rho}_M)_{ij} = -a_{ij}$.

Corollary 2.4. *The following conditions are equivalent.*

(i) *G has the vanishing n-fold Massey product property.*
(ii) *For every representation $\bar{\rho}\colon G \to \bar{\mathbb{U}}_{n+1}(A)$, there is a representation $\rho\colon G \to \mathbb{U}_{n+1}(A)$ such that $\rho_{i,i+1} = \bar{\rho}_{i,i+1}$, for $i = 1, 2, \ldots, n$.*

3. Embedding problems

A *weak embedding problem* $\mathcal{E}$ for a profinite group G is a diagram

$$\mathcal{E} := \begin{tikzcd} & G \arrow[d, "\alpha"] \\ U \arrow[r, "f"] & \bar{U} \end{tikzcd}$$

which consists of profinite groups U and $\bar{U}$ and homomorphisms $\alpha\colon G \to \bar{U}$, $f\colon U \to \bar{U}$ 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 $\beta\colon G \to U$ 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 $M := \ker(f)$.

Let $\phi_1\colon G_1 \to G$ be a homomorphism of profinite groups. Then ϕ_1 induces the following weak embedding problem

$$\mathcal{E}_1 := \begin{tikzcd} & G \arrow[d, "\alpha\circ\phi_1"] \\ U \arrow[r, "f"] & \bar{U}. \end{tikzcd}$$

If β is a weak solution of $\mathcal{E}$ then $\beta \circ \phi_1$ is a weak solution of $\mathcal{E}_1$.

Lemma 3.1. *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*

$$\begin{tikzcd} & & & G \arrow[dl, dashed] \arrow[d, "(\bar{\rho}_{12},\bar{\rho}_{23},\bar{\rho}_{34})"] & \\ 0 \arrow[r] & M \arrow[r] & \mathbb{U}_4(\mathbb{F}_p) \arrow[r] & (\mathbb{F}_p)^3 \arrow[r] & 1, \end{tikzcd}$$

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

Proof. This follows from Corollary 2.4. □

For $1 \le i, j \le 4$, let E_{ij} denote the 4-by-4 matrix with the 1 of $\mathbb{F}_p$ in the position (i, j) and 0 elsewhere. It is well-known that $1 + E_{12}, 1 + E_{23}$ and $1 + E_{34}$ generate $\mathbb{U}_4(\mathbb{F}_p)$.

Corollary 3.2. *Let p be an arbitrary prime. Let K be a field containing a primitive p-th root of unity. Assume that K has the vanishing triple Massey product property with respect to $\mathbb{F}_p$. Let $a, b, c \in K^\times$ and assume that the classes $[a], [b], [c]$ in the $\mathbb{F}_p$-vector space $K^\times/(K^\times)^p$ are linearly independent. Assume further that $\chi_a \cup \chi_b = \chi_b \cup \chi_c = 0$ in $H^2(G_K, \mathbb{F}_p)$. Then the Galois extension $K(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/K$ can be embedded in a $\mathbb{U}_4(\mathbb{F}_p)$-Galois extension L/K.*

Proof. Since $\chi_a \cup \chi_b = \chi_b \cup \chi_c = 0$, the triple Massey product $\langle -\chi_a, -\chi_b, -\chi_c\rangle$ is defined. By Theorem 2.3 there is a group homomorphism $\bar{\rho}\colon G_K \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$ such that $\bar{\rho}_{12} = \chi_a$, $\bar{\rho}_{23} = \chi_b$ and $\bar{\rho}_{34} = \chi_c$. By Lemma 3.1, $(\bar{\rho}_{12}, \bar{\rho}_{23}, \bar{\rho}_{34})$ can be lifted to a homomorphism $\rho\colon G_K \to \mathbb{U}_4(\mathbb{F}_p)$. Let $F = K(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$. Then F/K is a Galois extension, and its Galois group is generated by $\sigma_a, \sigma_b, \sigma_c$. Here σ_a is defined by

$$\sigma_a(\sqrt[p]{a}) = \zeta_p \sqrt[p]{a}, \quad \sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}, \quad \sigma_a(\sqrt[p]{c}) = \sqrt[p]{c}.$$

The automorphisms σ_b and σ_c are defined similarly by

$$\sigma_b(\sqrt[p]{a}) = \sqrt[p]{a}, \quad \sigma_a(\sqrt[p]{b}) = \xi_p \sqrt[p]{b}, \quad \sigma_a(\sqrt[p]{c}) = \xi_p \sqrt[p]{c},$$
$$\sigma_c(\sqrt[p]{a}) = \sqrt[p]{a}, \quad \sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}, \quad \sigma_a(\sqrt[p]{c}) = \xi_p \sqrt[p]{c}.$$

We extend σ_a, σ_b, σ_c to automorphisms of $K^{\rm sep}$ over K, still denoted by $\sigma_a, \sigma_b, \sigma_c$. Then $\rho(\sigma_a) \equiv 1 + E_{12} \bmod M$, where M is as in Lemma 3.1. In fact it follows from

$$\begin{aligned} \rho_{12}(\sigma_a) &= \chi_a(\sigma_a) = 1, \text{ and}\\ \rho_{23}(\sigma_a) &= \chi_b(\sigma_a) = 0, \text{ and}\\ \rho_{34}(\sigma_a) &= \chi_c(\sigma_a) = 0. \end{aligned}$$

Similarly, one can check that $\rho(\sigma_b) \equiv 1 + E_{23} \bmod M$ and $\rho(\sigma_c) \equiv 1 + E_{34} \bmod M$. Since M is the Frattini subgroup of $\mathbb{U}_4(\mathbb{F}_p)$, we obtain that $\rho\colon G_K \to \mathbb{U}_4(\mathbb{F}_p)$ is surjective, and the result follows. □

Remark 3.3. Let p be an arbitrary prime. Let K be a field containing a primitive p-th root of unity. Let L/K be a $\mathbb{U}_4(\mathbb{F}_p)$-extension. Then there exist $a, b, c \in K^\times \cap L^p$ such that the classes $[a], [b], [c]$ in the $\mathbb{F}_p$-vector space $K^\times/(K^\times)^p$ are linearly independent and that $\chi_a \cup \chi_b = \chi_b \cup \chi_c = 0$ in $H^2(G_K, \mathbb{F}_p)$. In fact let $\rho\colon G_K \twoheadrightarrow \mathrm{Gal}(L/K) \simeq \mathbb{U}_4(\mathbb{F}_p)$ be the corresponding homomorphism. Then by Kummer theory there exist a, b, c in $K^\times \cap L^p$ such that $\rho_{12} = \chi_a$, $\rho_{23} = \chi_b$ and $\rho_{34} = \chi_c$. Since $(\rho_{12}, \rho_{23}, \rho_{34})\colon G_K \to \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ is surjective, we see that the classes $[a], [b], [c]$ in $K^\times/(K^\times)^p$ are $\mathbb{F}_p$-linearly independent. By Theorem 2.3 (or by using directly the hypothesis that ρ is a group homomorphism), we see that

$$\chi_a \cup \chi_b = \rho_{12} \cup \rho_{23} = 0,$$

and that

$$\chi_b \cup \chi_c = \rho_{23} \cup \rho_{34} = 0.$$

Remark 3.4. Corollary 1.4 will follow immediately from Corollary 3.2 once we succeed in establishing Theorem 1.3 and its local version.

Lemma 3.5 (Hoechsmann). *Let $\mathcal{E}$ be a finite weak embedding problem for G with finite abelian kernel M. Let $\epsilon \in H^2(\bar{U}, M)$ be the cohomology class corresponding to the group extension of $\mathcal{E}$. Then $\mathcal{E}$ has a weak solution if and only if $\alpha^*(\epsilon) = 0 \in H^2(G, M)$.*

Proof. See [NSW, Chapter 3, §5, Proposition 3.5.9]. Note that the statement in *loc. cit.* requires that $\mathcal{E}$ is an embedding problem, but its proof goes well with weak embedding problems. □

Corollary 3.6. *Let $\mathcal{E}(G) = (\alpha\colon G \to \bar{U}, f\colon U \to \bar{U})$ be a finite weak embedding problem for G with abelian kernel M. Let $\phi_i\colon G_i \to G, i \in I$, be a family of homomorphisms of profinite groups. Assume that the natural homomorphism*

$$H^2(G, M) \to \prod_i H^2(G_i, M),$$

is injective. Then the weak embedding problem $\mathcal{E}(G)$ has a weak solution if and only if for every $i \in I$ the induced weak embedding problem $\mathcal{E}(G_i)$ has a weak solution.

Proof. The following diagram

$$\begin{tikzcd} H^2(\bar{U}, M) \arrow[r] \arrow[d, "\alpha^*"] & \prod_{i\in I} H^2(G_i, M) \arrow[d, equal] \\ H^2(G, M) \arrow[r] & \prod_{i\in I} H^2(G_i, M), \end{tikzcd}$$

is commutative. Now the statement follows from Lemma 3.5. □

4. Main Theorem

Consider the following exact sequence of finite groups

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

here $a_{ij}\colon \mathbb{U}_4(\mathbb{F}_p) \to \mathbb{F}_p$ is the map sending a matrix to its (i, j)-coefficient. Since M is abelian, the conjugate action of $\mathbb{U}_4(\mathbb{F}_p)$ on M induces an action of $B := (\mathbb{F}_p)^3$ on M, i.e., we get a homomorphism $\psi\colon B \to \mathrm{Aut}(M)$.

Let K be a global field containing a primitive p-th root of unity. Let $\bar{\rho}\colon G_K \to (\mathbb{F}_p)^3 = B$ be any (continuous) homomorphism, we consider M as a G_K-module via

$$\psi \circ \bar{\rho}\colon \mathrm{Gal}_K \xrightarrow{\bar{\rho}} B \xrightarrow{\psi} \mathrm{Aut}(M).$$

For each prime v of K, let K_v denote the completion of K at v. We will fix an embedding $\iota_v\colon G_{K_v} \hookrightarrow G_K$ which is induced by choosing an embedding of K^{sep} in K_v^{sep}. Then for each i, ι_v's induce a homomorphism

$$H^i(G_K, M) \to \prod_v H^i(G_{K_v}, M).$$

(Here the product is taken over the set of all primes of K.) This homomorphism does not depend on the choice of embeddings $K^{\mathrm{sep}} \hookrightarrow K_v^{\mathrm{sep}}$, and it is called the *localization map*.

Lemma 4.1. *The localization map*

$$H^2(G_K, M) \to \prod_v H^2(G_{K_v}, M),$$

is injective.

We will prove Lemma 4.1 in the next section.

Theorem 4.2. *Let K be a local field containing a primitive p-th root of unity. Then the triple Massey product $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0 whenever it is defined.*

Proof. Let $G = G_K(p)$ be the maximal pro-p quotient of the absolute Galois group of K. Then G is a Demushkin group. Hence, by [MT, Theorem 4.2] G has the vanishing triple Massey product property. □

Theorem 4.3. *Let K be a global field containing a primitive p-th root of unity. Then the triple Massey product $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0 whenever it is defined.*

Proof. We shall prove the condition (ii) in Lemma 3.1.

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

$$(\mathcal{E}) \qquad \begin{tikzcd} & & & G_K \arrow[d, "(\bar\rho_{12},\bar\rho_{23},\bar\rho_{34})"] & \\ 0 \arrow[r] & A \arrow[r] & \mathbb{U}_4(\mathbb{F}_p) \arrow[r] & (\mathbb{F}_p)^3 \arrow[r] & 1. \end{tikzcd}$$

Then by Theorem 4.2 and by Lemma 3.1, we deduce that for every prime v of K, the (local) weak embedding problem $(\mathcal{E}_v)$

$$(\mathcal{E}_v) \qquad \begin{tikzcd} & & & G_{K_v} \arrow[d, "(\bar\rho_{12},\bar\rho_{23},\bar\rho_{34})"] \arrow[dl, dashed] & \\ 0 \arrow[r] & A \arrow[r] & \mathbb{U}_4(\mathbb{F}_p) \arrow[r] & (\mathbb{F}_p)^3 \arrow[r] & 1, \end{tikzcd}$$

which is induced from $(\mathcal{E})$, has a weak solution. By Lemma 4.1 and Corollary 3.6, $(\mathcal{E})$ has a weak solution also, and we are done. □

5. Proof of Lemma 4.1

Let G be a profinite group, and let M be a discrete G-module. We define

$$H^1_*(G, M) = \ker(H^1(G, M) \to \prod_C H^1(C, M)),$$

where the product is over all closed cyclic subgroups (in the profinite sense) of G.

(The definition of $H^1_*(G, M)$ is due to Tate (see [Se, §2]). This definition also appeared in [DZ, §2], in which the authors used the notation $H^1_{\rm loc}$ instead of using H^1_*.)

Now let K be a global field. Let G_K be the absolute Galois group of K. For any G_K-module M with the structure map $\rho\colon G_K \to \mathrm{Aut}(M)$ we denote $K(M)$ the smallest splitting field of M, explicitly $K(M)$ is the fixed field of the separable closure K^{sep} under $\ker(\rho\colon G_K \to \mathrm{Aut}(M))$. In the next lemma for each prime v of K, we choose an extension w of v to K^{sep}.

Lemma 5.1. *Let F be a finite Galois extension of K containing $K(M)$. Let S be a set of primes of K with Dirichlet density 1. Let*

$$\beta^1_S(F/K, M)\colon H^1(\mathrm{Gal}(F/K), M) \to \prod_{v\in S} H^1(\mathrm{Gal}(F_w/K_v), M),$$

be the map induced by the restriction maps. Then we have the following commutative diagram

$$\begin{array}{ccc} \ker \beta^1_S(F/K, M) & \xrightarrow{\simeq} & \ker \beta^1_S(K^{\mathrm{sep}}/K, M) \\ \big\downarrow & & \big\downarrow \\ H^1_*(\mathrm{Gal}(F/K), M) & \xrightarrow{\simeq} & H^1_*(\mathrm{Gal}_K, M). \end{array}$$

Proof. See [Mi, Chapter I, Lemma 9.3] and/or [Ja, Lemma 1]. See also [Se, Proposition 8] for the case that S is the complement of a finite set of primes. □

We shall apply Lemma 5.1 to S consisting of all primes of K.

Now we recall that we have the following exact sequence of finite groups

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

here $a_{ij}\colon \mathbb{U}_4(\mathbb{F}_p) \to \mathbb{F}_p$ is the map sending a matrix to its (i,j)-coefficient. This exact sequence induces a $B := (\mathbb{F}_p)^3$-module structure on M.

Lemma 5.2. *Let $M' = \mathrm{Hom}(M, \mathbb{F}_p)$ be the dual B-module of the B-module M. Then there exists an $\mathbb{F}_p$-basis of M' such that with respect to this basis the structure map $\alpha\colon B \to \mathrm{Aut}(M')$ becomes the map $\alpha\colon B \to \mathrm{GL}_3(\mathbb{F}_p)$, which sends $(x,y,z) \in B$ to* $\begin{bmatrix} 1 & 0 & x \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix}$.

Proof. We first describe the action of $B := (\mathbb{F}_p)^3$ on M, i.e., we describe the map $\psi\colon B \to \mathrm{Aut}(M)$, as follows. Explicitly,

$$M = \{ \begin{bmatrix} 1 & 0 & a & b \\ 0 & 1 & 0 & c \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{F}_p \}.$$

Let $e_1 = I + E_{14}$, $e_2 = I + E_{13}$, $e_3 = I + E_{24}$. With respect to the $\mathbb{F}_p$-basis (e_1, e_2, e_3) of M, $(x,y,z) \in (\mathbb{F}_p)$ is sent to the matrix $\begin{bmatrix} 1 & z & -x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Now we consider the B-module M'. With respect to the dual basis of (e_1, e_2, e_3), the structure map $\alpha\colon B \to \mathrm{Aut}(M')$ describing the action of B on M' is given by:

$$(x,y,z) \mapsto \begin{bmatrix} 1 & 0 & 0 \\ -z & 1 & 0 \\ x & 0 & 1 \end{bmatrix}.$$

Then the statement follows by noting that the matrix $\begin{bmatrix} 1 & 0 & 0 \\ -z & 1 & 0 \\ x & 0 & 1 \end{bmatrix}$ is conjugate to the matrix $\begin{bmatrix} 1 & 0 & x \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix}$ via the element $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. □

The following lemma is a special case of [DZ, Lemma 3.3]. It is a simple lemma and therefore we also omit a proof.

Lemma 5.3. *Let V be a vector space of finite dimension over a field k. Let φ_1, φ_2 be elements in the dual k-vector space $V^* := \mathrm{Hom}(V, k)$. If $\ker \varphi_1 \subseteq \ker \varphi_2$ then there exists $\lambda \in k$ such that $\varphi_2 = \lambda\varphi_1$.*

Lemma 5.4. *Let*

$$G = \{ \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : a, b \in \mathbb{F}_p \},$$

and let $(\mathbb{F}_p)^3$ be the natural $\mathbb{F}_p[G]$-module where G acts on $(\mathbb{F}_p)^3$ by matrix multiplication. Then $H^1_*(G, (\mathbb{F}_p)^3) = 0$.

Proof. Let (Z_σ) be a cocycle representing an element in $H^1_*(G, (\mathbb{F}_p)^3)$. Then for each $\sigma \in G$, there exists $W_\sigma \in (\mathbb{F}_p)^3$ such that

$$Z_\sigma = (\sigma - 1)W_\sigma.$$

Writing $Z_\sigma = \begin{bmatrix} x_\sigma \\ y_\sigma \\ z_\sigma \end{bmatrix}$, $W_\sigma = \begin{bmatrix} u_\sigma \\ v_\sigma \\ t_\sigma \end{bmatrix}$ and $\sigma = \begin{bmatrix} 1 & 0 & a_\sigma \\ 0 & 1 & b_\sigma \\ 0 & 0 & 1 \end{bmatrix}$, we have

$$\begin{bmatrix} x_\sigma \\ y_\sigma \\ z_\sigma \end{bmatrix} = \begin{bmatrix} 0 & 0 & a_\sigma \\ 0 & 0 & b_\sigma \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} u_\sigma \\ v_\sigma \\ t_\sigma \end{bmatrix} = \begin{bmatrix} t_\sigma a_\sigma \\ t_\sigma b_\sigma \\ 0 \end{bmatrix}.$$

Hence

(1) $$x_\sigma = t_\sigma a_\sigma, y_\sigma = t_\sigma b_\sigma, z_\sigma = 0.$$

By the cocycle condition, $\sigma \mapsto x_\sigma$ and $\sigma \mapsto y_\sigma$ are homomorphisms. Also, $\sigma \mapsto a_\sigma$ and $\sigma \mapsto b_\sigma$ are homomorphisms. From (1), one has $\ker a_\sigma \subseteq \ker x_\sigma$ and $\ker b_\sigma \subseteq \ker y_\sigma$. Hence by Lemma 5.3, there exist $\lambda, \mu \in \mathbb{F}_p$ such that

(2) $$x_\sigma = \lambda a_\sigma; y_\sigma = \mu b_\sigma.$$

We consider the matrix $\sigma_0 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$, i.e., $a_{\sigma_0} = b_{\sigma_0} = 1$. Then (1) and (2) imply that

$$x_{\sigma_0} = t_{\sigma_0} = \lambda, \text{ and } y_{\sigma_0} = t_{\sigma_0} = \mu.$$

Thus $\lambda = \mu$. Hence $Z_\sigma = (\sigma - 1)W$, with $W = (0, 0, \lambda)^t$. Therefore (Z_σ) is cohomologous to 0, as desired. □

We are now ready to prove Lemma 4.1, and the proof of Theorem 4.3 will then be complete.

Proof of Lemma 4.1. First note that if we consider $M' = \mathrm{Hom}(M, \mathbb{F}_p)$ as a G_K-module via the map $\beta\colon \mathrm{Gal}_K \to B \xrightarrow{\alpha} \mathrm{Aut}(M')$, then M' is the dual G_K-module of the G_K-module M. Now by Poitou-Tate duality ([NSW, Theorem 8.6.7]), it is enough to show that

$$\ker(H^1(G_K, M') \to \prod_v H^1(G_{K_v}, M')) = 0. \tag{3}$$

Let $F = (K^{\mathrm{sep}})^{\ker \beta}$ be the splitting field of M'. Then $\mathrm{Gal}(F/K) \simeq \mathrm{im}\beta \subseteq \mathrm{im}\alpha = G$, where G is the group defined in Lemma 5.4.

If $\mathrm{Gal}(F/K) \simeq \mathrm{im}\beta = G$, then by Lemma 5.4, $H^1_*(\mathrm{Gal}(F/K), M') = 0$. If $\mathrm{Gal}(F/K) \simeq \mathrm{im}\beta \neq G$, then $\mathrm{Gal}(F/K)$ is of order dividing p, and hence it is cyclic. In this case, it is clear that $H^1_*(\mathrm{Gal}(F/K), M') = 0$. Thus in all cases we have $H^1_*(\mathrm{Gal}(F/K), (\mathbb{F}_p)^3) = 0$. Therefore by Lemma 5.1, it implies that (3) is true, as desired. □

References

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

[DZ] R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France 129 (3), 2001, 317-338.

[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*, available at arXiv:1301.0896.

[GLMS] W. Gao, D. B. Leep, J. Mináč and T. Smith, *Galois groups over nonrigid fields*. Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), 61-77, Fields Inst. Commun., 33, Amer. Math. Soc., Providence, RI, 2003.

[GM] P. A. Griffiths and J. W. Morgan, *Rational homotopy theory and differential forms*, Progress in Mathematics 16, Birkhäuser, Boston, Mass., 1981.

[HW] M. J. Hopkins and K. G. Wickelgren, *Splitting varieties for triple Massey products*, preprint (2012).

[Ja] U. Jannsen, *Galoismoduln mit Hasse-Prinzip*, J. Reine Angew. Math. 337 (1982), 154-158.

[LW] D. B. Leep and A. R. Wadsworth, *The transfer ideal of quadratic forms and a Hasse norm theorem mod squares*, Trans. Amer. Math. Soc. 315 (1989), no. 1, 415-432.

[Ma] W. S. Massey, *Some higher order cohomology operations*, Symposium internacional de topología algebraica (International symposium on algebraic topology), Mexico City: Universidad Nacional Autónoma de México and UNESCO (1958), 145-154,

[Mi] J. Milne, *Arithmetic duality theorems*, second edition, BookSurge, LLC, 2006.

[MT] J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*, preprint (2013) arXiv:1307.6624.

[Mo] M. Morishita, *Knots and primes. An introduction to arithmetic topology*, Universitext. Springer, London, 2012.

[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.

[Se] J.-P. Serre, *Sur les groupes de congruence des variétés abéliennes*, Izv. Akad. Nauk. SSSR 28 (1964), 3-20.

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