TRIPLE MASSEY PRODUCTS AND ABSOLUTE GALOIS GROUPS

IDOEFRAT AND ELIYAHU MATZRI

Abstract. Let $p$ be a prime number, $F$ a field containing a root of unity of order $p$, and $G_F$ the absolute Galois group. Extending results of Hopkins, Wickelgren, Mináč and Tărnăc, we prove that the triple Massey product $H^1(G_F)^3 \to H^2(G_F)$ contains 0 whenever it is nonempty. This gives a new restriction on the possible profinite group structure of $G_F$.

A main problem in modern Galois theory is to understand the group-theoretic structure of absolute Galois groups $G_F = \text{Gal}(F_{\text{sep}}/F)$ of fields $F$, that is, the possible symmetry patterns of roots of polynomials. General restrictions on the possible structure of the profinite group $G_F$ are rare: By classical results of Artin and Schreier, the torsion in $G_F$ can consist only of involutions. In addition, the celebrated work of Voevodsky and Rost ([Voe03], [Voe11]) identifies the cohomology ring $H^*(G_F) = H^*(G_F, \mathbb{Z}/m)$ with the mod-$m$ Milnor $K$-ring $K^M_*(F)/m$, assuming existence of $m$-th roots of unity. In particular, the graded ring $H^*(G_F)$ is generated by its degree 1 elements, and its relations originate from the degree 2 component. This can be used to rule out many more profinite groups from being absolute Galois groups of fields ([CEM12], [EM11b]). In fact, the Artin–Schreier restriction about the torsion also follows from the latter results [EM11b, Ex. 6.4(2)].

Very recently, a remarkable series of works by Hopkins, Wickelgren, Mináč and Tărnăc indicated the possible existence of a new kind of general restrictions on the structure of absolute Galois groups, related to the differential graded algebra $C^*(G_F) = C^*(G_F, \mathbb{Z}/m)$ of continuous cochains on $G_F$. The interplay between $C^*(G_F)$ and its cohomology algebra $H^*(G_F)$ gives rise to external operations on $H^*(G_F)$, in addition to its (“internal”) ring structure with respect to the cup product, notably, the $n$-fold Massey

2010 Mathematics Subject Classification. Primary 12G05, 12E30, 16K50.

Key words and phrases. Triple Massey products, absolute Galois groups, Galois cohomology.

The authors were supported by the Israel Science Foundation (grant No. 152/13). The second author was also partially supported by the Kreitman foundation.
products $H^1(G_F)^n \to H^2(G_F)$. The definition of the Massey product in the context of general differential algebras is recalled in §1, and at this stage we only mention that it is a multi-valued map, which for $n = 2$ coincides with the cup product. The Massey product $\langle \chi_1, \ldots, \chi_n \rangle \subseteq H^2(G_F)$ is essential if it is non-empty, but does not contain 0. The above-mentioned works show that, under various assumptions, the triple Massey product for $H^*(G_F)$ is never essential. Thus profinite groups $G$ for which $H^*(G)$ contains an essential triple Massey product cannot be realized as absolute Galois groups of fields containing a root of unity of order $p$ and satisfying these assumptions. In [MT14a] Mináč and Tân develop a method to produce such groups $G$, by examining their presentation by generators and relations modulo the 4th term in the $p$-Zassenhaus filtration. As a concrete example, the profinite group $G$ on 5 generators $\sigma_1, \ldots, \sigma_5$ and the single defining relation $[\sigma_4, \sigma_5][\sigma_2, \sigma_3, \sigma_1]$ gives rise to an essential triple Massey product [MT14a, Ex. 7.2].

Specifically, assume that $m = p$ is prime, and $F$ contains a root of order $p$ (so char $F \neq p$). It was shown that the triple Massey product for $H^*(G_F)$ is never essential in the following situations:

1) $p = 2$ and $F$ is a local field or a global field (Hopkins and Wickelgren [HW15]);
2) $p = 2$ and $F$ is arbitrary (Mináč and Tân [MT14a]);
3) $p$ is arbitrary and $F$ is a local field (Mináč and Tân; follows from [MT14a, Th. 4.3] and [MT15, Th. 8.5]);
4) $p$ is arbitrary, and $F$ is a global field (Mináč and Tân [MT14b]).

Moreover, it is conjectured in [MT15] that the $n$-fold Massey product above is never essential for every $n \geq 3$. Also, in [EM14] we find close connections between these results and classical facts in the theory of central simple algebras. In particular, 2) is closely related to Albert’s characterization from 1939 [Alb39] (as refined by Rowen [Row84]) of the central simple algebras of exponent 2 and degree 4 as biquaternionic algebras.

Motivated by these works, we prove in this paper the above conjecture for triple Massey products for arbitrary $p$ and general fields $F$ as above:

**Main Theorem.** Let $F$ be a field containing a root of unity of order $p$, and let $\chi_1, \chi_2, \chi_3 \in H^1(G_F)$. Then $\langle \chi_1, \chi_2, \chi_3 \rangle$ is not essential.

The Main Theorem was first proved by the second-named author using methods from the theory of central simple algebras, notably the Amitsur–Saltman theory of abelian crossed products [Mat14]. The current paper, which replaces [Mat14], is based on a shortcut which allows carrying
the original crossed product computations to the framework of profinite group cohomology (see Proposition 5.3). We also work in a more general formal context, and prove the Main Theorem for $p$-Kummer formations $(G, A, \{\kappa_U\}_U)$ (Theorem 5.4). These structures axiomatize the relevant Galois-theoretic properties of absolute Galois groups: the Kummer isomorphism, Hilbert’s Theorem 90, and the connections between restriction, correstriction, and cup product. The Main Theorem is just the case where $G = G_F$, $A = F_{\text{sep}}^\times$, and the $\kappa_U$ are the Kummer maps (see §5).

The Main Theorem is in a partial analogy with the important work of Deligne, Griffiths, Morgan, and Sullivan [DGMS75], which proves that any compact Kähler manifold is formal. This implies that its $n$-fold Massey products, with $n \geq 3$, are non-essential in the de Rahm context (see also [Huy05, Ch. 3.A]). On the other hand, links in $\mathbb{R}^3$ provide examples of essential Massey products in the algebra of singular cochains. For instance, the Borromean rings give rise to an essential triple Massey product [Hil12, §10.1], and this explains why they are not equivalent to three unconnected circles. Thus the Main Theorem means that a phenomena such as the Borromean rings is impossible in this Galois cohomology context. We also note that examples due to Positselski show that $H^*(G_F)$ may not be formal [Pos11, §9.11].

Among the other works on Massey products in Galois cohomology we mention those by Morishita [Mor04], Sharifi ([Sha99], [Sha07]), Wickelgren ([Wic12a], [Wic12b]), Vogel [Vog05], Gärtner [Gär15], and the first-named author [Efr14].

We thank Ján Mináč, Leonid Positselski, Louis Rowen, Nguyen Duy Tân, Uzi Vishne and Kirsten Wickelgren for discussions over the past few years on various aspects of Massey products and of this work.

Addendum (January 2015): In the recent paper [MT14c] (which was posted after the initial version [Mat14] of the current work) Mináč and Tân also give a Galois-cohomological proof of the Main Theorem, which is similar at several points to our proof. Moreover, they point out that the standard restriction-correstriction argument allows one to remove the assumption that the field contains a root of unity of order $p$. Namely, for a $p$th root of unity $\zeta$, the index of $U = G_{F(\zeta)}$ in $G = G_F$ is prime to $p$. If $\chi_1, \chi_2, \chi_3 \in H^1(G)$ and $\alpha \in \langle \chi_1, \chi_2, \chi_3 \rangle$, then by our Main Theorem, $\text{Res}_U \alpha = \text{Res}_U (\chi_1) \cup \psi_1 + \text{Res}_U (\chi_3) \cup \psi_3$ for some $\psi_1, \psi_3 \in H^1(U)$. Hence $(G: U) \alpha = \chi_1 \cup \text{Cor}_G(\psi_1) + \chi_3 \cup \text{Cor}_G(\psi_3)$, and consequently $0 \in \langle \chi_1, \chi_2, \chi_3 \rangle$ (see §1).
1. Massey products

We recall the definition and basic properties of Massey products of degree 1 cohomology elements. We first recall that a differential graded algebra over a ring $R$ (abbreviated R-DGA) is a graded $R$-algebra $C^\bullet = \bigoplus_{r=0}^\infty C^r$ equipped with $R$-module homomorphisms $\partial^r : C^r \to C^{r+1}$ such that $\partial = \bigoplus_{r=0}^\infty \partial^r$ satisfies $\partial \circ \partial = 0$ and one has: $\partial^{r+1}(ab) = \partial^r(a)b + (\partial b)a$ for $a \in C^r$, $b \in C^s$ (the Leibnitz rule). Set $Z^r = \text{Ker}(\partial^r)$, $B^r = \text{Im}(\partial^{r-1})$, and $H^r = Z^r / B^r$, and let $[c]$ denote the class of $c \in Z^r$ in $H^r$. Then $H^\bullet = \bigoplus_{r=0}^\infty H^r$ has an induced $R$-DGA structure with zero differentials $\partial^r$. We say that the DGA $C^\bullet$ is graded-commutative if $ab = (-1)^{rs}ba$ for $a \in C^r$ and $b \in C^s$.

We fix an integer $n \geq 2$. Consider a system $c_{ij} \in C^1$, where $1 \leq i \leq j \leq n$ and $(i, j) \neq (1, n)$. For any $i, j$ satisfying $1 \leq i \leq j \leq n$ (including $(i, j) = (1, n)$) we define

$$
\widetilde{c}_{ij} = \sum_{r=1}^{j-1} c_{ir}c_{r+1,j} \in C^2.
$$

One says that $(c_{ij})$ is a defining system of size $n$ in $C^\bullet$ if $\partial c_{ij} = \widetilde{c}_{ij}$ for every $1 \leq i \leq j \leq n$ with $(i, j) \neq (1, n)$. We also say that the defining system $(c_{ij})$ is on $c_{11}, \ldots, c_{nn}$. Note that then $c_{ii}$ is a 1-cocycle, $i = 1, 2, \ldots, n$. Further, $\widetilde{c}_{nn}$ is a 2-cocycle ([Kra66, p. 432], [Fen83, p. 233]). Its cohomology class depends only on the cohomology classes $[c_{11}], \ldots, [c_{nn}]$ [Kra66, Th. 3]. Given $c_1, \ldots, c_n \in Z^1$, the $n$-fold Massey product of $\langle [c_1], \ldots, [c_n] \rangle$ is the subset of $H^2$ consisting of all cohomology classes $[\widetilde{c}_{nn}]$ obtained from defining systems $(c_{ij})$ of size $n$ on $c_1, \ldots, c_n$ in $C^\bullet$. The Massey product $\langle [c_1], \ldots, [c_n] \rangle$ is essential if it is non-empty but does not contain $0$.

When $n = 2$, $\langle [c_1], [c_2] \rangle$ is always non-empty and consists only of $[c_1][c_2]$. In the case $n = 3$ one has the following well-known facts:

**Proposition 1.1** ([EM14, Prop. 6.1]). Let $c_1, c_2, c_3 \in Z^1$.

(a) $\langle [c_1], [c_2], [c_3] \rangle$ is non-empty if and only if $[c_1][c_2][c_3] = 0$;

(b) If $(c_{ij})$ is a defining system on $[c_1], [c_2], [c_3]$, then $\langle [c_1], [c_2], [c_3] \rangle = [\widetilde{c}_{13}] + [c_1]H^1 + H^1[c_3]$.

2. Cohomological Preliminaries

We refer, e.g., to [NSW08] for the basic notions and facts in profinite and Galois cohomology. Let $p$ be a fixed prime number and let $G$ be a profinite group acting trivially on $\mathbb{Z}/p$. We write $C^r(G)$ for the group $C^r(G, \mathbb{Z}/p)$ of continuous (inhomogenous) cochains $G^r \to \mathbb{Z}/p$. Let
Lemma 2.1. Let $\chi_1, \chi_2 \in H^1(G)$. Then there exists $\psi \in C^1(H)$ such that $\partial \psi = \chi_1 \cup \chi_2 + \chi_2 \cup \chi_1$ and $\psi$ is zero on $\text{Ker}(\chi_i)$, $i = 1, 2$.

Proof. When $\chi_1, \chi_2$ are $\mathbb{F}_p$-linearly independent, let $\bar{G} = G/(\text{Ker}(\chi_1) \cap \text{Ker}(\chi_2)) \cong (\mathbb{Z}/p)^2$, and choose $\bar{\sigma}_1, \bar{\sigma}_2 \in \bar{G}$ which are dual to $\chi_1, \chi_2$. Define $\bar{\psi} \in C^1(\bar{G})$ by $\bar{\psi}(\bar{\sigma}_1 \bar{\sigma}_2) = -ij$ for $0 \leq i, j < p$, and take $\psi = \text{Inf}_G \bar{\psi}$ be its inflation to $H^1(G)$.

When $\chi_1, \chi_2$ are nonzero and $\mathbb{F}_p$-linearly dependent, we write $\chi_2 = k\chi_1$ with $1 \leq k < p$ and $\bar{G} = G/\text{Ker}(\chi_1) \cong \mathbb{Z}/p$. We define $\bar{\psi} \in C^1(\bar{G})$ by $\bar{\psi}(\bar{\sigma}_1) = -kt^2 \in \mathbb{Z}/p$, and take $\psi = \text{inf}_G \bar{\psi}$.

Finally, when at least one of $\chi_1, \chi_2$ is 0 we take $\psi = 0 \in C^1(G)$. \qed

Example 2.2. When $G = G_F$ for a field $F$ containing a root of unity of order $p$, this sequence is exact for every such $U$ and $\chi$. This corresponds to the isomorphism $K^\times/N_{L/K}(L^\times) \cong \text{Br}(L/K)$ for the fixed fields $K, L$ of $U, \text{Ker}(\chi)$, respectively, where $\text{Br}(L/K)$ is the relative Brauer group of the field extension $L \supseteq K$ [Dra83, p. 73, Th. 1].

Proposition 2.3. Suppose that (2.1) with $U = G$ is exact at $H^2(G)$ for every $\chi \in H^1(G)$. For every $\chi_1, \chi_2, \chi_3 \in H^1(G)$ one has $\langle \chi_1, \chi_2, \chi_3 \rangle = \langle \chi_3, \chi_2, \chi_1 \rangle$.

Proof. Since both Massey products are cosets of $\chi_1 \cup H^1(G) + \chi_3 \cup H^1(G)$ (Proposition 1.1(b)), it suffices to show that $\langle \chi_1, \chi_2, \chi_3 \rangle \supseteq \langle \chi_3, \chi_2, \chi_1 \rangle$. So
let $\alpha \in \langle \chi_3, \chi_2, \chi_1 \rangle$. Then there exist $\varphi_{22}, \varphi_{21} \in C^1(G)$ such that

$$\partial \varphi_{22} = \chi_3 \cup \chi_2, \quad \partial \varphi_{21} = \chi_2 \cup \chi_1, \quad \alpha = [\chi_3 \cup \varphi_{21} + \varphi_{32} \cup \chi_1].$$

Let $K = \text{Ker}(\chi_1)$. Lemma 2.1 yields $\psi_{12} \in C^1(G)$ such that $\partial \psi_{12} = \chi_1 \cup \chi_2 + \chi_2 \cup \chi_1$ in $C^2(G)$ and $\psi_{12} = 0$ on $K = \text{Ker}(\chi_1)$. The graded-commutativity of $H^\bullet(G)$ yields $\psi_{23} \in C^1(G)$ such that $\partial \psi_{23} = \chi_2 \cup \chi_3 + \chi_3 \cup \chi_2$ in $C^2(G)$. Taking $\varphi_{12} = \psi_{12} - \varphi_{21}$ and $\varphi_{23} = \psi_{23} - \varphi_{32}$, we obtain that $\partial \varphi_{12} = \chi_1 \cup \chi_2$ and $\partial \varphi_{23} = \chi_2 \cup \chi_3$. It therefore suffices to show that $[\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3]$ and $\alpha$ are equal modulo the indeterminacy $\chi_1 \cup H^1(G) + \chi_3 \cup H^1(G)$ of both Massey products.

Now $\text{Res}_K(\partial \varphi_{21}) = \text{Res}_K(\chi_2 \cup \chi_1) = 0$, so $\text{Res}_K \varphi_{21} \in Z^1(K)$. The graded-commutativity of $H^\bullet(K)$ gives $\text{Res}_K(\varphi_{21} \cup \chi_3 + \chi_3 \varphi_{21}) \in B^2(K)$.

As $\text{Res}_K \psi_{12} = 0$ we obtain that

$$\text{Res}_K(\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3) = \text{Res}_K(\varphi_{12} \cup \chi_3) = -\text{Res}_K(\varphi_{21} \cup \chi_3)$$

$$\equiv \text{Res}_K(\chi_3 \cup \varphi_{21} + \varphi_{32} \cup \chi_1) \pmod{B^2(K)}.$$

Hence $\text{Res}_K[\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3] = \text{Res}_K \alpha$. By (2.1),

$$\alpha - [\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3] \in \chi_1 \cup H^1(G),$$

as desired. \qed

**Remark 2.4.** Vogel [Vog04, Example 1.2.11] proves the assertion of Proposition 2.3 under the assumption that $G = F/R$ for a free pro-$p$ group $F$ and a closed normal subgroup $R$ of $F$ contained in the third term of its lower central sequence. In a topological context, Kraines [Kra66, Th. 8] proves that Massey products of arbitrary length remain the same up to a sign when the order of the entries is reversed.

**Proposition 2.5.** Suppose that (2.1) with $U = G$ is exact at $H^2(G)$ for every $\chi \in H^1(G)$. The following conditions are equivalent:

1. For every $\chi_1, \chi_2, \chi_3 \in H^1(G)$, the Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is not essential.

2. For every $\chi_1, \chi_2, \chi_3 \in H^1(G)$ such that the pairs $\chi_1, \chi_3$ and $\chi_2, \chi_3$ are $\mathbb{F}_p$-linearly independent, $\langle \chi_1, \chi_2, \chi_3 \rangle$ is not essential.

**Proof.** (1)⇒(2): Trivial.

(2)⇒(1): Suppose that $\langle \chi_1, \chi_2, \chi_3 \rangle \neq \emptyset$. By Proposition 1.1(a), $\chi_1 \cup \chi_2 = 0 = \chi_2 \cup \chi_3$ in $H^2(G)$. Therefore there exist $\varphi_{12}, \varphi_{23} \in C^1(G)$ such that $\partial \varphi_{12} = \chi_1 \cup \chi_2$ and $\partial \varphi_{23} = \chi_2 \cup \chi_3$ in $C^2(G)$. Then $\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3 \in Z^2(G)$. By Proposition 1.1(b), we need to find $\varphi_{12}, \varphi_{23}$ such that the cohomology class of this 2-cocycle is contained in the subset
\( \chi_1 \cup H^1(G) + \chi_3 \cup H^1(G) \) of \( H^2(G) \). We break the discussion into several cases.

Case I: The pairs \( \chi_1, \chi_3 \) and \( \chi_2, \chi_3 \) are \( \mathbb{F}_p \)-linearly independent. Then we simply apply (2).

Case II: \( \chi_1, \chi_3 \) are \( \mathbb{F}_p \)-linearly dependent. We may assume that \( \chi_1 = i\chi_3 \) for some \( i \in \mathbb{F}_p \). Given \( \varphi_{12}, \varphi_{23} \) as above we then have

\[
\text{Res}_{\chi_3}(\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3) = 0.
\]

By (2.1), \( [\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3] \in \chi_3 \cup H^1(G) \), and we are done.

Case III: \( \chi_2 = 0 \). Then \( \chi_1 \cup \chi_2 = 0 = \chi_2 \cup \chi_3 \) in \( C^2(G) \), so for \( \varphi_{12} = \varphi_{23} = 0 \) we have \( [\chi_1 \cup \varphi_{23} + \varphi_{12} \cup \chi_3] = 0 \).

Case IV: \( \chi_1, \chi_3 \) are \( \mathbb{F}_p \)-linearly independent, \( \chi_2 \neq 0 \), and \( \chi_2, \chi_3 \) are \( \mathbb{F}_p \)-linearly dependent. Then \( \chi_1, \chi_2 \) are also \( \mathbb{F}_p \)-independent. By Proposition 2.3, \( \langle \chi_1, \chi_2, \chi_3 \rangle = \langle \chi_3, \chi_2, \chi_1 \rangle \), and by (2), \( \langle \chi_3, \chi_2, \chi_1 \rangle \) is not essential. \( \square \)

3. CUP PRODUCTS AS COBOUNDARIES

Let \( G \) be a profinite group and let \( \chi_a, \chi_b \in H^1(G) \) be \( \mathbb{F}_p \)-linearly independent. Set \( N_a = \text{Ker}(\chi_a) \), \( N_b = \text{Ker}(\chi_b) \) and \( L = N_a \cap N_b \). Thus \( G/L \cong (G/N_a) \times (G/N_b) \cong (\mathbb{Z}/p)^2 \). Let \( \sigma_a, \sigma_b \in G \) be dual to \( \chi_a, \chi_b \), respectively, i.e.,

\[
\chi_a(\sigma_a) = 1, \quad \chi_a(\sigma_b) = 0, \quad \chi_b(\sigma_a) = 0, \quad \chi_b(\sigma_b) = 1.
\]

Let \( \tau = [\sigma_a, \sigma_b] = \sigma_a \sigma_b \sigma_a^{-1} \sigma_b^{-1} \).

**Proposition 3.1.** Suppose that \( \omega \in H^1(N_b) \) satisfies \( \omega - \sigma_b \omega = \text{Res}_{N_b} \chi_a \). Then

(a) \( \omega(\tau) = 1 \);

(b) \( N_a \cap \text{Ker}(\omega) \) is normal in \( G \);

(c) \( (G : N_a \cap \text{Ker}(\omega)) = p^3 \);

(d) The images \( \bar{\sigma}_a, \bar{\sigma}_b, \bar{\tau} \) of \( \sigma_a, \sigma_b, \tau \), respectively, in \( \bar{G} = G/(N_a \cap \text{Ker}(\omega)) \) generate \( \bar{G} \) and satisfy \( [\bar{\tau}, \bar{\sigma}_a] = [\bar{\tau}, \bar{\sigma}_b] = 1 \).

**Proof.** (a) Since \( \sigma_a, \sigma_b \sigma_a \sigma_b^{-1} \in N_b \), the assumption on \( \omega \) gives

\[
\omega(\tau) = \omega(\sigma_a) + \omega(\sigma_b \sigma_a^{-1} \sigma_b^{-1}) = \omega(\sigma_a) - (\sigma_b \omega)(\sigma_a) = (\text{Res}_{N_b} \chi_a)(\sigma_a) = 1.
\]

(b) For every \( \sigma \in N_b \), we have \( \sigma \omega = \omega \), and therefore \( \sigma(\text{Res}_L \omega) = \text{Res}_L \omega \). By the assumption on \( \omega \), \( \text{Res}_L \omega = \sigma_b(\text{Res}_L \omega) = \text{Res}_L \chi_a = 0 \). Therefore \( \sigma(\text{Res}_L \omega) = \text{Res}_L \omega \) for every \( \sigma \in \langle N_b, \sigma_b \rangle = G \). This means that
\[ \omega(\sigma h \sigma^{-1}) = \omega(h) \] for every \( \sigma \in G \) and \( h \in L \). Consequently, \( \text{Ker}(\text{Res}_L \omega) \) is normal in \( G \), and we observe that \( N_a \cap \text{Ker}(\omega) = \text{Ker}(\text{Res}_L \omega) \).

(c) We note that every commutator in \( G \) is contained in \( L \). By this and (a), \( \tau \in L \setminus \text{Ker}(\text{Res}_L \omega) \), whence \( (L : \text{Ker}(\text{Res}_L \omega)) = p \). Consequently,

\[ (G : N_a \cap \text{Ker}(\omega)) = (G : L)(L : \text{Ker}(\text{Res}_L \omega)) = p^2 \cdot p = p^3. \]

(d) The images of \( \bar{\sigma}_a, \bar{\sigma}_b \) generate \( G/L \cong (\mathbb{Z}/p)^2 \). Also, \( L/(N_a \cap \text{Ker}(\omega)) = L/\text{Ker}(\text{Res}_L(\omega)) \) is generated by \( \bar{\tau} \), by (a). Hence \( \bar{\sigma}_a, \bar{\sigma}_b, \bar{\tau} \) generate \( G \). Since \( \bar{\sigma}_a, \bar{\tau} \in N_b \), we have \( \omega(\tau \sigma_a \tau^{-1} \sigma_a^{-1}) = 0 \), so \( \tau \sigma_a \tau^{-1} \sigma_a^{-1} \in N_a \cap \text{Ker}(\omega) \). Therefore \( [\bar{\tau}, \bar{\sigma}_a] = 1 \).

As \( \tau \in N_a \cap N_b \),

\[ \omega(\tau \sigma_b \tau^{-1} \sigma_b^{-1}) = \omega(\tau) + (\sigma_b \omega)(\tau^{-1}) = \omega(\tau) - (\sigma_b \omega)(\tau) = (\text{Res}_N \chi_a)(\tau) = 0. \]

Therefore \( \tau \sigma_b \tau^{-1} \sigma_b^{-1} \in N_a \cap \text{Ker}(\omega) \), i.e., \([\bar{\tau}, \bar{\sigma}_b] = 1\). \( \square \)

It follows from Proposition 3.1 that \( \bar{G} \) is the Heisenberg group \( H_{p^3} (D_4) \) when \( p = 2 \). We refer to [Sha99, Ch. II] for related results.

**Proposition 3.2.** Suppose that \( \omega \in H^1(N_b) \) satisfies \( \omega - \sigma_b \omega = \text{Res}_{N_b} \chi_a \). There exists \( \varphi \in C^1(G) \) with \( \partial \varphi = -\chi_a \cup \chi_b \) in \( C^2(G) \) and \( \omega = \text{Res}_{N_b} \varphi \) in \( C^1(N_b) \).

**Proof.** Let \( \bar{\chi}_a, \bar{\chi}_b \in Z^1(\bar{G}) \) be the characters with inflations \( \chi_a, \chi_b \), respectively, to \( G \). Every element of \( \bar{G} \) can be uniquely written as \( \bar{\sigma}_d \bar{\sigma}_a \bar{\tau}^k \) for integers \( 0 \leq i, j, k < p \) (which we also consider as elements of \( \mathbb{Z}/p \)). We define \( \bar{\varphi} \in C^1(\bar{G}) \) by \( \varphi(\bar{\sigma}) = \omega(\sigma_a)j + k \). Let \( \varphi \in C^1(G) \) be the inflation of \( \bar{\varphi} \) to \( G \).

To compute \( \partial \varphi \), we take \( 0 \leq i, j, k, r, s, t < p \). Then \( \bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^k = \bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^{jr} \), so

\[ \bar{\varphi}(\bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^k) = \bar{\varphi}(\bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^{jr}) = \omega(\sigma_a)(j + k + r) \]

Therefore

\[ (\partial \varphi)(\bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^k, \bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^t) = \bar{\varphi}(\bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^k) + \bar{\varphi}(\bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^t) - \bar{\varphi}(\bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^k \bar{\sigma}_d^i \bar{\sigma}_a^j \bar{\tau}^t) \]

\[ = \omega(\sigma_a)(j + k + r) \]

The first equality of the Proposition now follows by inflation to \( G \).

For the second equality, let \( \sigma \in N_b \) and let \( \bar{\sigma} \) be the image of \( \sigma \) in \( N_b/(N_a \cap \text{Ker}(\omega)) \). We may write \( \bar{\sigma} = \bar{\sigma}_d^j \bar{\tau}^k \) for some integers \( 0 \leq j, k < p \). Since \( \omega(\tau) = 1 \) (Proposition 3.1(a)) we have

\[ \omega(\sigma) = \omega(\sigma_d^j \bar{\tau}^k) = \omega(\sigma_a)j + k = \varphi(\sigma). \] \( \square \)
4. Massey products containing 0

Let \( \chi_1, \chi_2, \chi_3 \in H^1(G) \), and set \( N_1 = \ker(\chi_1), N_3 = \ker(\chi_3) \) and \( M = N_1 \cap N_3 \). Also let \( \omega \in H^1(N_3) \). We assume that
\[
\omega - \sigma_3 \omega = \text{Res}_{N_3} \chi_2, \quad \chi_1 \cup \chi_2 = 0,
\]
and \( \chi_2, \chi_3 \) are \( \mathbb{F}_p \)-linearly independent.

**Lemma 4.1.** The triple Massey product \( \langle \chi_1, \chi_2, \chi_3 \rangle \) has a representative \( \alpha \) such that \( \text{Res}_{N_3} \alpha = -\text{Res}_{N_3}(\chi_1) \cup \omega \).

**Proof.** Since \( \chi_1 \cup \chi_2 = 0 \) in \( H^2(G) \) there exists \( \varphi_{12} \in C^2(G) \) such that \( \partial \varphi_{12} = \chi_1 \cup \chi_2 \) in \( C^2(G) \). Proposition 3.2 and (4.1) give rise to \( \varphi_{23} \in C^1(G) \) with \( \partial \varphi_{23} = -\chi_2 \cup \chi_3 \) and \( \omega = \text{Res}_{N_3} \varphi_{23} \). Then \( \chi_1 \cup (\varphi_{23}) + \varphi_{12} \cup \chi_3 \) is a 2-cocycle with cohomology class \( \alpha \) in \( \langle \chi_1, \chi_2, \chi_3 \rangle \). We have
\[
\text{Res}_{N_3} \chi_1 \cup (\varphi_{23}) + \varphi_{12} \cup \chi_3 = -\text{Res}_{N_3} \chi_1 \cup \omega,
\]
in \( C^2(N_3) \), whence \( \text{Res}_{N_3} \alpha = -\text{Res}_{N_3}(\chi_1) \cup \omega \) in \( H^2(N_3) \). \( \square \)

**Theorem 4.2.** In the above setup (4.1), assume further that the sequence (2.1) is exact for every open subgroup \( U \) of \( G \) of index dividing \( p \). Then the following conditions are equivalent:

1. \( 0 \in \langle \chi_1, \chi_2, \chi_3 \rangle \);
2. There exists \( \lambda \in H^1(G) \) such that \( \text{Res}_{N_3}(\chi_1 \cup \lambda) = \text{Res}_{N_3}(\chi_1) \cup \omega \);
3. \( \omega \in \text{Res}_{N_3} H^1(G) + \text{Cor}_{N_3} H^1(M) \).

**Proof.** (1)\( \Rightarrow \) (2): Lemma 4.1 yields \( \alpha \in \langle \chi_1, \chi_2, \chi_3 \rangle \) with \( \text{Res}_{N_3} \alpha = -\text{Res}_{N_3}(\chi_1) \cup \omega \). Since also \( 0 \in \langle \chi_1, \chi_2, \chi_3 \rangle \), Proposition 1.1(b) gives \( \lambda, \lambda' \in H^1(G) \) such that \( -\alpha = \chi_1 \cup \lambda + \chi_3 \cup \lambda' \). Now this implies that \( \text{Res}_{N_3} \alpha = -\text{Res}_{N_3}(\chi_1 \cup \lambda) \), whence (2).

(2)\( \Rightarrow \) (1): For \( \alpha \) as in Lemma 4.1, \( \text{Res}_{N_3}(\alpha + \chi_1 \cup \lambda) = 0 \). By the exact sequence (2.1), \( \alpha + \chi_1 \cup \lambda \in \chi_3 \cup H^1(G) \), whence (1).

(2)\( \Leftrightarrow \) (3): This follows again from (2.1). \( \square \)

5. Kummer formations

Let \( A \) be a discrete \( G \)-module. For a closed normal subgroup \( U \) of \( G \) let \( A^U \) be the submodule of \( G \) fixed by \( U \). There is an induced \( G/U \)-action on \( A^U \).

For every open normal subgroups \( U \leq U' \) of \( G \) let \( N_{U'/U} : A^U \to A^{U'} \) be the trace map \( \alpha \mapsto \sum \sigma a \), where \( \sigma \) ranges over a system of representatives for the cosets of \( U' \) modulo \( U \).
Let $I_{U'/U}$ be the subgroup of $A^U$ consisting of all elements of the form $\bar{\sigma}a - a$ with $\bar{\sigma} \in U'/U$ and $a \in A$. We recall that
\[
\hat{H}^{-1}(U'/U, A^U) = \text{Ker}(N_{U'/U})/I_{U'/U}.
\]
When $U'/U$ is cyclic with generator $\bar{\sigma}$, the subgroup $I_{U'/U}$ consists of all elements $\bar{\sigma}a - a$, with $a \in A$ (since $\bar{\sigma}^k - 1 = (\bar{\sigma} - 1)\sum_{i=0}^{k-1} \bar{\sigma}^i$). Then $\hat{H}^{-1}(U'/U, A^U) \cong H^1(U'/U, A^U)$ [NSW08, Prop. 1.7.1].

**Definition 5.1.** A $p$-Kummer formation $(G, A, \{\kappa_U\}_U)$ consists of a profinite group $G$, a discrete $G$-module $A$, and for each open normal subgroup $U$ of $G$ a $G$-equivariant epimorphism $\kappa_U: A^U \to H^1(U)$ such that for every open normal subgroup $U$ of $G$ the following conditions hold:

(i) the sequence (2.1) is exact for every $\chi \in H^1(U)$;
(ii) $\text{Ker}(\kappa_U) = pA^U$;
(iii) for every open normal subgroup $U'$ of $G$ such that $U \leq U'$, there are commutative squares
\[
\begin{array}{ccc}
A^U & \xrightarrow{\kappa_U} & H^1(U) \\
\downarrow \text{Res}_U & & \downarrow \text{Res}_U \\
A^{U'} & \xrightarrow{\kappa_{U'}} & H^1(U');
\end{array}
\quad
\begin{array}{ccc}
A^U & \xrightarrow{\kappa_U} & H^1(U) \\
\downarrow N_{U'/U} & & \downarrow \text{Cor}_{U'} \\
A^{U'} & \xrightarrow{\kappa_{U'}} & H^1(U');
\end{array}
\]

(iv) for every open normal subgroup $U'$ of $G$ such that $U \leq U'$ and $(U'/U) = p$ one has $\hat{H}^{-1}(U'/U, A^U) = 0$.

**Example 5.2.** Let $F$ be a field which contains a root of unity of order $p$. We fix an isomorphism between the group $\mu_p$ of $p$th roots of unity and $\mathbb{Z}/p$. Given an open subgroup $U$ of $G_F$ let $E = F_{\text{sep}}^U$ be its fixed field. The Kummer homomorphism $\kappa_U: E^\times \to H^1(U)$ is the connecting homomorphism arising from the short exact sequence of $U$-modules
\[
0 \to \mathbb{Z}/p \to F_{\text{sep}}^\times \xrightarrow{\rho_p} F_{\text{sep}}^\times \to 1.
\]
By Hilbert’s Theorem 90 it is surjective. Then $(G_F, F_{\text{sep}}^\times, \{\kappa_U\}_U)$ is a $p$-Kummer formation. Indeed, (i) was pointed out in Example 2.2. (ii) is the standard fact that $\text{Ker}(\kappa_U) = (E^\times)^p$, and (iii) follows from the commutativity of connecting homomorphisms with restrictions and corestrictions. For (iv) use the isomorphism $\hat{H}^{-1}(U'/U, A^U) = H^1(U'/U, A^U)$ for $U'/U$ cyclic and Hilbert’s Theorem 90.

**Proposition 5.3.** Let $(G, A, \{\kappa_U\}_U)$ be a $p$-Kummer formation. Let $M_1, M_3$ be distinct normal subgroups of $G$ of index $p$, let $M = M_1 \cap M_3$, and let $\sigma_3 \in
$M_1$ satisfy $G = \langle M_1, \sigma_3 \rangle$. Suppose that $\lambda_1 \in H^1(M_1)$ and $\lambda_3 \in H^1(M_3)$ satisfy $\text{Cor}_G \lambda_1 = \text{Cor}_G \lambda_3$. Then there exists $\omega \in H^1(M_3)$ such that

$$\sigma_3 \omega - \omega = -\text{Res}_{M_3} \text{Cor}_G \lambda_3, \quad \omega \in \text{Res}_{M_3} H^1(G) + \text{Cor}_{M_3} H^1(M).$$

**Proof.** There exist $y_1 \in A^{M_1}$ and $y_3 \in A^{M_3}$ such that $\kappa_{M_1}(y_1) = \lambda_1$ and $\kappa_{M_3}(y_3) = \lambda_3$. Let $w = \sum_{i=0}^{p-1} \sigma_3^i y_3$, and note that $w \in A^{M_3}$. Since $\sigma_3$ has order $p$, we have $(\sigma_3 - 1) \sum_{i=0}^{p-1} \sigma_3^i = p1 - \sum_{i=0}^{p-1} \sigma_3^i$ in $\mathbb{Z}[G]$. Hence

$$(\sigma_3 - 1)w = (p1 - N_{G/M_3})y_3 = p(y_3 - N_{G/M_3}y_3).$$

Setting $\omega = \kappa_{M_3}(w) \in H^1(M_3)$, the $G$-equivariance of $\kappa_{M_3}$ and assumption (iii) imply that

$$\sigma_3 \omega - \omega = \kappa_{M_3}((\sigma_3 - 1)w) = -\kappa_{M_3}(N_{G/M_3}y_3) = -\text{Res}_{M_3} \kappa_G(N_{G/M_3}y_3)$$

$$= -\text{Res}_{M_3} \text{Cor}_G \kappa_{M_3}(y_3) = -\text{Res}_{M_3} \text{Cor}_G \lambda_3.$$

By (iii),

$$\kappa_G(N_{G/M_1}y_1 - N_{G/M_3}y_3) = \text{Cor}_G \kappa_{M_1}(y_1) - \text{Cor}_G \kappa_{M_3}(y_3)$$

$$= \text{Cor}_G \lambda_1 - \text{Cor}_G \lambda_3 = 0.$$

From (ii) we obtain $b \in A^G$ such that $N_{G/M_1}y_1 - N_{G/M_3}y_3 = pb$.

Next we choose $\sigma_1 \in M_3$ such that $G = \langle M_1, \sigma_1 \rangle$, and denote $M' = \langle M, \sigma_1 \sigma_3 \rangle$. We note that $\sigma_1, \sigma_3$ commute modulo $M$, so $N_{M'/M} = \sum_{i=0}^{p-1} \sigma_1^i \sigma_3^i$ on $A^M$. Therefore $N_{M'/M} = N_{G/M_3}$ on $A^{M_3}$, and $N_{M'/M} = N_{G/M_1}$ on $A^{M_1}$. We obtain that

$$N_{M'/M}(y_3 - y_1 + b) = N_{G/M_3}y_3 - N_{G/M_1}y_1 + pb = 0.$$

By (iv), $\hat{H}^{-1}(M'/M, A^M) = 0$, so $y_3 - y_1 + b = (\sigma_1 \sigma_3 - 1)t$ for some $t \in A^M$. Therefore

$$(\sigma_3 - 1)w = p(y_3 - N_{G/M_3}y_3) = N_{M_3/M}y_3 - N_{G/M_1}y_1 + pb$$

$$= N_{M_3/M}y_3 - N_{M_3/M}y_1 + pb = N_{M_3/M}(y_3 - y_1 + b)$$

$$= N_{M_3/M}(\sigma_1 \sigma_3 - 1)t = \sigma_3 \sigma_1 N_{M_3/M}t - N_{M_3/M}t = (\sigma_3 - 1)N_{M_3/M}t,$$

since $\sigma_1 N_{M'/M} = N_{M'/M}$ on $A^M$. Thus $w - N_{M_3/M}t \in A^{(M_5, \sigma_3)} = A^G$.

Taking $\eta = \kappa_M(t) \in H^1(M)$, we obtain using (iii) that

$$\omega - \text{Cor}_{M_3} \eta = \kappa_{M_3}(w - N_{M_3/M}t) = \text{Res}_{M_3} \kappa_G(w - N_{M_3/M}t) \in \text{Res}_{M_3} H^1(G).$$

Consequently, $\omega \in \text{Res}_{M_3} H^1(G) + \text{Cor}_{M_3} H^1(M)$. \qed

**Theorem 5.4.** Let $(G, A, \{\kappa_v\}_{v})$ be a $p$-Kummer formation and let $\chi_1, \chi_2, \chi_3 \in H^1(G)$. Then the Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is not essential.
Proof. We assume that $\langle \chi_1, \chi_2, \chi_3 \rangle$ is non-empty. By Proposition 1.1(a), $\chi_1 \cup \chi_2 = 0 = \chi_2 \cup \chi_3$. By Proposition 2.5, we may assume that the pairs $\chi_1, \chi_3$ and $\chi_2, \chi_3$ are $\mathbb{F}_p$-linearly independent.

Let $M_1 = \text{Ker}(\chi_1)$, $M_3 = \text{Ker}(\chi_3)$, and $M = M_1 \cap M_3$, and choose $\sigma_3 \in M_1$ such that $G = \langle M_3, \sigma_3 \rangle$. The exact sequence (2.1) yields $\lambda_1 \in H^1(M_1)$ and $\lambda_3 \in H^1(M_3)$ such that $\text{Cor}_G \lambda_1 = \chi_2 = \text{Cor}_G \lambda_3$.

Proposition 5.3 gives rise to $\omega \in H^1(M_3)$ such that $\sigma_3 \omega - \omega = -\text{Res}_{M_3} \chi_2$ and $\omega \in \text{Res}_{M_3} H^1(G) + \text{Cor}_{M_3} H^1(M)$. By Theorem 4.2, $0 \in \langle \chi_1, \chi_2, \chi_3 \rangle$. □

Theorem 5.4 and Example 5.2 imply the Main Theorem.

References


TRIPLE MASSEY PRODUCTS AND ABSOLUTE GALOIS GROUPS


DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, BE’ER-SHEVA 84105, ISRAEL

E-mail address: efrat@math.bgu.ac.il, elimatzri@gmail.com