Canad. Math. Bull. Vol. 58 (4), 2015 pp. 730–740
http://dx.doi.org/10.4153/CMB-2015-026-5

Vanishing of Massey Products and Brauer Groups

Ido Efrat and Eliyahu Matzri

Abstract. Let p be a prime number and F a field containing a root of unity of order p. We relate recent results on vanishing of triple Massey products in the mod-p Galois cohomology of F, due to Hopkins, Wickelgren, Mináč, and Tân, to classical results in the theory of central simple algebras. We prove a stronger form of the vanishing property for global fields.

1 Introduction

We fix a prime number p. Let F be a field, which will always be assumed to contain a root of unity of order p. Let G_F be the absolute Galois group of F. Recent works by Hopkins, Wickelgren, Mináč, and Tân revealed a remarkable new property of the mod-p Galois cohomology groups $H^i(G_F, \mathbb{Z}/p)$, $i = 1, 2$, related to triple Massey products. This property, which they proved in several important cases, puts new restrictions on the possible group-theoretic structure of maximal pro-p Galois groups of fields, and in particular, of absolute Galois groups. For instance, Mináč and Tân [16] use this method to give new examples of pro-2 groups that cannot occur as absolute Galois groups of fields.

More specifically, for an arbitrary profinite group G that acts trivially on $\mathbb{Z}/p$, let $H^i(G) = H^i(G, \mathbb{Z}/p)$. We recall that the triple Massey product is a multi-valued map $\langle \cdot, \cdot, \cdot \rangle : H^1(G)^3 \to H^2(G)$ (see §6 for its precise definition). We consider the following cohomological condition:

> If $\chi_1, \chi_2, \chi_3 \in H^1(G)$ and $\langle \chi_1, \chi_2, \chi_3 \rangle \subseteq H^2(G)$ is nonempty, then it contains zero.

Following Mináč and Tân, we call this condition the *vanishing triple Massey product property* for G.

When $G = G_F$ for a field F as above, this property can be rephrased in more basic Galois-theoretic language, in terms of the groups $\mathbb{U}_n(\mathbb{F}_p)$ of unipotent upper triangular $n \times n$ matrices over $\mathbb{F}_p$. Namely, χ_1, χ_2, χ_3 are the Kummer characters corresponding the elements a_1, a_2, a_3 of $F^\times$, which we assume for simplicity to be $\mathbb{F}_p$-linearly independent in $F^\times/(F^\times)^p$. Then the following hold (see Corollary 6.4):

Received by the editors November 16, 2014; revised March 3, 2015.
Published electronically May 21, 2015.
The authors were supported by the Israel Science Foundation (grant No. 152/13). The second author was also partially supported by the Kreitman foundation.
AMS subject classification: **16K50**, 11R34, 12G05, 12E30.
Keywords: Galois cohomology, Brauer groups, triple Massey products, global fields.

- $\langle \chi_1, \chi_2, \chi_3 \rangle \neq \varnothing$ if and only if each of $F(a_1^{1/p}, a_2^{1/p})$ and $F(a_2^{1/p}, a_3^{1/p})$ embeds into a Galois extension of F with Galois group $\mathbb{U}_3(\mathbb{F}_p)$;
- $0 \in \langle \chi_1, \chi_2, \chi_3 \rangle$ if and only if $F(a_1^{1/p}, a_2^{1/p}, a_3^{1/p})$ embeds into a Galois extension of F with Galois group $\mathbb{U}_4(\mathbb{F}_p)$.

The vanishing triple Massey product condition was shown to hold for $G = G_F$ in the following situations:

(a) $p = 2$ and F is a global field [10];
(b) $p = 2$ and F is arbitrary [16];
(c) p is arbitrary and F is a global field [17].

Moreover, Mináč and Tân conjecture that G_F satisfies the vanishing triple Massey product property for every field F containing a root of unity of order p [18]. If true, this would give new kinds of examples of pro-p groups that are not realizable as absolute Galois groups for arbitrary primes p, along the lines of [16] (where this is done for $p = 2$). In view of the interpretations of triple Massey products in terms of $\mathbb{U}_3(\mathbb{F}_p)$- and $\mathbb{U}_4(\mathbb{F}_p)$-Galois extension, one also obtains an "automatic realization" principle in the above cases, and conjecturally always.

In this note we relate these recent developments to classical results in the theory of central simple algebras and Brauer groups. We investigate another cohomological property of G, which we call the *cup product-restriction property* for characters $\chi_1, \ldots, \chi_r \in H^1(G)$. This property for $r = 2$ implies the vanishing triple Massey product property, but unlike the latter property, it does not involve external cohomological operations. Now, when $G = G_F$, we prove this cup product-restriction property for global fields and arbitrary r, using the Albert–Brauer–Hasse–Noether theorem and an injectivity theorem for H^1 due to Artin and Tate. In the case where $p = 2$ and $r = 2$ the cup product-restriction property for G_F was proved by Tignol [24, Cor. 2.8] and is an easy consequence of a refinement, also due to Tignol [23, Th. 1], of a result of Albert on the decomposition of central simple algebras as a tensor product of two quaternion algebras.

Specifically, let G be an arbitrary profinite group, let $\chi_1, \ldots, \chi_r \in H^1(G) = \mathrm{Hom}(G, \mathbb{Z}/p)$, and set $K = \bigcap_{i=1}^r \mathrm{Ker}(\chi_i)$. We define a multi-linear map $\Lambda_{(\chi_i)}: H^1(G)^r \to H^2(G)$ by $\Lambda_{(\chi_i)}(\phi_1, \ldots, \phi_r) = \sum_{i=1}^r \chi_i \cup \phi_i$. It lifts to a homomorphism $\Lambda_{(\chi_i)}: H^1(G)^{\otimes r} \to H^2(G)$. We say that the *cup product-restriction property* holds for $\chi_1, \ldots, \chi_r$ if the sequence

$$H^1(G)^{\otimes r} \xrightarrow{\Lambda_{(\chi_i)}} H^2(G) \xrightarrow{\mathrm{res}_K} H^2(K) \tag{1.1}$$

is exact. Note that (1.1) is always a complex. Further, its exactness depends only on K (but not on the choice of $\chi_1, \ldots, \chi_r$; see Proposition 3.1).

Now when $\chi_1, \chi_2, \chi_3 \in H^1(G)$, the cup product-restriction property for $\chi_1, \chi_3 \in H^1(G)$ implies the vanishing triple Massey product property for $\langle \chi_1, \chi_2, \chi_3 \rangle$ (Proposition 6.2).

Theorem 1.1 (Main Theorem) *Let $a_1, \ldots, a_r \in F^\times$. Suppose that one of the following conditions holds:*

(i) *F is a global field;*

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

(ii) $p = 2$ *and* $r = 2$.

Then the cup product-restriction property holds for the Kummer elements $(a_1), \dots, (a_r)$ *in* $H^1(F)$.

In particular, by restricting to $r = 2$, this gives alternative algebra-theoretic proofs of the results of Hopkins, Wickelgren, Mináč, and Tân on the vanishing of triple Massey products, and relates these works to the above-mentioned classical results on Brauer groups. As remarked above, case (ii) was earlier proved in [24, Cor. 2.8] and is brought here in order to relate the respective results on Massey products to their algebra-theoretic counterparts (see §5). The cup product-restriction property for $G = G_F$ is also closely related to the subgroup $\mathrm{Dec}(L/F)$ of ${}_p\mathrm{Br}(F)$, introduced in [24, 25], where L is the fixed field of K in the separable closure of F.

In the case where $p = 2$ the cup product-restriction property for absolute Galois groups of fields is essentially the property P_2 studied in [8, 24]. In particular, in this situation, case (i) of Theorem 1.1 was earlier proved in [8, Cor. 3.18].

On the other hand, constructions of Tignol [26] and McKinnie [15] show that, for p odd, there exist fields F for which the cup product-restriction property with $r = 2$ does not hold (Example 3.4). This shows that some assumptions on F, as in Theorem 1.1, are needed.

2 Preliminaries in Galois Cohomology

Let F be again a field containing a root of unity of order p. We abbreviate $H^i(F) = H^i(G_F, \mathbb{Z}/p)$. We fix an isomorphism between the group μ_p of the p-th roots of unity and $\mathbb{Z}/p$. This isomorphism induces the Kummer isomorphism $H^1(F) \cong F^\times/(F^\times)^p$. Given $a \in F^\times$, let $(a) \in H^1(F)$ be the corresponding Kummer element.

Let $\mathrm{Br}(F)$ be the Brauer group of F and let ${}_p\mathrm{Br}(F)$ be its subgroup consisting of all elements with exponent dividing p. Given a field extension L/F we write $\mathrm{Br}(L/F)$ for the kernel of the restriction map $\mathrm{Br}(F) \to \mathrm{Br}(L)$. The isomorphism $\mu_p \cong \mathbb{Z}/p$ also induces in a standard way an isomorphism $H^2(F) \cong {}_p\mathrm{Br}(F)$. For $a, b \in F^\times$, let $(a, b)_F$ be the corresponding symbol F-algebra of degree p. The cup product $(a) \cup (b)$ in $H^2(F)$ then corresponds to the similarity class $[(a, b)_F]$ in ${}_p\mathrm{Br}(F)$.

3 The Cup Product-Restriction Property

We first show that the cup product-restriction property depends only on the subgroup $K = \bigcap_{i=1}^r \mathrm{Ker}(\chi_i)$, but not on the choice of $\chi_1, \dots, \chi_r$.

Proposition 3.1 *Let G be a profinite group and let K be an open subgroup of G. Consider $\chi_1, \dots, \chi_r, \mu_1, \dots, \mu_s \in H^1(G)$ such that $K = \bigcap_{i=1}^r \mathrm{Ker}(\chi_i) = \bigcap_{j=1}^s \mathrm{Ker}(\mu_j)$. Then the cup product-restriction property holds for $\chi_1, \dots, \chi_r$ if and only if it holds for $\mu_1, \dots, \mu_s$.*

Proof There is a perfect pairing

$$G/G^p[G, G] \times H^1(G) \to \mathbb{Z}/p, \quad (\bar{g}, \phi) \mapsto \phi(g)$$

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

[7, Cor. 2.2]. It induces a perfect pairing $G/K \times \langle \chi_1, \dots, \chi_r \rangle \to \mathbb{Z}/p$, and similarly for the μ_j. Therefore, $\langle \chi_1, \dots, \chi_r \rangle = \langle \mu_1, \dots, \mu_s \rangle$. It follows that

$$\chi_1 \cup H^1(G) + \cdots + \chi_r \cup H^1(G) = \mu_1 \cup H^1(G) + \cdots + \mu_s \cup H^1(G);$$

i.e., the homomorphisms

$$\Lambda_{(\chi_i)} : H^1(G)^{\otimes r} \to H^2(G), \quad \Lambda_{(\mu_j)} : H^1(G)^{\otimes s} \to H^2(G)$$

have the same image, and the assertion follows. ∎

Consequently, for every open subgroup K of G such that G/K is an elementary abelian p-group, we may define the *cup product-restriction property for K* to be the cup product-restriction property for $\chi_1, \dots, \chi_r$, where $\chi_1, \dots, \chi_r$ is any list of elements in $H^1(G)$ such that $K = \bigcap_{i=1}^{r} \mathrm{Ker}(\chi_i)$.

Example 3.2 Let $\chi = \chi_1 \in H^1(G)$, so $K = \mathrm{Ker}(\chi)$. The cup product-restriction property for χ means that the sequence

$$H^1(G) \xrightarrow{\chi\cup} H^2(G) \xrightarrow{\mathrm{res}} H^2(K) \tag{3.1}$$

is exact. This is trivial when $\chi = 0$, so we assume that $\chi \neq 0$, and therefore $(G:K) = p$.

When $p = 2$ (3.1) is always exact and is in fact a segment of the infinite Arason exact sequence [2, Satz 4.5]:

$$\cdots \xrightarrow{\mathrm{res}} H^i(K) \xrightarrow{\mathrm{cor}} H^i(G) \xrightarrow{\chi\cup} H^{i+1}(G) \xrightarrow{\mathrm{res}} H^{i+1}(K) \xrightarrow{\mathrm{cor}} \cdots .$$

When p is an arbitrary prime and F is a field (containing as always a fixed root of unity of order p), we may write $\chi = (a)$ for some $a \in F^\times$. Then $L = F(a^{1/p})$ is the $\mathbb{Z}/p$-Galois extension corresponding to K. There is an isomorphism

$$F^\times / N_{L/F} L^\times \xrightarrow{\sim} \mathrm{Br}(L/F), \quad x N_{L/F} L^\times \mapsto [(a,x)_F]$$

[4, p. 73, Th. 1]. It follows that (3.1) is exact; *i.e.,* the cup product-restriction property for χ holds. This is again a part of a more general fact: Based on results of Voevodsky [27, §5], it was shown by Lemire, Mináč, and Swallow [12, Thm. 6] that for every $i \geq 1$ the following sequence is exact:

$$H^i(L) \xrightarrow{\mathrm{cor}} H^i(F) \xrightarrow{\chi\cup} H^{i+1}(F) \xrightarrow{\mathrm{res}} H^{i+1}(L).$$

Remark 3.3 Suppose that F is a field containing a root of unity of order p, and L is a Galois extension of F with $\mathrm{Gal}(L/F)$ an elementary abelian p-group. As in [24, 25] let $\mathrm{Dec}(L/F)$ be the subgroup of $\mathrm{Br}(L/F)$ generated by all subgroups $\mathrm{Br}(L'/F)$, where L' ranges over all cyclic p-extensions of F contained in L. Then the cup product-restriction property holds for the subgroup G_L of G_F if and only if $\mathrm{Dec}(L/F) = {}_p\,\mathrm{Br}(L/F)$.

Example 3.4 For p odd there are constructions due to McKinnie [15] and Tignol [26, Th. 1, Rem. 1.3(a)] (see also [19, 21] for related works), of division algebras D over a field F which contains a root of unity of order p, such that

(i) D splits in $L = F(a_1^{1/p}, a_2^{1/p})$ for certain $a_1, a_2 \in F^\times$;
(ii) $[D] \notin \mathrm{Dec}(L/F)$.

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

In view of Remark 3.3, this means that the cup product-restriction property does not hold for the subgroup $K = G_L$ of $G = G_F$.

4 Global Fields

Throughout this section we assume that F is a global field containing a root of unity of order p. For every place v on F we write F_v for the completion of F relative to v, and denote the canonical extension of v to F_v also by v. There is a canonical monomorphism $\mathrm{inv}_v\colon \mathrm{Br}(F_v) \to \mathbb{Q}/\mathbb{Z}$ that is an isomorphism for v non-archimedean. Restricting to ${}_p\,\mathrm{Br}(F)$, we obtain a monomorphism $\mathrm{inv}_v\colon H^2(F_v) \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$. It is an isomorphism unless v is archimedean and $p \neq 2$ (and in the latter case $H^2(F_v) = 0$). Given a finite extension E of F_v, there is a commutative square

$$\begin{array}{ccc} \mathrm{Br}(E) & \xrightarrow{\mathrm{inv}_u} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{res}_E}\uparrow & & \uparrow{\scriptstyle [E:F_v]} \\ \mathrm{Br}(F_v) & \xrightarrow{\mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

where the map on the right means multiplication by the degree $[E:F_v]$ [22, Ch. XIII, §3, Prop. 7]. Consequently, if $p|[E:F_v]$, then $\mathrm{res}_E\colon H^2(F_v) \to H^2(E)$ is the zero map.

We recall that, by classical results of Albert, Brauer, Hasse and Noether, the following sequence is exact:

$$0 \to \mathrm{Br}(F) \xrightarrow{\mathrm{res}} \bigoplus_v \mathrm{Br}(F_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

It gives rise to an exact sequence

$$0 \to H^2(F) \xrightarrow{\mathrm{res}} \bigoplus_v H^2(F_v) \xrightarrow{\sum_v \mathrm{inv}_v} \tfrac{1}{p}\mathbb{Z}/\mathbb{Z}. \tag{4.1}$$

Lemma 4.1 *Let S be a finite set of places on F and let $a_1, \dots, a_r \in F^\times$. Suppose that $a_1 \notin (F^\times)^p$. Then there exists a place v_0 on F such that $v_0 \notin S$ and $a_1, a_2', \dots, a_r' \notin (F_{v_0}^\times)^p$, where for each $2 \le i \le r$, either $a_i' = a_i$ or $a_i' = a_1 a_i$.*

Proof The restriction map $H^1(F) \to \prod_{v \notin S} H^1(F_v)$ is injective [3, Ch. IX, Th. 1]. Hence there is a place $v_0 \notin S$ with $(a_1) \neq 0 \in H^1(F_{v_0})$. Then for every i with $2 \le i \le r$ we have $(a_i) \neq 0 \in H^1(F_{v_0})$ or $(a_1 a_i) = (a_1) + (a_i) \neq 0 \in H^1(F_{v_0})$, and we can choose a_i' accordingly. ∎

Proof of Case (i) of Theorem 1.1 Let $a_1, \dots, a_r \in F^\times$. If $a_1, \dots, a_r \in (F^\times)^p$, then the cup product-restriction property for $(a_1), \dots, (a_r) \in H^1(F)$ is trivial. We may therefore assume that $a_1 \notin (F^\times)^p$. Let $L = F(a_1^{1/p}, \dots, a_r^{1/p})$, and consider $\alpha \in H^2(F)$ with $\mathrm{res}_L(\alpha) = 0$ in $H^2(L)$. We have to show that $\alpha \in (a_1) \cup H^1(F) + \cdots + (a_r) \cup H^1(F)$.

To this end, let S be the set of all places v on F such that $\alpha_{F_v} \neq 0$, where α_{F_v} denotes the restriction of α to $H^2(F_v)$. By (4.1), S is finite. Let v_0 and $a_2', \dots, a_r'$ be as in Lemma

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

4.1. In particular, $\alpha_{F_{v_0}} = 0$. Now $L = F(a_1^{1/p}, (a_2')^{1/p}, \dots, (a_r')^{1/p})$ and

$$(a_1) \cup H^1(F) + (a_2) \cup H^1(F) + \cdots + (a_r) \cup H^1(F) = (a_1) \cup H^1(F) + (a_2') \cup H^1(F) + \cdots + (a_r') \cup H^1(F).$$

We may therefore replace a_i by a_i', $i = 2, \dots, r$, to assume without loss of generality that $a_1, \dots, a_r \notin (F_{v_0}^\times)^p$.

Next for $1 \le i \le r$ let $S_i = \{v \mid a_i^{1/p} \notin F_v\}$. Thus, $v_0 \in (S_1 \cap \cdots \cap S_r) \smallsetminus S$.

If $v \in S$, then $L \not\subseteq F_v$, so $a_i^{1/p} \notin F_v$ for some $1 \le i \le r$. This shows that $S \subseteq S_1 \cup \cdots \cup S_r$. Hence we may decompose $S = S_1' \dot\cup \cdots \dot\cup S_r'$ with $S_i' \subseteq S_i$, $i = 1, 2, \dots, r$. Note that $v_0 \notin S_i'$ for every i.

For every i, let

$$t_i := \sum_{v \in S_i'} \operatorname{inv}_v(\alpha_{F_v}).$$

Then (4.1) gives rise to $\alpha_i \in H^2(F)$ with local invariants

$$\operatorname{inv}_v((\alpha_i)_{F_v}) = \begin{cases} \operatorname{inv}_v(\alpha_{F_v}), & \text{if } v \in S_i', \\ -t_i, & \text{if } v = v_0, \\ 0, & \text{otherwise.} \end{cases}$$

Claim 1: For every place w on F,

$$\operatorname{inv}_w(\alpha_{F_w}) = \sum_{i=1}^{r} \operatorname{inv}_w((\alpha_i)_{F_w}). \tag{4.2}$$

Indeed, when $w \in S_i'$ for some i, this follows from the disjointness of $S_1', \dots, S_r'$. When $w = v_0$ we compute using (4.1),

$$\begin{aligned} \operatorname{inv}_w(\alpha_{F_w}) = 0 &= -\sum_v \operatorname{inv}_v(\alpha_{F_v}) = -\sum_{v \in S} \operatorname{inv}_v(\alpha_{F_v}) \\ &= -\sum_{i=1}^{r} \sum_{v \in S_i'} \operatorname{inv}_v(\alpha_{F_v}) = -\sum_{i=1}^{r} t_i = \sum_{i=1}^{r} \operatorname{inv}_w((\alpha_i)_{F_w}). \end{aligned}$$

For all other places, the left-hand side of (4.2) is zero, by the definition of S, and all summands on the right-hand side are zero by the choice of α_i. This proves the claim.

We conclude from Claim 1 and from (4.1) that $\alpha = \sum_{i=1}^r \alpha_i$ in $H^2(F)$.

Claim 2: For every $1 \le i \le r$ and every place u on $F(a_i^{1/p})$, one has

$$(\alpha_i)_{F(a_i^{1/p})_u} = 0.$$

To see this, let v be the place on F that lies under u.

Case 1: $v \in S_i$. Then $p = [F_v(a_i^{1/p}) : F_v] \mid [F(a_i^{1/p})_u : F_v]$, so as we have seen, $\operatorname{res}: H^2(F_v) \to H^2(F(a_i^{1/p})_u)$ is the zero map. In particular, $(\alpha_i)_{F(a_i^{1/p})_u} = 0$.

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

Case 2: $v \notin S_i$. Then $a_i^{1/p} \in F_v$ and $v \neq v_0$. Hence $F(a_i^{1/p})_u = F_v$. The choice of α_i implies that $\mathrm{inv}_v((\alpha_i)_{F_v}) = 0$, so again, $(\alpha_i)_{F(a_i^{1/p})_u} = (\alpha_i)_{F_v} = 0$.

We conclude from Claim 2 and from (4.1) that $(\alpha_i)_{F(a_i^{1/p})} = 0$, $i = 1, 2, \ldots, r$. Therefore $\alpha_i \in (a_i) \cup H^1(F)$ (Example 3.2). It follows that

$$\alpha = \sum_{i=1}^{r} \alpha_i \in (a_1) \cup H^1(F) + \cdots + (a_r) \cup H^1(F). \qquad \blacksquare$$

5 The Case $p = 2$

Let $p = 2$ and let F be a field of characteristic $\neq 2$. By a classical result of Albert [1], every central simple F-algebra of degree 4 and exponent 2 is F-isomorphic to a tensor product of two quaternion F-algebras. This was extended by Tignol [23, Th. 1] as follows. Recall that an involution on a central simple F-algebra is of the *first kind* if it is the identity on F.

Theorem 5.1 (Tignol) *Let A be a central simple F-algebra with involution of the first kind that is split by a Galois extension M of F with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$. Let L_1, L_2 be quadratic extensions of F with $M = L_1L_2$. Then there are quaternion F-algebras Q_1, Q_2 such that $L_i \subset Q_i \subset A$, $i = 1, 2$, and $A \cong_F Q_1 \otimes_F Q_2$.*

For a closely related result see [20, Cor. 5].

The case $p = 2$, $r = 2$ of the Theorem 1.1 is an easy corollary of Theorem 5.1. In a different terminology it was obtained by Tignol in [24, Cor. 2.8], however we provide a short proof showing its relation to Theorem 5.1.

Proof of Case (ii) of Theorem 1.1 Let $a_1, a_2 \in F^\times$ and denote $M = F(\sqrt{a_1}, \sqrt{a_2})$. Thus in the terminology of sequence (1.1), $K = G_M$. Since the sequence (1.1) is always a complex, we need to show that for every central simple F-algebra A of exponent 2 that splits in M the similarity class $[A]$ of A in ${}_2\mathrm{Br}(F)$ is contained in $(a_1) \cup H^1(G) + (a_2) \cup H^1(G)$. We may assume that A does not split in F. If a_1, a_2 have $\mathbb{F}_2$-linearly dependent cosets in $F^\times/(F^\times)^2$, then we are done by Example 3.2. So assume that a_1, a_2 have $\mathbb{F}_2$-linearly independent cosets in $F^\times/(F^\times)^2$.

Since A splits in M, it is similar to a central simple F-algebra A' of degree $[M:F] = 4$ that contains M [4, p. 64, Th. 7]. The exponent of A' is also 2, and therefore it has an involution of the first kind [1, Ch. X, Th. 19]. Let $L_i = F(\sqrt{a_i})$, $i = 1, 2$. Theorem 5.1 yields quaternion F-subalgebras Q_1, Q_2 of A' that contain L_1, L_2, respectively, and such that $A' \cong_F Q_1 \otimes_F Q_2$. Then $Q_1 \cong_F (a_1, x)_F$ and $Q_2 \cong_F (a_2, y)_F$ for some $x, y \in F^\times$ [4, p. 104, Th. 4]. Therefore, $[A] = [A'] = (a_1) \cup (x) + (a_2) \cup (y)$, as desired. $\blacksquare$

Remark 5.2 There are no known direct generalizations of Theorem 5.1 and [20, Cor. 5] for odd primes. For instance, when $p = 3$, it seems that the best result to date is that a central simple F-algebra that contains a maximal subfield L that is Galois over F with $\mathrm{Gal}(L/F) \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ (*i.e.*, A is a $\mathbb{Z}/3 \times \mathbb{Z}/3$-crossed product over F) is similar to the tensor product of ≤ 31 symbol algebras of degree 3 over F [13].

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

6 Massey Products

We recall the definition and basic properties of Massey products of degree 1 cohomology elements. For more information see, *e.g.,* Fenn [9], Kraines [11], Dwyer [5] (and in a more general setting, May [14]). Note that the various sources use different sign conventions.

We first recall that a *differential graded algebra* over a ring R (R-DGA) is a graded R-algebra $C^\bullet = \bigoplus_{s=0}^{\infty} C^s$ equipped with R-module homomorphisms $\partial^s : C^s \to C^{s+1}$ such that $(C^\bullet, \bigoplus_{s=0}^{\infty} \partial^s)$ is a complex satisfying the *Leibnitz rule* $\partial^{r+s}(ab) = \partial^r(a)b + (-1)^r a\partial^s(b)$ for $a \in C^r$, $b \in C^s$. Set $Z^r = \mathrm{Ker}(\partial^r)$, $B^r = \mathrm{Im}(\partial^{r-1})$, and $H^r = Z^r/B^r$, and let $[c]$ denote the class of $c \in Z^r$ in H^r.

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

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

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 c_{ii} is then a 1-cocycle, $i = 1, 2, \ldots, n$. Further, $\widetilde{c}_{1n}$ is a 2-cocycle ([11, p. 432], [9, p. 233]. Its cohomology class depends only on the cohomology classes $[c_{11}], \ldots, [c_{nn}]$ [11, 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 $[\widetilde{c_{1n}}]$ obtained from defining systems (c_{ij}) of size n on $c_1, \ldots, c_n$ in $C^\bullet$. This construction is functorial in the natural sense. When this subset is nonempty, one says that $\langle [c_1], \ldots, [c_n] \rangle$ is *defined*. Note that $\langle [c_1], \ldots, [c_n] \rangle$ contains 0 if and only if there is an array (c_{ij}), $1 \leq i \leq j \leq n$, in C^1 such that $\partial c_{ij} = \widetilde{c}_{ij}$ for every $1 \leq i \leq j \leq n$ (including $(i, j) = (1, n)$). In this case one says that the Massey product $\langle [c_1], \ldots, [c_n] \rangle$ is *trivial*.

When $n = 2$, $\langle [c_1], [c_2] \rangle$ is always defined and consists only of $-[c_1][c_2]$.

Next we record some well-known facts on the case $n = 3$.

Proposition 6.1 *Let $c_1, c_2, c_3 \in Z^1$.*

(i) $\langle [c_1], [c_2], [c_3] \rangle$ *is defined if and only if* $[c_1][c_2] = [c_2][c_3] = 0$.

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

Proof (i) Having a defining system on c_1, c_2, c_3 means that there exist $c_{12}, c_{23} \in C^1$ with $\partial c_{12} = -c_1c_2$ and $\partial c_{23} = -c_2c_3$, *i.e.,* $c_1c_2, c_2c_3 \in B^2$.

(ii) Suppose that (c'_{ij}) is another defining system on c_1, c_2, c_3. For $d_{12} = c'_{12} - c_{12}$ and $d_{23} = c_{23} - c'_{23}$ we have $\partial d_{12} = \widetilde{c'_{12}} - \widetilde{c_{12}} = -c_1c_2 + c_1c_2 = 0$. Thus $d_{12} \in Z^1$, and similarly $d_{23} \in Z^1$. By a direct calculation $[\widetilde{c'_{13}}] = [\widetilde{c_{13}}] + [c_1][d_{23}] + [c_3][d_{12}]$.

Conversely, for every $d_{12}, d_{23} \in Z^1$, the system (c'_{ij}) is also a defining system on c_1, c_2, c_3, where we take $c'_{ii} = c_i$, $c'_{12} = c_{12} - d_{12}$ and $c'_{23} = c_{23} + d_{23}$. One has $[\widetilde{c'_{13}}] = [\widetilde{c_{13}}] + [c_1][d_{23}] + [c_3][d_{12}]$. ∎

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

Now for the fixed prime number p, let G be a profinite group acting trivially on $\mathbb{Z}/p$. Let $C^\bullet = \bigoplus_{s=0}^{\infty} C^s(G, \mathbb{Z}/p)$ be the $\mathbb{Z}/p$-DGA of continuous cochains from G to $\mathbb{Z}/p$, with the cup product. Thus, in our previous notation, $H^i = H^i(G)$.

Proposition 6.2 *Let $\chi_1, \chi_2, \chi_3 \in H^1(G)$. Suppose that the triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined and that the cup product-restriction property holds for χ_1, χ_3. Then $0 \in \langle \chi_1, \chi_2, \chi_3 \rangle$.*

Proof Take $\alpha \in \langle \chi_1, \chi_2, \chi_3 \rangle$. Let $K = \mathrm{Ker}(\chi_1) \cap \mathrm{Ker}(\chi_3)$. The functoriality of the Massey product implies that

$$\mathrm{res}_K(\alpha) \in \langle \mathrm{res}_K(\chi_1), \mathrm{res}_K(\chi_2), \mathrm{res}_K(\chi_3) \rangle = \langle 0, \mathrm{res}_K(\chi_2), 0 \rangle = \{0\}.$$

By the exactness of (1.1), $\alpha \in \mathrm{Im}(\Lambda_{(\chi_1,\chi_3)})$; that is, $\alpha = \chi_1 \cup \beta_1 + \chi_3 \cup \beta_3$ for some $\beta_1, \beta_3 \in H^1(G)$. Now Proposition 6.1 implies that

$$0 = \alpha - \chi_1 \cup \beta_1 - \chi_3 \cup \beta_3 \in \langle \chi_1, \chi_2, \chi_3 \rangle. \qquad \blacksquare$$

Dwyer [5] relates n-fold Massey products in $C^\bullet(G, \mathbb{Z}/p)$ to unipotent upper triangular $n+1$-dimensional representations of G as follows ([5] works in a discrete context and with more a general coefficients ring; see [6, §8] for the profinite context, and [28] for a generalization to the case of non-trivial actions). For $n \geq 2$ let $\mathbb{U}_{n+1}(\mathbb{F}_p)$ be as before the group of all unipotent upper triangular $(n+1) \times (n+1)$-matrices over $\mathbb{F}_p$. Its center consists of all matrices which are 0 on all off-diagonal entries, except possibly for entry $(1, n+1)$. Let $\bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ be the quotient of $\mathbb{U}_{n+1}(\mathbb{F}_p)$ by this center. Its elements may be viewed as unipotent upper triangular $(n+1) \times (n+1)$-matrices with the $(1, n+1)$-entry deleted. We notice that $\mathbb{U}_{n+1}(\mathbb{F}_p)$ is a p-group, and its Frattini subgroup is the kernel of the epimorphism $\mathbb{U}_{n+1}(\mathbb{F}_p) \to (\mathbb{Z}/p)^n$, $(c_{ij}) \mapsto (c_{12}, c_{23}, \ldots, c_{n,n+1})$, and similarly for $\bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$.

Given an array (c_{ij}), $1 \leq i \leq j \leq n$, in $C^1(G, \mathbb{Z}/p)$, we define a continuous map $\gamma: G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ by $\gamma(\sigma)_{ij} = (-1)^{j-i} c_{i,j-1}(\sigma)$ for $\sigma \in G$ and for $1 \leq i < j \leq n+1$. Then $\widetilde{c_{ij}} = \partial c_{ij}$ for every $i < j$ if and only if $\gamma: G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ is a homomorphism. Similarly, $\widetilde{c_{ij}} = \partial c_{ij}$ for every $i < j$ with $(i, j) \neq (1, n)$ if and only if the induced map $\bar{\gamma}: G \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ is a homomorphism. We write $\gamma_{ij}, \bar{\gamma}_{ij}$ for the projections of $\gamma, \bar{\gamma}$, respectively, on the (i, j)-coordinate.

Proposition 6.3 *Let $\chi_1, \ldots, \chi_n \in H^1(G)$ be $\mathbb{F}_p$-linearly independent.*

(i) *$\langle \chi_1, \ldots, \chi_n \rangle$ is defined if and only if there exists a continuous homomorphism $\bar{\gamma}: G \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ such that $\bar{\gamma}_{i,i+1} = \chi_i$, $i = 1, 2, \ldots, n$.*

(ii) *$\langle \chi_1, \ldots, \chi_n \rangle$ is trivial if and only if there exists a continuous homomorphism $\gamma: G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ such that $\gamma_{i,i+1} = \chi_i$, $i = 1, 2, \ldots, n$.*

Moreover, such homomorphisms $\gamma, \bar{\gamma}$ are necessarily surjective.

Proof (i) and (ii) follow from the above discussion. The surjectivity of γ and $\bar{\gamma}$ follows by a Frattini argument. $\blacksquare$

This and Proposition 6.1(i) imply the following facts, mentioned in the Introduction, which are also implicit in [17, Cor. 3.2].

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press

Corollary 6.4 *Let $\chi_1, \chi_2, \chi_3 \in H^1(G)$ be $\mathbb{F}_p$-linearly independent. Then*

(i) *$\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined if and only if there exist continuous epimorphisms $\gamma', \gamma'' \colon G \to \mathbb{U}_3(\mathbb{F}_p)$ such that $\gamma'_{12} = \chi_1$, $\gamma'_{23} = \chi_2$, $\gamma''_{12} = \chi_2$, $\gamma''_{23} = \chi_3$;*

(i) *$\langle \chi_1, \chi_2, \chi_3 \rangle$ is trivial if and only if there exists a continuous epimorphism $\gamma \colon G \to \mathbb{U}_4(\mathbb{F}_p)$ such that $\gamma_{12} = \chi_1$, $\gamma_{23} = \chi_2$ and $\gamma_{34} = \chi_3$.*

Acknowledgments We thank the referees of this paper for very valuable comments and in particular for drawing our attention to several important references, which we included in the reference list.

References

[1] A. A. Adrian, *Structure of algebras*. American Mathematical Society Colloquium Publications, XXIV, American Mathematical Society, Providence, RI, 1939.
[2] J. Kr. Arason, *Cohomologische Invarianten quadratischer Formen*. J. Algebra **36**(1975), 448–491. http://dx.doi.org/10.1016/0021-8693(75)90145-3
[3] E. Artin and J. Tate, *Class field theory.* AMS Chelsea Publishing, Providence, RI, 2009.
[4] P. K. Draxl, *Skew fields*. London Mathematical Society Lecture Notes Series, 81, Cambridge University Press, Cambridge, 1983.
[5] W. G. Dwyer, *Homology, Massey products and maps between groups*. J. Pure Appl. Algebra **6**(1975), 177–190. http://dx.doi.org/10.1016/0022-4049(75)90006-7
[6] I. Efrat, *The Zassenhaus filtration, Massey products, and representations of profinite groups*. Adv. Math. **263**(2014), 389–411. http://dx.doi.org/10.1016/j.aim.2014.07.006
[7] I. Efrat and J. Mináč, *On the descending central sequence of absolute Galois groups*. Amer. J. Math. **133**(2011), no. 6, 1503–1532. http://dx.doi.org/10.1353/ajm.2011.0041
[8] R. Elman, T. Y. Lam, J.-P. Tignol, and A. R. Wadsworth, *Witt rings and Brauer groups under multiquadratic extensions. I*. Amer. J. Math. **105**(1983), no. 5, 1119–1170. http://dx.doi.org/10.2307/2374336
[9] R. A. Fenn, *Techniques of geometric topology*. London Mathematical Society Lecture Notes Series, 57, Cambridge University Press, Cambridge, 1983.
[10] M. J. Hopkins and K. G. Wickelgren, *Splitting varieties for triple Massey products*. J. Pure Appl. Algebra **219**(2015), no. 5, 1304–1319. http://dx.doi.org/10.1016/j.jpaa.2014.06.006
[11] D. Kraines, *Massey higher products*. Trans. Amer. Math. Soc. **124**(1966), 431–449. http://dx.doi.org/10.1090/S0002-9947-1966-0202136-1
[12] N. Lemire, J. Mináč, and J. Swallow, *Galois module structure of Galois cohomology and partial Euler-Poincaré characteristics.* J. Reine Angew. Math. **613**(2007), 147–173.
[13] E. Matzri, *$\mathbb{Z}_3 \times \mathbb{Z}_3$-crossed products*. J. Algebra, **418**(2014), 1–7. http://dx.doi.org/10.1016/j.jalgebra.2014.06.035
[14] J. P. May, *Matric Massey products*. J. Algebra **12**(1969), 533–568. http://dx.doi.org/10.1016/0021-8693(69)90027-1
[15] K. McKinnie, *Degeneracy and decomposability in abelian crossed products*. J. Algebra **328**(2011), 443–460. http://dx.doi.org/10.1016/j.jalgebra.2010.10.029
[16] J. Mináč and N. D. Tân, *Triple Massey products and Galois theory*. J. Eur. Math. Soc., to appear. arxiv:1307.6624
[17] ———, *Triple Massey products over global fields*. arxiv:1403.4586
[18] ———, *The kernel unipotent conjecture and the vanishing of Massey products for odd rigid fields*. (with an appendix by I. Efrat, J. Mináč, and N.D. Tân) Adv. Math. **273**(2015), 242–270. http://dx.doi.org/10.1016/j.aim.2014.12.028
[19] L. H. Rowen, *Cyclic division algebras*. Israel J. Math. **41**(1982), no. 3, 213–234; Correction: Israel J. Math. **43**(1982), no. 3, 277–280. http://dx.doi.org/10.1007/BF02771722
[20] ———, *Division algebras of exponent* 2 *and characteristic* 2. J. Algebra **90**(1984), no. 1, 71–83. http://dx.doi.org/10.1016/0021-8693(84)90199-6
[21] D. J. Saltman, *Indecomposable division algebras*. Comm. Algebra **7**(1979), no. 8, 791–817. http://dx.doi.org/10.1080/00927877908822376
[22] J.-P. Serre, *Local fields*. Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.

[23] J.-P. Tignol, *Central simple algebras with involution*. In: Ring theory (Proc. Antwerp Conf. (NATO Adv. Study Inst.), Univ. Antwerp, 1978), Lecture Notes in Pure and Appl. Math., 51, Dekker, New York, 1979, pp. 279–285.
[24] ———, *Corps à involution neutralisés par une extension abélienne élémentaire*. In: The Brauer Group (Sem., Les Plans-sur-Bex, 1980), Lecture Notes in Math, 844, Springer, Berlin, 1981, pp. 1–34.
[25] ———, *Produits croisés abéliens*. J. Algebra **70**(1981), no. 2, 420–436. http://dx.doi.org/10.1016/0021-8693(81)90227-1
[26] ———, *Algèbres indécomposables d'exposant premier*. Adv. in Math. **65**(1987), 205–228. http://dx.doi.org/10.1016/0001-8708(87)90022-3
[27] V. Voevodsky, *Motivic cohomology with* $\mathbb{Z}/2$*-coefficients*. Publ. Math. Inst. Hautes Études Sci. **98**(2003), 59–104.
[28] K. Wickelgren, *n-nilpotent obstructions to* π_1 *sections of* $\mathbb{P}^1 - \{0, 1, \infty\}$ *and Massey products*. In: Galois-Teichmüller theory and arithmetic geometry, Adv. Stud. Pure Math., 63, Math. Soc. Japan, Tokyo, 2012, pp. 579–600.

Department of Mathematics, Ben-Gurion University of the Negev, Be'er-Sheva 84105, Israel
e-mail: efrat@math.bgu.ac.il elimatzri@gmail.com

https://doi.org/10.4153/CMB-2015-026-5 Published online by Cambridge University Press