LECTURES ON THE MASSEY VANISHING CONJECTURE

ALEXANDER MERKURJEV AND FEDERICO SCAVIA

Abstract. These are lecture notes for the 2024 PCMI Graduate Summer School. We present our joint work on Massey products in Galois cohomology. The highlights are a proof of the Massey Vanishing Conjecture for mod 2 fourfold Massey products over arbitrary fields, and the construction, for every prime p, of a field containing all primitive p-power roots of unity whose mod p Galois cohomology DGA is not formal.

Contents

1. Lecture 1. The Massey Vanishing Conjecture

1.1. Massey products.

Massey products. Massey products are a higher cohomological operation on the cohomology $H^*(A)$ of a differential graded ring A which generalizes the cup product. They were introduced in algebraic topology by Massey [Mas58]: here A is the differential graded ring of singular cochains of a topological space, with coefficients in a ring.

Let Γ be a profinite group, and let p be a prime number. In this lecture series, we are interested in Massey products in the group cohomology of profinite groups:

Date: July 2024.

here $A = C^*(\Gamma, \mathbb{Z}/p\mathbb{Z})$ is the differential graded ring of continuous cochains of a profinite group with $\mathbb{Z}/p\mathbb{Z}$ coefficients, so that $H^*(A) = H^*(\Gamma, \mathbb{Z}/p\mathbb{Z})$ is the mod p group cohomology ring of Γ. The Massey product of elements of $H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$ admits a simple group-theoretic description, due to Dwyer [Dwy75], which we now recall.

Let $n \geq 2$ be an integer, and let U_{n+1} be the subgroup of upper unitriangular matrices in $\mathrm{GL}_{n+1}(\mathbb{Z}/p\mathbb{Z})$, that is, upper triangular matrices with all diagonal entries equal to 1. This is a p-Sylow subgroup of $\mathrm{GL}_{n+1}(\mathbb{Z}/p\mathbb{Z})$. Its center Z_{n+1} consists of those matrices in U_{n+1} which are zero on every non-diagonal entry except possibly for entry $(1, n+1)$ (the top-right corner). We let $\overline{U}_{n+1} \coloneqq U_{n+1}/Z_{n+1}$ denote the factor group: we can think of elements of $\overline{U}_{n+1}$ as upper unitriangular matrices with the top-right corner removed.

For all i and j such that $1 \leq i < j \leq n+1$, we let $u_{i,j} \colon U_{n+1} \to \mathbb{Z}/p\mathbb{Z}$ be the coordinate function corresponding to entry (i, j). For all $(i, j) \neq (1, n+1)$, the $u_{i,j}$ also define coordinate functions on $\overline{U}_{n+1} \to \mathbb{Z}/p\mathbb{Z}$. The $u_{i,j}$ are not necessarily group homomorphisms.

Exercise 1.1. Show that $u_{i,i+1}$ is a group homomorphism for all $1 \leq i \leq n$. Convince yourself that $u_{i,j}$ is not a group homomorphism if $j \geq i+2$.

We have a diagram of surjective group homomorphisms

$$\begin{tikzcd} U_{n+1} \arrow[r, two heads] & \overline{U}_{n+1} \arrow[r, two heads] & (\mathbb{Z}/p\mathbb{Z})^n, \end{tikzcd} \tag{1.1}$$

where the right map is given $(u_{12}, \dots u_{n,n+1})$, that is, by forgetting all entries except for the first upper diagonal.

Now let Γ be a profinite group, let p be a prime number, and consider $\mathbb{Z}/p\mathbb{Z}$ as a Γ-module with trivial action. We have

$$H^1(\Gamma, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cont}}(\Gamma, \mathbb{Z}/p\mathbb{Z}).$$

Let $\chi_1, \dots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$ be continuous homomorphisms, and define

$$\chi \coloneqq (\chi_1, \dots, \chi_n) \colon \Gamma \to \mathbb{Z}/p\mathbb{Z}.$$

Consider the diagram

$$\begin{tikzcd} & & \Gamma \arrow[d, "\chi"] \\ U_{n+1} \arrow[r, two heads] & \overline{U}_{n+1} \arrow[r] & (\mathbb{Z}/p\mathbb{Z})^n, \end{tikzcd}$$

where the bottom row is (1.1).

Let $\overline{\rho} \colon \Gamma \to \overline{U}_{n+1}$ be a (continuous) lift of χ. Such a lift may not exist, or one may get several liftings. We want to understand when $\overline{\rho}$, if it exists, may be lifted to a homomorphism $\rho \colon \Gamma \to \overline{U}_{n+1}$. Pictorially, we want to determine whether a dashed arrow ρ in the commutative diagram below exists:

$$\begin{tikzcd} & & \Gamma \arrow[dll, dashed, "\rho"'] \arrow[dl, "\overline{\rho}"] \arrow[d, "\chi"] \\ U_{n+1} \arrow[r, two heads] & \overline{U}_{n+1} \arrow[r] & (\mathbb{Z}/p\mathbb{Z})^n. \end{tikzcd} \tag{1.2}$$

Concretely, $\overline{\rho}$ may be viewed as a matrix

$$\begin{bmatrix} 1 & \overline{\rho}_{12} & \dots & \overline{\rho}_{1,n} & \square \\ & 1 & & & \overline{\rho}_{2,n+1} \\ & & 1 & & \vdots \\ & & & 1 & \overline{\rho}_{n,n+1} \\ & & & & 1 \end{bmatrix}$$

where $\overline{\rho}_{ij} \coloneqq u_{ij} \circ \overline{\rho} \colon \Gamma \to \mathbb{Z}/p\mathbb{Z}$ are cochains. By Exercise 1.1, only the $\overline{\rho}_{ij}$ appearing in the first upper diagonal are homomorphisms: in fact, the commutativity of the right triangle in (1.2) is equivalent to

$$\overline{\rho}_{i,i+1} = \chi_i.$$

We now express in matrix notation the condition that $\overline{\rho}$ lifts to a homomorphism $\rho \colon \Gamma \to U_{n+1}$. Let $\eta \colon \Gamma \to \mathbb{Z}/p\mathbb{Z}$ be a cochain, and consider the function $\rho \colon \Gamma \to U_{n+1}$ with matrix representation

$$\begin{bmatrix} 1 & \overline{\rho}_{12} & \dots & \overline{\rho}_{1,n} & \eta \\ & 1 & & & \overline{\rho}_{2,n+1} \\ & & 1 & & \vdots \\ & & & 1 & \overline{\rho}_{n,n+1} \\ & & & & 1 \end{bmatrix}$$

The function ρ is a group homomorphism if and only if, for all $x, y \in \Gamma$ one has

$$\rho(xy) = \rho(x)\rho(y).$$

By considering the $(1, n+1)$ entry on both sides, we see that this condition is equivalent to

$$\eta(xy) = \eta(y) + \sum_{i=2}^{n} \overline{\rho}_{1i}(x)\overline{\rho}_{i,n+1}(y) + \eta(x) \tag{1.3}$$

for all $x, y \in \Gamma$. Let us set

$$\Delta(\overline{\rho}) \colon \Gamma^2 \to \mathbb{Z}/p\mathbb{Z}, \qquad \Delta(\overline{\rho})(x,y) = \sum_{i=2}^{n} \overline{\rho}_{1i}(x)\overline{\rho}_{i,n+1}(y).$$

Exercise 1.2. Using the fact that $\overline{\rho}$ is a homomorphism, check that $\Delta(\overline{\rho})$ is 2-cocycle:

$$\Delta(\overline{\rho}) \in Z^2(\Gamma, \mathbb{Z}/p\mathbb{Z}).$$

Note that $\eta(x) + \eta(y) - \eta(xy) = \partial(\eta)(x,y)$, where ∂ denotes the coboundary operator. Equation (1.3) may thus be rewritten as

$$\Delta(\overline{\rho})(x,y) = \partial(-\eta)(x,y). \tag{1.4}$$

Thus $\Delta(\overline{\rho})$ represents the obstruction to lifting $\overline{\rho}$ to some $\overline{\rho}$:

$$\overline{\rho} \text{ lifts to } \rho \iff [\Delta(\overline{\rho})] = 0 \text{ in } H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}).$$

This motivates the following definition.

Definition 1.3. Let Γ be a profinite group, let p be a prime number, and let $\chi_1, \dots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$. The mod p Massey product of $\chi_1, \dots, \chi_n$ is the set

$$\langle \chi_1, \dots, \chi_n \rangle \coloneqq \{[\Delta(\overline{\rho})] : \ \overline{\rho}\colon \Gamma \to \overline{U}_{n+1} \text{ lifts } \chi\} \subset H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}).$$

We say that $\langle \chi_1, \dots, \chi_n \rangle$ is defined if it is non-empty, that is, if and only if there exists a $\overline{\rho}\colon \Gamma \to \overline{U}_{n+1}$ lifting χ.

We say that $\langle \chi_1, \dots, \chi_n \rangle$ vanishes if it contains 0, that is, if and only if there exists a $\rho\colon \Gamma \to U_{n+1}$ lifting χ.

Of course, if $\langle \chi_1, \dots, \chi_n \rangle$ vanishes, then it is defined.

Example 1.4. Suppose that $n = 2$, so that $\chi = (\chi_1, \chi_2)$. Then

$$\overline{\rho} = \begin{bmatrix} 1 & \chi_1 & \square \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{bmatrix}$$

and $\langle \chi_1, \chi_2 \rangle = \{\chi_1 \cup \chi_2\}$. Therefore $\langle \chi_1, \chi_2 \rangle$ is defined, and it vanishes if and only if $\chi_1 \cup \chi_2 = 0$ in $H^2(\Gamma, \mathbb{Z}/p\mathbb{Z})$.

1.2. **The Massey Vanishing Conjecture.** Let Γ be a profinite group, let p be a prime number, let $n \geq 3$ be an integer, and let $\chi_1, \dots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$. We have the following implications:

(1.5)
$$\langle \chi_1, \dots, \chi_n \rangle \text{ vanishes} \Rightarrow \langle \chi_1, \dots, \chi_n \rangle \text{ is defined} \Rightarrow \chi_i \cup \chi_{i+1} = 0 \ (1 \leq i \leq n).$$

Exercise 1.5. Prove the second implication. Where do you need to use that $n \geq 3$?

Hint: First show that the function

$$\pi_i \colon \overline{U}_{n+1} \to U_3, \qquad A \mapsto \begin{bmatrix} 1 & u_{i,i+1}(A) & u_{i,i+2}(A) \\ 0 & 1 & u_{i+1,i+2}(A) \\ 0 & 0 & 1 \end{bmatrix}$$

is a well-defined group homomorphism, for all $1 \leq i \leq n-1$. Then use Example 1.4.

For an arbitrary profinite group Γ, the implications of (1.5) cannot be reversed in general.

Exercise 1.6. (1) Let p be an odd prime, let Γ be a cyclic group of order p, and let $\chi \in H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$ be a non-zero character. Show that the p-fold mod p Massey product $\langle \chi, \dots, \chi \rangle$ is defined but does not vanish. (See [MT17, Example 4.7] for a solution.)

(2) Let $G \coloneqq \langle a, b : a^2 b = b a^2 \rangle$, and let Γ be the pro-2 completion of G. Find $\chi_1, \chi_2, \chi_3 \in H^1(\Gamma, \mathbb{Z}/2\mathbb{Z})$ such that $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined but does not vanish. (See [MS23c, Proposition 8.3(3)] for a solution.)

Let F be a field, let p be a prime number invertible in F, let F_s be a separable closure of F, and let $\Gamma_F = \mathrm{Gal}(F_s/F)$ be the absolute Galois group of F.

Theorem 1.7 (Hopkins–Wickelgren)**.** *Suppose that F is a number field. Then every triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle \subset H^2(F, \mathbb{Z}/2\mathbb{Z})$ vanishes if and only if it is defined.*

Theorem 1.8 (Mináč–Tân)**.** *Let F be an arbitrary field. Then every triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle \subset H^2(F, \mathbb{Z}/2\mathbb{Z})$ vanishes if and only if it is defined.*

Conjecture 1.9 (Massey Vanishing Conjecture (Mináč–Tân))**.** *Let F be a field, let $n \geq 3$ be an integer, let p be a prime number, and let $\chi_1, \ldots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$. If $\langle \chi_1, \ldots, \chi_n \rangle$ is defined, then it vanishes.*

Remark 1.10 (Motivation for Conjecture 1.9). The main motivation for the Massey Vanishing Conjecture comes from the Profinite Inverse Galois Problem: Which profinite groups are absolute Galois groups of fields?

Some restrictions are known. For example, the only finite absolute Galois groups are the trivial group and the cylic group of order two (Artin–Schreier).

Assume that F contains a primitive p-th root of unity. The Bloch–Kato Conjecture, proved by Voevodsky and Rost, implies that the cohomology ring $H^*(F, \mathbb{Z}/p\mathbb{Z})$ is quadratic: it admits a presentation with generators in degree 1 (corresponding to elements of $F^\times$) and relations in degree 2 (the Steinberg relations).

Here is a summary of the known results on Conjecture 1.9.

F	n	p	Authors	Ref.
Number field	3	2	Hopkins–Wickelgren	[HW15]
Arbitrary	3	2	Mináč–Tân	[MT15]
Arbitrary	3	Any	Efrat–Matzri, Mináč–Tân	[EM17], [MT17]
Number fields	4	2	Guillot–Mináč–Topaz–Wittenberg	[GMT18]
Number fields	Any	Any	Harpaz–Wittenberg	[HW23]
Arbitrary	4	2	Merkurjev–Scavia	[MS23a]

Exercise 1.11. Prove the Massey Vanishing Conjecture for local fields. (See [MT17, Theorem 4.3] for a solution.)

(Hint: Let K be a local field. Given a homomorphism $\overline{\rho}\colon \Gamma_K \to \overline{U}_{n+1}$ lifting $(\chi_1, \ldots, \chi_n)\colon \Gamma_K \to (\mathbb{Z}/p\mathbb{Z})^n$, if $\chi_1 \neq 0$ then suitably modify entry $(2, n+1)$ of $\overline{\rho}$. Recall that for every local field K, we have $\dim_{\mathbb{F}_p} H^2(K, \mathbb{Z}/p\mathbb{Z}) = 1$ and the cup-product $H^1(K, \mathbb{Z}/p\mathbb{Z}) \times H^1(K, \mathbb{Z}/p\mathbb{Z}) \to H^2(K, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{F}_p$ is a non-degenerate bilinear form. Treat the case $\chi_1 = 0$ separately.)

Remark 1.12 (Number field case). The general proof strategy for the Massey Vanishing Conjecture over number fields is as follows. Let $\chi_1, \ldots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$ be such that $\langle \chi_1, \ldots, \chi_n \rangle$ is defined. One first constructs an F-variety X such that, for every field extension K/F, we have $X(K) \neq \emptyset$ if and only if $\langle \chi_1, \ldots, \chi_n \rangle$ is defined over K. (Here we are considering the pullback $H^*(F, \mathbb{Z}/p\mathbb{Z}) \to H^*(K, \mathbb{Z}/p\mathbb{Z})$ in étale cohomology induced by the morphism $\mathrm{Spec}(K) \to \mathrm{Spec}(F)$.)

Since $\langle \chi_1, \ldots, \chi_n \rangle$ is defined over F, it is defined over F_v for every place v of F. By Exercise 1.11, this implies that $\langle \chi_1, \ldots, \chi_n \rangle$ vanishes over F_v for every place v, that is, $X(F_v) \neq \emptyset$ for every v.

Using Brauer–Manin obstruction techniques, one then tries to deduce that $X(F) \neq \emptyset$. This is by far the hardest part of argument, and its feasability is highly dependent on the geometry of X. In [HW23], Harpaz and Wittenberg take X to be an SL_N-homogeneous space with finite supersolvable geometric stabilizer.

The main objective of Lectures 2 and 3 is to explain the proof of the statement appearing in the bottom row of the table.

Theorem 1.13. *Let F be a field, let $\chi_1, \chi_2, \chi_3, \chi_4 \in H^1(F, \mathbb{Z}/2\mathbb{Z})$, be such that the Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle \subset H^2(F, \mathbb{Z}/2\mathbb{Z})$ is defined. Then $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle$ vanishes.*

Remark 1.14. Let p be a prime, and let F be a field such that $H^2(F,\mathbb{Z}/p\mathbb{Z})=0$. Then, for all $n\geq 2$, the map $H^1(F,U_{n+1})\to H^1(F,\overline{U}_{n+1})$ is surjective, and hence the Massey Vanishing Conjecture holds for F.

In particular, the Massey Vanishing Conjecture holds for fields of characteristic p and for field of cohomological dimension 1 (for example finite fields and function fields of curves over algebraically closed fields).

1.3. **The case when F contains a primitive p-th root of unity.** Suppose that F contains primitive p-th root of unity $\zeta\in F^\times$. We identify $\mathbb{Z}/p\mathbb{Z}=\mu_p$ by means of the isomorphism sending 1 to ζ. Kummer Theory gives the identifications

$$H^1(F,\mathbb{Z}/p\mathbb{Z})=F^\times/F^{\times p},\qquad H^2(F,\mathbb{Z}/p\mathbb{Z})=\mathrm{Br}(F)[p].$$

If $a\in F^\times$, we let $\chi_a\colon\Gamma_F\to\mathbb{Z}/p\mathbb{Z}$ be the corresponding continuous homomorphism, that is, letting $a'\in F_s^\times$ be a p-th root of a, we have $(g-1)(a')=\zeta^{\chi_a(g)}$ for all $g\in\Gamma_F$. (We always use additive notation for the Galois action on $F_s^\times$.) Under these identifications, the cup product $\chi_a\cup\chi_b$ corresponds to (a,b), the Brauer class of the degree-p cyclic algebra determined by a and b.

We may restate (1.5) for $\Gamma=\Gamma_F$ purely in terms of F:

$$\langle a_1,\dots,a_n\rangle \text{ vanishes} \Rightarrow \langle a_1,\dots,a_n\rangle \text{ is defined} \Rightarrow a_i\cup a_{i+1}=0\ (1\leq i\leq n). \tag{1.6}$$

1.4. **Galois algebras.** Let G be a finite group. By definition, a *G-algebra L/F* is an étale F-algebra on which G acts via F-algebra automorphisms. We say that the G-algebra L is *Galois* if $|G|=\dim_F L$ and $L^G=F$; see [KMRT98, Definitions (18.15)]. A G-algebra L/F is Galois if and only if the morphism of schemes $\mathrm{Spec}(L)\to\mathrm{Spec}(F)$ is an étale G-torsor. By [KMRT98, Example (28.15)], we have a canonical bijection

$$H^1(F,G)\xrightarrow{\sim}\{\text{Isomorphism classes of Galois } G\text{-algebras over } F\} \tag{1.7}$$

which is functorial in F and G.

1.5. **Galois U_3-algebras.**

Lemma 1.15. *Let p be a prime, and let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ. The following are equivalent:*

(i) $(a,b)=0$ in $\mathrm{Br}(F)$;
(ii) there exists $\alpha\in F_a^\times$ such that $b=N_a(\alpha)$;
(iii) there exists $\beta\in F_b^\times$ such that $a=N_b(\beta)$.

Proof. See [Ser79, Chapter XIV, Proposition 4(iii)]. □

Let $a,b\in F^\times$, and suppose that $(a,b)=0$ in $\mathrm{Br}(F)$. By Lemma 1.15, we may fix $\alpha\in F_a^\times$ and $\beta\in F_b^\times$ such that $N_a(\alpha)=b$ and $N_b(\beta)=a$.

We write $(\mathbb{Z}/p\mathbb{Z})^2=\langle\sigma_a,\sigma_b\rangle$, and we view $F_{a,b}$ as a Galois $(\mathbb{Z}/p\mathbb{Z})^2$-algebra via

$$(\sigma_a-1)(a^{1/p})=(\sigma_b-1)(b^{1/p})=\zeta,\qquad(\sigma_a-1)(b^{1/p})=(\sigma_b-1)(a^{1/p})=1.$$

The projection $U_3\to\overline{U}_3=(\mathbb{Z}/p\mathbb{Z})^2$ sends $e_{12}\mapsto\sigma_a$ and $e_{23}\mapsto\sigma_b$. We define the following elements of U_3:

$$\sigma_a:=e_{12},\qquad\sigma_b:=e_{23},\qquad\tau:=e_{13}=[\sigma_a,\sigma_b].$$

Suppose given $x\in F_a^\times$ such that

$$(\sigma_a-1)x=\frac{b}{\alpha^p}. \tag{1.8}$$

The étale F-algebra $K \coloneqq (F_{a,b})_x$ has the structure of a Galois U_3-algebra such that the Galois $(\mathbb{Z}/p\mathbb{Z})^2$-algebra K^{Q_3} is equal to $F_{a,b}$, and

$$(\sigma_a - 1)x^{1/p} = \frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)x^{1/p} = 1, \qquad (\tau - 1)x^{1/p} = \zeta^{-1}. \tag{1.9}$$

Similarly, suppose given $y \in F_b^\times$ such that

$$(\sigma_b - 1)y = \frac{a}{\beta^p}. \tag{1.10}$$

The étale F-algebra $K \coloneqq (F_{a,b})_y$ has the structure of a Galois U_3-algebra, such that the Galois $(\mathbb{Z}/p\mathbb{Z})^2$-algebra K^{Q_3} is equal to $F_{a,b}$, and

$$(\sigma_a - 1)y^{1/p} = 1, \qquad (\sigma_b - 1)y^{1/p} = \frac{a^{1/p}}{\beta}, \qquad (\tau - 1)y^{1/p} = \zeta. \tag{1.11}$$

In (1.9) and (1.11), the relation involving τ follows from the first two.

If $x \in F_a^\times$ satisfies (1.8), then so does ax. We may thus apply (1.9) to $(F_{a,b})_{ax}$. Therefore $(F_{a,b})_{ax}$ has the structure of a Galois U_3-algebra, where U_3 acts via $\overline{U}_3 = \mathrm{Gal}(F_{a,b}/F)$ on $F_{a,b}$, and

$$(\sigma_a - 1)(ax)^{1/p} = \frac{b^{1/p}}{\alpha}, \qquad (\sigma_b - 1)(ax)^{1/p} = 1, \qquad (\tau - 1)(ax)^{1/p} = \zeta^{-1}.$$

Similarly, if $y \in F_b^\times$ satisfies (1.10), we may apply (1.11) to $(F_{a,b})_{by}$. Therefore $(F_{a,b})_{by}$ admits a Galois U_3-algebra structure, where U_3 acts via $\overline{U}_3 = \mathrm{Gal}(F_{a,b}/F)$ on $F_{a,b}$, and

$$(\sigma_a - 1)(by)^{1/p} = 1, \qquad (\sigma_b - 1)(by)^{1/p} = \frac{a^{1/p}}{\beta}, \qquad (\tau - 1)(by)^{1/p} = \zeta.$$

Lemma 1.16. *(1) Let $x \in F_a^\times$ satisfy (1.8), and consider the Galois U_3-algebras $(F_{a,b})_x$ and $(F_{a,b})_{ax}$ as in (1.9). Then $(F_{a,b})_x \simeq (F_{a,b})_{ax}$ as Galois U_3-algebras.*

(2) Let $y \in F_b^\times$ satisfy (1.8), and consider the Galois U_3-algebras $(F_{a,b})_y$ and $(F_{a,b})_{by}$ as in (1.11). Then $(F_{a,b})_y \simeq (F_{a,b})_{by}$ as Galois U_3-algebras.

Proof. (1) The automorphism $\sigma_b \colon F_{a,b} \to F_{a,b}$ extends to an isomorphism of étale algebras $f \colon (F_{a,b})_{ax} \to (F_{a,b})_x$ by sending $(ax)^{1/p}$ to $a^{1/p}x^{1/p}$. The map f is well defined because $f((ax)^{1/p})^p = [a^{1/p}x^{1/p}]^p = ax$. We now show that f is U_3-equivariant. The restriction of f to $F_{a,b}$ is U_3-equivariant because $\sigma_a\sigma_b = \sigma_b\sigma_a$ on $F_{a,b}$. We have

$$\sigma_a(f((ax)^{1/p})) = \sigma_a(a^{1/p}) \cdot \sigma_a(x^{1/p}) = \zeta \cdot a^{1/p} \cdot \frac{b^{1/p}}{\alpha} \cdot x^{1/p} = \frac{\zeta a^{1/p} b^{1/p} x^{1/p}}{\alpha}$$

and

$$f(\sigma_a((ax)^{1/p})) = f((b^{1/p}/\alpha) \cdot (ax)^{1/p}) = \zeta \cdot \frac{b^{1/p}}{\alpha} \cdot a^{1/p} \cdot x^{1/p} = \frac{\zeta a^{1/p} b^{1/p} x^{1/p}}{\alpha}.$$

Thus f is $\langle\sigma_a\rangle$-equivariant. We also have

$$\sigma_b(f((ax)^{1/p})) = \sigma_b(a^{1/p}) \cdot \sigma_b(x^{1/p}) = a^{1/p} \cdot x^{1/p}$$

and

$$f(\sigma_b((ax)^{1/p})) = f((ax)^{1/p}) = a^{1/p} \cdot x^{1/p}.$$

Thus f is $\langle\sigma_b\rangle$-equivariant. Since σ_a and σ_b generate U_3, we conclude that f is U_3-equivariant, as desired.

(2) The proof is similar to that of (1). □

Proposition 1.17. *Let $a, b \in F^\times$ be such that $(a, b) = 0$ in $\mathrm{Br}(F)$, and fix $\alpha \in F_a^\times$ and $\beta \in F_b^\times$ such that $N_a(\alpha) = b$ and $N_b(\beta) = a$.*

(1) Every Galois U_3-algebra K over F such that $K^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras is of the form $(F_{a,b})_x$ for some $x \in F_a^\times$ as in (1.8), with U_3-action given by (1.9).

(2) Every Galois U_3-algebra K over F such that $K^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras is of the form $(F_{a,b})_y$ for some $y \in F_b^\times$ as in (1.10), with U_3-action given by (1.11).

Proof. (1) Since $Q_3 = \langle \tau \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ and $K^{Q_3} \simeq F_{a,b}$ as $(\mathbb{Z}/p\mathbb{Z})^2$-algebras, we have an isomorphism of étale $F_{a,b}$-algebras $K \simeq (F_{a,b})_z$, for some $z \in F_{a,b}^\times$ such that $(\tau - 1)z^{1/p} = \zeta^{-1}$. We may suppose that $K = (F_{a,b})_z$. As τ commutes with σ_b we have

$$(\tau - 1)(\sigma_b - 1)z^{1/p} = (\sigma_b - 1)(\tau - 1)z^{1/p} = (\sigma_b - 1)\zeta^{-1} = 1,$$

hence $(\sigma_b - 1)z^{1/p} \in F_{a,b}^\times$. By Hilbert's Theorem 90 for the extension $F_{a,b}/F_a$, there is $t \in F_{a,b}^\times$ such that $(\sigma_b - 1)z^{1/p} = (\sigma_b - 1)t$. Replacing z by zt^{-p}, we may thus assume that $(\sigma_b - 1)z^{1/p} = 1$. In particular, $z \in F_a^\times$. Since $(\tau - 1)z^{1/p} = \zeta^{-1}$, we have $\sigma_b\sigma_a(z^{1/p}) = \zeta\sigma_a\sigma_b(z^{1/p})$. Thus

$$(\sigma_b - 1)(\sigma_a - 1)z^{1/p} = (\sigma_b\sigma_a - \sigma_a\sigma_b + (\sigma_a - 1)(\sigma_b - 1))z^{1/p} = \zeta(\sigma_a - 1)(\sigma_b - 1)z^{1/p} = \zeta,$$

and hence $(\sigma_a - 1)z^{1/p} = b^{1/p}/\alpha'$ for some $\alpha' \in F_a^\times$. Moreover $N_a(\alpha'/\alpha) = b/b = 1$, and so by Hilbert's Theorem 90 there exists $\theta \in F_a^\times$ such that $\alpha'/\alpha = (\sigma_a - 1)\theta$. We define $x := z\theta^p \in F_a^\times$, and set $x^{1/p} := z^{1/p}\theta \in (F_{a,b})_z^\times$. Then $K = (F_{a,b})_x$, where

$$(\sigma_a - 1)x^{1/p} = (\sigma_a - 1)z^{1/p} \cdot (\sigma_a - 1)\theta = \frac{b^{1/p}}{\alpha'} \cdot \frac{\alpha'}{\alpha} = \frac{b^{1/p}}{\alpha}$$

and $(\sigma_b - 1)x^{1/p} = 1$, as desired.

(2) The proof is analogous to that of (1). □

1.6. **Proof of Massey Vanishing for $n = 3$.** As as warm-up for the proof of Theorem 1.13, we first prove the case $n = 3$ of the Massey Vanishing Conjecture.

Theorem 1.18 (Efrat–Matzri, Mináč–Tân)**.** *Let F be a field, let p be a prime number, and let $\chi_1, \chi_2, \chi_3 \in H^1(F, \mathbb{Z}/p\mathbb{Z})$. The following are equivalent:*

(1) $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$ in $H^2(F, \mathbb{Z}/p\mathbb{Z})$;
(2) $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined;
(3) $\langle \chi_1, \chi_2, \chi_3 \rangle$ vanishes.

Proof. It suffices to prove that (1) implies (3). A simple argument [MT16, Proposition 4.14] shows that we may assume that F contains a primitive p-th root of unity ζ. We also easily reduce to the case when χ_1 and χ_3 are non-zero. We fix $a, b, c \in F^\times$ such that $\chi_1 = \chi_a$, $\chi_2 = \chi_b$ and $\chi_3 = \chi_c$. Thus a and c are not squares in F. Let $\alpha \in F_a^\times$ such that $N_a(\alpha) = b$. By Proposition 1.17(1), there exists a cochain $\rho : \Gamma_F \to \mathbb{Z}/p\mathbb{Z}$ such that $\rho|_{\Gamma_a} = \chi_\theta$ for some $\theta \in F_a^\times$ such that $(\sigma_a - 1)\theta = b/\alpha^p$ and

$$\begin{bmatrix} 1 & \chi_a & \rho \\ 0 & 1 & \chi_b \\ 0 & 0 & 1 \end{bmatrix}$$

is a homomorphism. By a similar argument, there exists a cochain $\rho : \Gamma_F \to \mathbb{Z}/p\mathbb{Z}$ such that

$$\begin{bmatrix} 1 & \chi_b & \rho' \\ 0 & 1 & \chi_c \\ 0 & 0 & 1 \end{bmatrix}$$

is a homomorphism. Thus

$$\begin{bmatrix} 1 & \chi_a & \rho & \square \\ 0 & 1 & \chi_b & \rho' \\ 0 & 0 & 1 & \chi_c \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

is a homomorphism. The obstruction $A \in \mathrm{Br}(F)[p]$ to lifting this homomorphism to U_4 is represented by the cocycle $\chi_a \cup \rho' + \rho \cup \chi_c$.

Let $\gamma \in F_c^\times$ such that $N_c(\gamma) = b$. Then

$$N_{\sigma_a\sigma_c}(\alpha/\gamma) = N_a(\alpha)/N_c(\gamma) = b/b = 1,$$

and hence by Hilbert's Theorem 90 there exists $\omega \in F_{a,c}^\times$ such that

$$\alpha/\gamma = (\sigma_a\sigma_c - 1)\omega.$$

Set $e \coloneqq \theta \cdot N_c(\omega) \in F_a^\times$. We have

$$\begin{aligned}(\sigma_a - 1)e &= (b/\alpha^p) \cdot N_c((\sigma_a - 1)\omega) = (b/\alpha^p) \cdot N_c((\sigma_a\sigma_c - 1)\omega) \\ &= (b/\alpha^p) \cdot N_C(\alpha/\gamma) = (b/\alpha^p)(\alpha^p/b) = 1.\end{aligned}$$

Therefore $e \in F^\times$. We have

$$A_{F_a} = (\rho \cup \chi_c)_{F_a} = (\theta, c) = (\theta \cdot N_c(\omega), c) = (e, c)_{F_a}.$$

Thus $A - (e, c)$ is split by F_a, and hence $A - (e, c) = (a, f)$ for some $f \in F^\times$, that is, $A = (e, c) + (a, f)$. Consider the continuous homomorphism

$$\begin{bmatrix} 1 & \chi_a & \rho - \chi_f & \square \\ 0 & 1 & \chi_b & \rho' - \chi_e \\ 0 & 0 & 1 & \chi_c \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The obstruction to lifting this homomorphism to U_4 is given by

$$\chi_a \cup (\rho' - \chi_f) + (\rho - \chi_e) \cup \chi_c = A - A = 0.$$

Thus the homomorphism lifts to U_4 and $\langle a, b, c\rangle$ vanishes, as desired. □

2. Lecture 2. Beginning of Proof of Theorem 1.13

2.1. **Galois U_3-algebras, $p = 2$.** Suppose that $\mathrm{char}(F) \neq 2$, let $a, b \in F^\times$, and suppose that $(a, b) = 0$ in $\mathrm{Br}(F)[2]$. We write $(\mathbb{Z}/2\mathbb{Z})^2 = \langle \sigma_a, \sigma_b\rangle$, and we view $F_{a,b}$ as a Galois $(\mathbb{Z}/2\mathbb{Z})^2$-algebra by

$$(\sigma_a - 1)(\sqrt{a}) = (\sigma_b - 1)(\sqrt{b}) = -1, \qquad (\sigma_a - 1)(\sqrt{b}) = (\sigma_b - 1)(\sqrt{a}) = 1.$$

Let $\alpha \in F_a^\times$ satisfy $N_a(\alpha) = bx^2$ for some $x \in F^\times$, and consider the étale F-algebra $(F_{a,b})_\alpha$. We have

$$U_3 = \langle \sigma_a, \sigma_b : \sigma_a^2 = \sigma_b^2 = [\sigma_a, \sigma_b]^2 = 1\rangle.$$

Moreover, $\overline{U}_3 = (\mathbb{Z}/2\mathbb{Z})^2$ and the surjective homomorphism $U_3 \to \overline{U}_3$ is given by $\sigma_a \mapsto \sigma_a$ and $\sigma_b \mapsto \sigma_b$. Observe that $\sigma_a(\alpha) = bx^2/\alpha$ and $\sigma_b(\alpha) = \alpha$. We may thus define a Galois U_3-algebra structure on $(F_{a,b})_\alpha$ by letting U_3 act on $F_{a,b}$ via $\overline{U}_3$ and by setting

$$\sigma_a(\sqrt{\alpha}) = x\sqrt{b}/\sqrt{\alpha}, \qquad \sigma_b(\sqrt{\alpha}) = \sqrt{\alpha}. \tag{2.1}$$

Exercise 2.1. Verify that $\sigma_a^2 = \sigma_b^2 = [\sigma_a, \sigma_b]^2 = 1$ on $(F_{a,b})_\alpha$, that $(F_{a,b})_\alpha$ is a Galois U_3-algebra and that the subalgebra of Q_3-invariants is $F_{a,b}$.

Verify that replacing x by $-x$ in (2.1) does not change $(F_{a,b})_\alpha$ up to U_3-algebra isomorphism.

Symmetrically, if $\beta \in F_b^\times$ satisfies $N_b(\beta) = ay^2$ for some $y \in F^\times$, the étale F-algebra $(F_{a,b})_\beta$ has structure of a Galois U_3-algebra defined by

$$\sigma_a(\sqrt{\beta}) = \sqrt{\beta}, \qquad \sigma_b(\sqrt{\beta}) = y\sqrt{a}/\sqrt{\beta}. \tag{2.2}$$

Proposition 2.2. *Let $a, b \in F^\times$.*

(1) Every Galois U_3-algebra K over F such that $K^{Z_3} = F_{a,b}$ is of the form $(F_{a,b})_\alpha$ for some $\alpha \in F_a^\times$ with the property $N_a(\alpha) = b$ in $F^\times/F^{\times 2}$ and U_3-algebra structure as in (2.1).

(2) Every Galois U_3-algebra K over F such that $K^{Z_3} = F_{a,b}$ is of the form $(F_{a,b})_\beta$ for some $\beta \in F_b^\times$ with the property $N_b(\beta) = a$ in $F^\times/F^{\times 2}$ and U_3-algebra structure as in (2.2).

Proof. (1) By Proposition 1.17(1), we have $K \cong (F_{a,b})_\alpha$, where $\alpha \in F_a^\times$ satisfies

$$(\sigma_a - 1)\sqrt{\alpha} = \frac{\sqrt{b}}{\theta}, \qquad (\sigma_b - 1)\sqrt{\alpha} = 1$$

for some $\theta \in F_a^\times$; see (1.9). Taking norms, we see that $N_a(\theta) = b$. Moreover,

$$(\sigma_a - 1)\theta = N_a(\theta)/\theta^2 = b/\theta^2 = (\sigma_a - 1)\alpha,$$

and hence α/θ is σ_a-invariant, that is, $\alpha = \theta x$ for some $x \in F^\times$. Thus $N_a(\alpha) = bx^2$, $(\sigma_a - 1)\sqrt{\alpha} = \sqrt{b}/(\alpha/x) = x\sqrt{b}/\alpha$ and $(\sigma_b - 1)\sqrt{\alpha} = 1$, as desired. □

2.2. **Beginning of proof of Theorem 1.13.** We begin the proof of Theorem 1.13. In view of Remark 1.14, we may suppose that $\mathrm{char}(F) \neq 2$, so that Theorem 1.13 may be restated as follows.

Theorem 2.3. *Let F be a field of characteristic different from 2, let $a, b, c, d \in F^\times$, be such that the mod 2 Massey product $\langle a, b, c, d\rangle$ is defined. Then $\langle a, b, c, d\rangle$ vanishes.*

We first show that Theorem 2.3 follows from the next proposition.

Proposition 2.4. *Let $a, d \in F^\times$, $\alpha \in F_a^\times$ and $\delta \in F_d^\times$ be such that*

$$(\alpha, \delta) \in \mathrm{Im}(\mathrm{Br}(F)[2] \to \mathrm{Br}(F_{a,d})[2]).$$

Then there exist $x, y \in F^\times$ such that $(x, N_d(\delta)) = (N_a(\alpha), y) = 0$ in $\mathrm{Br}(F)$ and $(\alpha x, \delta y) = 0$ in $\mathrm{Br}(F_{a,d})$.

Proof of 2.4 ⇒ 2.3. Suppose that $\langle a, b, c, d\rangle$ is defined. We have a homomorphism

$$\overline{\rho} = \begin{bmatrix} 1 & \chi_a & \theta & \epsilon & \square \\ & 1 & \chi_b & \pi & \nu \\ & & 1 & \chi_c & \mu \\ & & & 1 & \chi_d \\ & & & & 1 \end{bmatrix} : \Gamma_F \to \overline{U}_5.$$

By Proposition 1.17(2), we can choose θ so that $\theta|_{\Gamma_a} = \chi_\alpha$, where $\alpha \in F_a^\times$ is such that $N_a(\alpha) = b$ in $F^\times/F^{\times 2}$ and μ so that $\mu|_{\Gamma_d} = \chi_\delta$, where $\delta \in F_d^\times$ is such that $N_d(\delta) = c$ in $F^\times/F^{\times 2}$. The obstruction to lifting to U_5 is equal to

$$\Delta = \chi_a \cup \nu + \theta \cup \mu + \epsilon \cup \chi_d \in \mathrm{Br}(F)[2].$$

As $\chi_a|_{\Gamma_a} = 0$ and $\chi_d|_{\Gamma_d} = 0$, the restriction of Δ to $(F_s)^{\Gamma_{a,d}}$ is equal to

$$\Delta|_{\Gamma_{a,d}} = (\theta|_{\Gamma_{a,d}}) \cup (\mu|_{\Gamma_{a,d}}) = (\alpha, \delta) \in \mathrm{Br}((F_s)^{\Gamma_{a,d}})[2].$$

Thus

$$(\alpha, \delta) \in \mathrm{Im}(\mathrm{Br}(F)[2] \to \mathrm{Br}((F_s)^{\Gamma_{a,d}})[2].$$

Let $x, y \in F^\times$ be so that $(x, c) = (b, y) = 0$. Choose the 1-cochains ϵ' and ν' such that $\partial(\epsilon') = \chi_a \cup \chi_c$ and $\partial(\nu') = \chi_b \cup \chi_y$. Then the map

$$\overline{\rho}' = \begin{bmatrix} 1 & \chi_a & \theta + \theta' & \epsilon + \epsilon' & \square \\ & 1 & \chi_b & \pi & \nu + \nu' \\ & & 1 & \chi_c & \mu + \mu' \\ & & & 1 & \chi_d \\ & & & & 1 \end{bmatrix} : \Gamma_F \to \overline{U}_5$$

is also a homomorphism. The obstruction for lifting $\overline{\rho}'$ to U_5 is the element

$$\Delta' = \chi_a \cup (\nu + \nu') + (\theta + \chi_x) \cup (\mu + \chi_y) + (\epsilon + \epsilon') \cup \chi_d \in \mathrm{Br}(F)[2].$$

We have

$$\Delta'|_{F_{a,d}} = ((\theta + \chi_x)|_{F_{a,d}}) \cup ((\mu + \chi_y)|_{F_{a,d}}) = (\alpha x, \delta y) \in \mathrm{Br}((F_s)^{\Gamma_{a,d}})[2].$$

Note that $(\alpha x, \delta y) = 0$ in $\mathrm{Br}((F_s)^{\Gamma_{a,d}})[2]$ if and only if $(\alpha x, \delta y) = 0$ over $F_{a,d}$. By Proposition 2.4, we can find $\overline{\rho}'$ such that Δ' is split over $F_{a,d}$ and hence Δ' is decomposable: $\Delta' = (a, u) + (v, d)$. Then the map

$$\overline{\rho}'' = \begin{bmatrix} 1 & \chi_a & \theta & \epsilon + \chi_v & \square \\ & 1 & \chi_b & \pi & \nu + \chi_u \\ & & 1 & \chi_c & \mu \\ & & & 1 & \chi_d \\ & & & & 1 \end{bmatrix} : \Gamma_F \to \overline{U}_5$$

is a homomorphism. The obstruction Δ'' to lifting $\overline{\rho}''$ is given by $\Delta' + \chi_a \cup \chi_u + \chi_v \cup \chi_d = 2\Delta' = 0$ in $\mathrm{Br}(F)[2]$. □

Thus Proposition 2.4 implies Theorem 2.3. In turn, Proposition 2.4 is implied by the combination of the next two statements.

Proposition 2.5. *Let $a \in F^\times$, let $\pi, \mu \in F_a^\times$ such that (π, μ) belongs to the image of the restriction $\mathrm{Br}(F)[2] \to \mathrm{Br}(F_a)[2]$. Then there exists $y \in N_a(F_a^\times)$ such that $(\pi, \mu y) = 0$ in $\mathrm{Br}(F_a)$.*

Proposition 2.6. *Let $a, c, d \in F^\times$, let $\alpha \in F_a^\times$, let $\delta \in F_d^\times$ such that $N_d(\delta) = c$ in $F^\times$ and (α, δ) is in the image of $\mathrm{Br}(F)[2] \to \mathrm{Br}(F_{a,d})[2]$. Suppose that c is not a square in $F^\times$. Then there exist $x \in N_c(F_c^\times)$ and $\nu \in F_a^\times$ such that*

$$\begin{aligned} (\alpha x, \delta) &= (\alpha x, \nu) && \text{in } \mathrm{Br}(F_{a,d})[2], \\ N_a(\alpha x, \nu) &= 0 && \text{in } \mathrm{Br}(F)[2]. \end{aligned}$$

We prove 2.5 in this lecture. In the next lecture, we will prove Proposition 2.6, and hence complete the proof of Theorem 1.13.

Proof of Proposition 2.5. Let A be a biquaternion algebra, that is, A is the tensor product of two quaternion algebras (a_1, b_1) and (a_2, b_2), where $a_1, b_1, a_2, b_2 \in F^\times$. The Albert form of A is the quadratic form $q := \langle a_1, b_1, -a_1b_1, -a_2, -b_2, a_2b_2\rangle$. (This is a quadratic form, not a Massey product!) The Albert form of A depends on the presentation of A as $(a_1, b_1) \otimes (a_2, b_2)$, but it is well-defined up to similarity.

Let $w(q)$ be the Witt index of q, that is, the dimension of a maximal totally isotropic subspace of q. By a theorem of Albert, the index of A and the Witt index of q determine each other: In particular A is split if and only if q is hyperbolic.

$\mathrm{ind}(A)$	$w(q)$
4	0
2	1
1	3

Let:

- $s\colon F_a \to F$ be a non-zero F-linear map such that $s(1) = 0$;
- Q be the quaternion algebra (π, μ);
- $Q^\circ \subset Q$ the subspace of pure quaternions;
- $q\colon Q^\circ \to F_a$ be the quadratic form given by $q(x) = x^2$. A computation shows that $q = \langle \pi, \mu, -\pi\mu\rangle$;
- $s_*(q)\colon Q^\circ \to F_a \xrightarrow{s} F$ the Scharlau transfer of q.

By another theorem of Albert, $s_*(q)$ is an Albert form for $N_a(Q)$.

By assumption, $N_a(Q)$ is split, and hence $s_*(q)$ is hyperbolic. Thus $s_*\langle \mu, -\pi\mu\rangle$ is a 4-dimensional subform of a 6-dimensional hyperbolic form. Since $4 > 6/2$, this implies that $s_*\langle \mu, -\pi\mu\rangle$ is isotropic:

$$\text{There exist } p, q \in F_a^\times, \text{ and } z \in F \text{ such that } \mu p^2 - \pi\mu q^2 = z.$$

If $z = 0$, then π is a square and we may take $y = 1$.

If $z \neq 0$, then $(\mu p)^2 - \pi(\mu q)^2 = \mu z$ implies that $\mu z \in F_a^\times$ is a norm from $((F_a)_\pi)^\times$. This is equivalent to $(\pi, \mu z) = 0$ in $\mathrm{Br}(F_a)$. We set $y = z$. Then $(\pi, \mu y) = 0$ and, as (π, μ) comes from $\mathrm{Br}(F)[2]$, we have $N_a(\pi, y) = N_a(\pi, \mu) = 0$, and hence $y = N_a(\pi) \in N_a(F_a^\times)$. □

Remark 2.7. The combination of Proposition 2.4 and Proposition 2.5 immediately implies the Massey Vanishing Conjecture for degenerate fourfold Massey products, that is, Massey products of the form $\langle a, b, c, a\rangle$.

3. Lecture 3. End of proof of Theorem 1.13 and Formal Hilbert 90

3.1. **Specialization in Galois cohomology.** Recall from [Ros96, Remarks 1.11 and 2.5] that the Galois cohomology functor $H^*(-, \mathbb{Z}/2\mathbb{Z})$ from the category of field extensions of F is a cycle module, that is, it satisfies the axioms of [Ros96, Definitions 1.1 and 2.1].

For all integers $n \geq 1$, all regular local F-algebras R of dimension n and all ordered systems of parameters $\pi := (\pi_1, \dots, \pi_n)$ in R, letting K and $K_0 := R/(\pi_1, \dots, \pi_n)$ be the fraction field and residue field of R, respectively, we have a specialization map

$$s_\pi \colon H^*(K, \mathbb{Z}/2\mathbb{Z}) \to H^*(K_0, \mathbb{Z}/2\mathbb{Z}),$$

which is a graded ring homomorphism defined as follows.

Suppose first that $n = 1$, that is, R is a discrete valuation ring and $\pi = (\pi_1)$. Then we set $s_\pi \coloneqq \partial_{\pi_1}((-\pi_1) \cup (-))$, where $\partial_{\pi_1} \colon H^{*+1}(K, \mathbb{Z}/2\mathbb{Z}) \to H^*(K_0, \mathbb{Z}/2\mathbb{Z})$ is the residue map at π_1; see [Ros96, Definition 1.1, below D4].

Suppose now that $n \geq 2$ and that the specialization map has been defined for all regular local F-algebras of dimension $< n$ and all ordered systems of parameters on such algebras. For $i = 2, \dots, n$ let $\overline{\pi}_i \in R/(\pi_1)$ be the reduction of π_i modulo π_1 and set $\overline{\pi} \coloneqq (\overline{\pi}_2, \dots, \overline{\pi}_n)$: it is an ordered system of parameters in the regular local ring $R/(\pi_1)$. Then s_π is defined by $s_\pi \coloneqq s_{\overline{\pi}} \circ s_{(\pi_1)}$, where π_1 is viewed as an element of the localization $R_{(\pi_1)}$.

The ring homomorphism s_π depends on the choice of the ordered set π. Using the isomorphism $H^2(F, \mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{Br}(F)[2]$ coming from Kummer Theory, we obtain a specialization map

$$s_\pi \colon \mathrm{Br}(K)[2] \to \mathrm{Br}(K_0)[2].$$

Let X be an F-variety and $P \in X$ be a regular F-point. For all ordered systems of parameters $\pi = (\pi_1, \dots, \pi_n)$ in the regular local ring $R = O_{X,P}$ the previous discussion yields specialization maps

$$s_{P,\pi} \colon H^*(F(X), \mathbb{Z}/2\mathbb{Z}) \to H^*(F, \mathbb{Z}/2\mathbb{Z}), \qquad s_{P,\pi} \colon \mathrm{Br}(F(X))[2] \to \mathrm{Br}(F)[2].$$

If $f \in O_{X,P}^\times$ (that is, f is regular and nonzero at P) then it follows from the definition that $s_{P,\pi}(f) = (f(P))$. In particular, if $f \in F^\times$ is constant then $s_{P,\pi}(f) = (f)$.

Lemma 3.1. *Let $n \geq 1$ be an integer, X be an n-dimensional F-variety, $P \in X$ be a regular F-point, and $\pi \coloneqq (\pi_1, \dots, \pi_n)$ be an ordered system of parameters in $O_{X,P}$. Let F' be a finite separable field extension of F, let $X' \coloneqq X \times_F F'$, let P' be the only F'-point of X' lying over P, and consider the system of parameters $\pi' \coloneqq (\pi_1 \otimes 1, \dots, \pi_n \otimes 1)$ in the regular local ring $O_{X',P'} = O_{X,P} \otimes_F F'$. Then the following squares commute:*

$$\begin{tikzcd}
H^*(F(X), \mathbb{Z}/2\mathbb{Z}) \arrow[r, "s_{P,\pi}"] \arrow[d, "(-)_{F'(X')}"] & H^*(F, \mathbb{Z}/2\mathbb{Z}) \arrow[d, "(-)_{F'}"] \\
H^*(F'(X'), \mathbb{Z}/2\mathbb{Z}) \arrow[r, "s_{P',\pi'}"] & H^*(F', \mathbb{Z}/2\mathbb{Z})
\end{tikzcd}
\qquad
\begin{tikzcd}
H^*(F'(X'), \mathbb{Z}/2\mathbb{Z}) \arrow[r, "s_{P',\pi'}"] \arrow[d, "N_{F'(X')/F(X)}"] & H^*(F', \mathbb{Z}/2\mathbb{Z}) \arrow[d, "N_{F'/F}"] \\
H^*(F(X), \mathbb{Z}/2\mathbb{Z}) \arrow[r, "s_{P,\pi}"] & H^*(F, \mathbb{Z}/2\mathbb{Z}).
\end{tikzcd}$$

Lemma 3.1 admits an obvious generalization to the case when F' is an étale F-algebra.

Proof. One proves the result by induction on $n \geq 1$; see [MS23a, Lemma 2.9]. □

3.2. **A calculation.** Let F be a field of characteristic different from 2, let c, x_1, x_2, y_1, y_2, u be variables over F. Consider the polynomials

$$\begin{aligned}
d &= u^2 - c, \\
w &= x_1 y_2 + x_2 y_1 \\
h &= x_1 y_1 + u x_1 y_2 + u x_2 y_1 + c x_2 y_2.
\end{aligned}$$

Note that these polynomials are symmetric with respect to the change of variables $x_i \leftrightarrow y_i$.

Proposition 3.2. *Let F be a field of characteristic different from 2, let c, x_1, x_2, y_1, y_2, u be variables over F, and let $L \coloneqq F(c, x_1, x_2, y_1, y_2, u)$. Then we have the following* *equality in* $\mathrm{Br}(L)[2]$*:*

$$\begin{aligned}\Big((x_1^2-cx_2^2)(y_1^2-cy_2^2),2wh\Big) &= \Big(x_1^2-cx_2^2,2x_2(x_1+ux_2)\Big)\\ &+\Big(y_1^2-cy_2^2,2y_2(y_1+uy_2)\Big)\\ &+\Big(d,(x_1+ux_2)(y_1+uy_2)h\Big).\end{aligned}$$

Proof. We have

$$x_2h+(x_1^2-cx_2^2)y_2=w(x_1+ux_2). \tag{3.1}$$

Indeed,

$$\begin{aligned}x_2h+(x_1^2-cx_2^2)y_2 &= x_2(x_1y_1+ux_1y_2+ux_2y_1+cx_2y_2)+(x_1^2-cx_2^2)y_2\\ &=(x_1y_2+x_2y_1)(x_1+ux_2)\\ &=w(x_1+ux_2).\end{aligned}$$

Symmetrically, we get the equality

$$y_2h+(y_1^2-cy_2^2)x_2=w(y_1+uy_2). \tag{3.2}$$

We deduce from (3.1) and (3.2) that

$$(x_1^2-cx_2^2)(y_1^2-cy_2^2)x_2y_2=(w(x_1+ux_2)-x_2h)(w(y_1+uy_2)-y_2h). \tag{3.3}$$

Note that

$$h=(x_1+ux_2)(y_1+uy_2)-dx_2y_2. \tag{3.4}$$

Combining (3.1), (3.2) and (3.4), we get the equality

$$(x_2h+(x_1^2-cx_2^2)y_2)\cdot(y_2h+(y_1^2-cy_2^2)x_2)=w^2(h+dx_2y_2). \tag{3.5}$$

We have

$$x_1^2-cx_2^2=(x_1+ux_2)(x_1-ux_2)+dx_2^2, \tag{3.6}$$

and symmetrically

$$y_1^2-cy_2^2=(y_1+uy_2)(y_1-uy_2)+dy_2^2. \tag{3.7}$$

We prove that the residues of both sides of the equality with respect to every irreducible polynomial $p\in F[c,x_1,x_2,y_1,y_2,u]$ are equal.

1. The cases $p=x_1+ux_2$ (resp. $p=y_1+uy_2$) follow from (3.6) (resp. (3.7)).
2. The cases $p=x_1^2-cx_2^2$ (resp. $p=y_1^2-cy_2^2$) follows from (3.1) (resp. (3.2)).
3. The case $p=h$ follows from (3.5).
4. The case $p=w$ follows from (3.3).
5. The case $p=d$ follows from (3.4).
6. The cases $p=x_2$ (resp. $p=y_2$) are obvious.
7. The case when p is any other polynomial is obvious.

This shows that the two sides differ by a class in the image of $\mathrm{Br}(F)\to\mathrm{Br}(L)$. As the equality holds after specializing $x_2=y_2=0$, the proof is complete. □

3.3. Proof of the Key Proposition 2.6.

Lemma 3.3 (Trace Lemma)**.** *Let $a, b \in F^\times$, $\rho \in F_a^\times$ and $\mu \in F_b^\times$ be such that $N_a(\rho) = N_b(\mu)$. Let $g \coloneqq \mathrm{Tr}_a(\rho) + \mathrm{Tr}_b(\mu) \in F$, and suppose $g \neq 0$. Then $(\mu, a) = (g, a)$ in $\mathrm{Br}(F_b)[2]$.*

Exercise 3.4. Prove Lemma 3.3.

Proof of Proposition 2.6. Since $(\alpha, c) = 0$, there exist $\alpha_1, \alpha_2 \in F_a^\times$ such that

$$\alpha = \alpha_1^2 - c\alpha_2^2.$$

Claim 3.5. We may suppose α_1, α_2 linearly independent over F.

Proof of Claim 3.5. Suppose that α_1 and α_2 are linearly dependent over F, so that there exists $t \in F$ such that either $\alpha_1 = t\alpha_2$ or $\alpha_2 = t\alpha_1$. In the first case $\alpha = (t^2 - c)\alpha_2^2$, and in the second case $\alpha = (1 - ct^2)\alpha_1^2$. Thus, there exist $i \in \{1, 2\}$ and $u \in F^\times$ such that $\alpha = u\alpha_i^2$. Note that $u \in F^\times$ and $\alpha_i \in F_a^\times$ because $\alpha \in F_a^\times$. Letting $x = u$ and $\nu = 1$, we have $(\alpha x, \delta) = (u^2, \delta) = 0$ in $\mathrm{Br}(F_{a,d})$ and $(\alpha x, \nu) = (ux, \nu) = 0$ in $\mathrm{Br}(F_a)$, which proves Proposition 2.6 in this case. □

From now on, we assume that α_1 and α_2 are linearly independent over F. Let $K \coloneqq F(\mathbb{A}^2) = F(x_1, x_2)$, and define

$$f \coloneqq x_1^2 - cx_2^2 \in K^\times.$$

Let

$$h_1 \coloneqq \alpha_1 x_1 + c\alpha_2 x_2 \in K_a^\times, \qquad h_2 \coloneqq \alpha_1 x_2 + \alpha_2 x_1 \in K_a^\times.$$

Let $u_1, u_2 \in F$ be such that

$$\delta = u_1 + u_2\sqrt{d},$$

so that $N_d(\delta) = u_1^2 - du_2^2 = c$. We define the following elements of $F_a^\times$:

$$\beta_1 \coloneqq \alpha_1 + u_1\alpha_2, \qquad \beta_2 \coloneqq u_1\alpha_1 + c\alpha_2, \qquad \theta \coloneqq 2\alpha_2\beta_1.$$

Finally, we define

$$g \coloneqq 2hh_2 \in K_a^\times, \qquad t \coloneqq x_1 + u_1x_2 \in K^\times, \qquad s \coloneqq 2x_2t = 2(x_1x_2 + u_1x_2^2) \in K^\times.$$

Lemma 3.6. *We have $(\alpha, \theta) = (\alpha, \delta)$ and $(\alpha f, g) = (\alpha f, \delta)$ in $\mathrm{Br}(K_{a,d})[2]$.*

Proof. Set $\rho \coloneqq (\alpha_1 + \sqrt{\alpha})\alpha_2{}^{-1}$. We have $N_\alpha(\rho) = c = N_d(\delta)$. The equality

$$\mathrm{Tr}_\alpha(\rho) + \mathrm{Tr}_d(\delta) = 2(\alpha_1\alpha_2^{-1} + u_1) = 2\alpha_2^{-1}\beta_1,$$

and Lemma 3.3 imply that $(\alpha, \theta) = (\alpha, 2\alpha_2\beta_1) = (\alpha, \delta)$ over $F_{a,d}$. The proof that $(\alpha f, g) = (\alpha f, \delta)$ over $K_{a,d}$ is similar. □

Specialization of the equality of Proposition 3.2 at $y_1 = \alpha_1$, $y_2 = \alpha_2$ and $u = u_1$ yields

$$(f\alpha, 2h_2h) = (f, 2x_2t) + (\alpha, 2\alpha_2\beta_1) + (d, t\beta_1 h) \quad \text{in } \mathrm{Br}(K_a)[2],$$

or equivalently

$$(\alpha f, g) + (f, s) + (d, \beta_1 ht) + (\alpha, \theta) = 0 \quad \text{in } \mathrm{Br}(K_a)[2]. \tag{3.8}$$

So far, we have not yet used the fact that (α, δ) comes from $\mathrm{Br}(F)[2]$. Let $A \in \mathrm{Br}(F)[2]$ be such that $(\alpha, \delta) = A_{F_{a,d}}$ over $F_{a,d}$. Applying $N_{K_a/K}$ to (3.8), we get

$$N_{K_a/K}(\alpha f, g) = (d, N_{K_a/K}(h\eta)),$$

where $\eta \coloneqq \epsilon\beta_1 \in F_a^\times$. Let $P = (P_1, P_2) \in \mathbb{A}^2_F$ such that h is regular at P, let $\pi \coloneqq (x_1 - P_1, x_2 - P_2)$ be a system of parameters at P, and define the specializations $x \coloneqq s_\pi(f) \in F^\times$ and $\nu \coloneqq s_\pi(g)$. We specialize the above equation at P via π to obtain

$$N_{F_a/F}(\alpha x, \nu) = (d, N_{F_a/F}(h(P)\eta)).$$

We wish to find P so that the right-hand side is zero. This would be case if we could choose P such that h is regular at P and $h(P) = \eta$. We have

$$\begin{aligned} h(P) = \eta &\iff u_1(\alpha_1 P_2 + \alpha_2 P_1) + (\alpha_1 P_1 + c\alpha_2 P_2) = \eta \\ &\iff (\alpha_1 + u_1\alpha_2)P_1 + (u_1\alpha_1 + c\alpha_2)P_2 = \eta. \end{aligned}$$

Recall that α_1 and α_2 were chosen to be linearly independent over F. Thus it suffices to check that

$$\det \begin{bmatrix} 1 & u_1 \\ u_1 & c \end{bmatrix} = c - u_1^2$$

is not zero. This is true because c is not square in F. Thus we may find P such that $h(P) = \eta$, and the proof is complete. □

4. Lecture 4. Formal Hilbert 90 and non-formality of Galois cohomology

4.1. Formal Hilbert 90.

We wish to examine the following vague question.

Question 4.1. *Is the Massey Vanishing Conjecture a consequence of Hilbert's Theorem 90 alone?*

Here is one way to make this question precise. Let p be a prime number, let Γ be a profinite group, and let $\theta \colon \Gamma \to \mathbb{Z}_p^\times$ be a continuous group homomorphism. We call θ a *p-orientation* of Γ and the pair (Γ, θ) a *p-oriented profinite group*.

We write $\mathbb{Z}_p(1)$ for the topological Γ-module with underlying topological group $\mathbb{Z}_p$ and where Γ acts via θ, that is, $g \cdot v \coloneqq \theta(g)v$ for every $g \in \Gamma$ and every $v \in \mathbb{Z}_p$. For all $n \geq 0$, we set $\mathbb{Z}/p^n\mathbb{Z}(1) \coloneqq \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)$.

Let (Γ, θ) be a p-oriented profinite group. We say that (Γ, θ) *satisfies formal Hilbert 90* if for every open subgroup $H \subset \Gamma$ and all $n \geq 1$ the reduction map $H^1(H, \mathbb{Z}/p^n\mathbb{Z}(1)) \to H^1(H, \mathbb{Z}/p\mathbb{Z}(1))$ is surjective.

Example 4.2. Let F be a field and write Γ_F for the absolute Galois group of F. We define the *canonical p-orientation* θ_F on Γ_F as follows. If $\mathrm{char}(F) \neq p$, we define θ_F as the continuous homomorphism $\theta_F \colon \Gamma_F \to \mathbb{Z}_p^\times$ given by $g(\zeta) = \zeta^{\theta_F(g)}$ for every root of unity ζ of p-power order. If $\mathrm{char}(F) = p$, we let θ_F be the trivial homomorphism. The pair (Γ_F, θ_F) is a p-oriented profinite group.

Exercise 4.3. Let F be a field, let Γ_F be the absolute Galois group of F, and let θ_F be the canonical orientation on Γ_F defined in Example 4.2. Prove that (Γ_F, θ_F) satisfies formal Hilbert 90.

We now may now formulate Question 4.1 in a more precise way.

Question 4.4. *Let p be a prime number, let (Γ, θ) be a p-oriented profinite gruop which satisfies formal Hilbert 90, let $n \geq 3$, and let $\chi_1, \dots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$. If $\langle \chi_1, \dots, \chi_n \rangle$ is defined, does it vanish?*

We prove that Question 4.4 has affirmative answer when $n = 3$, or when $(n, p) = (4, 2)$ and $\chi_1 = \chi_4$ (the degenerate case).

Theorem 4.5. *Let p be a prime number, let (Γ, θ) be a p-oriented profinite group satisfying formal Hilbert 90 and let $\chi_1, \chi_2, \chi_3 \in H^1(\Gamma, \mathbb{Z}/p\mathbb{Z})$. The following are equivalent:*

(1) $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$ in $H^2(\Gamma, \mathbb{Z}/p\mathbb{Z})$;
(2) the mod p Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined;
(3) the mod p Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ vanishes.

Theorem 4.6. *Let (Γ, θ) be a 2-oriented profinite group satisfying formal Hilbert 90 and let $\chi_1, \chi_2, \chi_3 \in H^1(\Gamma, \mathbb{Z}/2\mathbb{Z})$. If the mod 2 Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ is defined, then it vanishes.*

Recall that, in the case of absolute Galois groups, this had been proved by using quadratic forms theory (in particular, the theory of Albert forms associated to biquaternion algebras). Theorem 4.6 generalizes [MS22, Theorem 1.3] and shows that the latter can be proved using Hilbert's Theorem 90 only.

Remark 4.7. We do not know whether Theorem 1.13 can be extended to 2-oriented profinite groups satisfying formal Hilbert 90. The reason is that we do not know how to generalize Proposition 2.5 to this setting.

The group $\mathbb{Z}_p^\times$ acts on the abelian group $\mathbb{Q}/\mathbb{Z}_{(p)}$ by multiplication. We let S be the Γ-module whose underlying abelian group is $\mathbb{Q}/\mathbb{Z}_{(p)}$ and on which Γ acts via θ. For all $n \geq 1$, we have an isomorphism of Γ-modules $\mathbb{Z}/p^n\mathbb{Z}(1) \to S[p^n]$ given by $a + p^n\mathbb{Z} \mapsto a/p^n + \mathbb{Z}_{(p)}$. Therefore, S is the colimit of the $\mathbb{Z}/p^n\mathbb{Z}(1)$ for $n \geq 1$.

The key idea for the proof of Theorems 4.5 and 4.6 is contained in the following definition.

Definition 4.8. Let (Γ, θ) be a p-oriented profinite group. A *Hilbert 90 module* for (Γ, θ) is a discrete Γ-module M such that

(i) $pM = M$,
(ii) $M[p^\infty] \simeq S$ as Γ-modules, and
(iii) $H^1(H, M) = 0$ for any open subgroup $H \subset \Gamma$.

Example 4.9. Let p be a prime number, let F be a field of characteristic different from p, let Γ_F be the absolute Galois group of F, and let θ be the canonical orientation on Γ_F; see Example 4.2. It follows from Hilbert's Theorem 90 that $F_{\mathrm{sep}}^\times$ is a Hilbert 90 module for (Γ_F, θ_F).

It turns out that every p-oriented profinite group satisfying formal Hilbert 90 admits a Hilbert 90 module.

Theorem 4.10. *Let (Γ, θ) be a p-oriented profinite group. Then (Γ, θ) satisfies formal Hilbert 90 if and only if it admits a Hilbert 90 module.*

With Theorem 4.10 at our disposal, one may try to adapt the proofs of the Massey Vanishing Conjecture in the $n = 3$ case or in the degenerate $(n, p) = (4, 2)$ case. In the first case, one must replace the arguments involving central simple algebras split by a $(\mathbb{Z}/p\mathbb{Z})^2$-extension by cocycle arguments. In the second case, the key point is to prove Proposition 2.6 without quadratic form theory. The point is that Proposition 2.6 may be also proved

To help the reader see the point of a Hilbert 90 module, we propose the following exercise.

Exercise 4.11. Let (Γ, θ) be a p-oriented profinite group satisfying formal Hilbert 90, and let M be a Hilbert 90 module for (Γ, θ).

(1) Let $\chi : \Gamma \to \mathbb{Z}/p\mathbb{Z}$ be a character and set $H \coloneqq \mathrm{Ker}(\chi)$. Then the sequence

$$H^1(H, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\mathrm{Cor}} H^1(\Gamma, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup\chi} H^2(\Gamma, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\mathrm{Res}} H^2(H, \mathbb{Z}/p\mathbb{Z})$$

is exact.

(2) Let $a, b \in M^\Gamma$ be such that $\chi_a \cup \chi_b = 0$ in $H^2(\Gamma, \mathbb{Z}/p\mathbb{Z})$. Then there exists $\alpha \in M^{\Gamma_a}$ such that $N_{\Gamma/\Gamma_a}(\alpha) = b$ in M^Γ.

Hint: look at the classical proofs in the case of a field F, and replace the Galois module $(F_s)^\times$ by the Γ-module M.

4.2. **Non-formality of Galois cohomology: Positselski's question.** Let (A, ∂) be a differential graded ring, i.e, $A = \oplus_{i\geq 0} A^i$ is a non-negatively graded abelian group with an associative multiplication which respects the grading, and $\partial \colon A \to A$ is a group homomorphism of degree 1 such that $\partial \circ \partial = 0$ and $\partial(ab) = \partial(a)b + (-1)^i a\partial(b)$ for all $i \geq 0$, $a \in A^i$ and $b \in A$.

We say that A is *formal* if it is quasi-isomorphic as a differential graded ring to $H^*(A)$ with the zero differential, that is, if there exist a differential graded ring B and a diagram

$$A \longleftarrow B \longrightarrow H^*(A),$$

where both maps are quasi-isomorphisms. Loosing speaking, A is formal if no essential information about A is lost when passing to $H^*(A)$.

Hopkins–Wickelgren [HW15] asked whether $C^{\boldsymbol{\cdot}}(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is formal for every field F and every prime p. The authors of [HW15] were unaware of earlier work of Positselski, who had already showed in [Pos10, Section 9.11] that $C^{\boldsymbol{\cdot}}(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is not formal for some finite extensions F of $\mathbb{Q}_\ell$ and $\mathbb{F}_\ell((z))$, where $\ell \neq p$. Positselski then wrote a detailed exposition of his counterexamples in [Pos17].

For Positselski's method to work, it seemed important that F did not contain all the roots of unity of p-power order. This motivated the following question; see [Pos17, p. 226].

Question 4.12 (Positselski)**.** *Does there exist a field F containing all roots of unity of p-power order such that $C^{\boldsymbol{\cdot}}(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is not formal?*

4.3. **Massey products and formality.** Let $n \geq 2$ be an integer and $a_1, \ldots, a_n \in H^1(A)$. A *defining system* for the n-th order Massey product $\langle a_1, \ldots, a_n\rangle$ is a collection M of elements of $a_{ij} \in A^1$, where $1 \leq i < j \leq n+1$, $(i, j) \neq (1, n+1)$, such that

(1) $\partial(a_{i,i+1}) = 0$ and $a_{i,i+1}$ represents a_i in $H^1(A)$, and
(2) $\partial(a_{ij}) = -\sum_{l=i+1}^{j-1} a_{il}a_{lj}$ for all $i < j-1$.

It follows from (2) that $-\sum_{l=2}^{n} a_{1l}a_{l,n+1}$ is a 2-cocycle: we write $\langle a_1, \ldots, a_n\rangle_M$ for its cohomology class in $H^2(A)$, called the *value* of $\langle a_1, \ldots, a_n\rangle$ corresponding to M.

Definition 4.13. The *Massey product* of $a_1, \ldots, a_n$ is the subset $\langle a_1, \ldots, a_n\rangle$ of $H^2(A)$ consisting of the values $\langle a_1, \ldots, a_n\rangle_M$ of all defining systems M. We say that the Massey product $\langle a_1, \ldots, a_n\rangle$ is *defined* if it is non-empty, and that it *vanishes* if $0 \in \langle a_1, \ldots, a_n\rangle$.

By a theorem of Dwyer [Dwy75], this definition reduces to Definition 1.3 when A is the cochain DGA of a profinite group.

Lemma 4.14. *Let (A, ∂) be a differential graded ring, let $n \geq 3$ be an integer, and let $a_1, \dots, a_n$ be elements of $H^1(A)$ satisfying $a_i \cup a_{i+1} = 0$ for all $1 \leq i \leq n-1$. If A is formal, then $\langle a_1, \dots, a_n \rangle$ vanishes.*

Proof. See [PQ22, Theorem 3.8]. □

Exercise 4.15. Find a direct proof of Lemma 4.14 in the case $n = 4$. (This is the only case that we will need.)

Recall that the Massey Vanishing Conjecture asks whether the first implication of (1.5) can be reversed for absolute Galois groups. It is natural to wonder whether both implications of (1.5) can be reversed for absolute Galois groups; see [PS18, Definition 1.3].

Question 4.16 (Strong Massey Vanishing (Mináč–Tân))**.** *Let F be a field, let $n \geq 3$ be an integer, let p be a prime number, and let $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$ be such that $\chi_i \cup \chi_{i+1} = 0$ for all $i = 1, \dots, n$. Does $\langle \chi_1, \dots, \chi_n \rangle$ vanish?*

If Strong Massey Vanishing is true for F, then the Massey Vanishing Conjecture holds for F. Moreover, if F is a field for which the Strong Massey Vanishing Conjecture fails, for some $n \geq 3$ and some prime p, then $C^\cdot(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ is not formal. However, as shown by Harpaz and Wittenberg [GMT18, Example A.15], Strong Massey Vanishing does not always hold.

Example 4.17 (Harpaz–Wittenberg)**.** Strong Massey Vanishing fails for $F = \mathbb{Q}$, $n = 4$, and $p = 2$. More precisely, if we let $b = 2$, $c = 17$ and $a = d = bc = 34$, then $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(\mathbb{Q})$ but $\langle a, b, c, d \rangle$ is not defined over $\mathbb{Q}$.

In [MS22, Theorem 1.4], we have generalized the Harpaz–Wittenberg example to arbitrary fields as follows.

Theorem 4.18 (Merkurjev–Scavia)**.** *Let $p = 2$, let F be a field of characteristic different from 2, and let $b, c \in F^\times$. The following are equivalent:*

(1) the Massey product $\langle bc, b, c, bc \rangle$ is defined,
(2) the Massey product $\langle bc, b, c, bc \rangle$ vanishes,
(3) $(b, c) = 0$ in $\mathrm{Br}(F)$ and $-1 \in N_{b,c}(F^\times_{b,c})$.

Theorem 4.18 does not imply Theorem 4.19. Indeed, if F contains a primitive 8-th root of unity ζ_8, then $-1 = N_{b,c}(\zeta_8) \in N_{b,c}(F^\times_{b,c})$, and hence if $(b, c) = 0$ then $\langle bc, b, c, bc \rangle$ vanishes by Theorem 4.18.

Nevertheless, we showed in [MS23b] that Question 4.12 has negative answer.

Theorem 4.19. *Let p be a prime number and let F be a field of characteristic different from p. There exists a field L containing F such that the differential graded ring $C^\cdot(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$ is not formal.*

This is a consequence of the next more precise result.

Theorem 4.20. *Let p be a prime number, let F be a field of characteristic different from p. There exist a field L containing F and $\chi_1, \chi_2, \chi_3, \chi_4 \in H^1(L, \mathbb{Z}/p\mathbb{Z})$ such that $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \chi_3 \cup \chi_4 = 0$ in $H^2(L, \mathbb{Z}/p\mathbb{Z})$ but $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle$ is not defined. Thus the Strong Massey Vanishing conjecture at $n = 4$ and the prime p fails for L, and $C^\cdot(\Gamma_L, \mathbb{Z}/p\mathbb{Z})$ is not formal.*

The field L is a function field over F. Replacing F by a finite extension if necessary, we may suppose that F contains a primitive p-th root of unity ζ. Let $E \coloneqq F(x,y)$, where x and y are independent variables over F, let X be the Severi-Brauer variety of the degree-p cyclic algebra (x,y) over E, and let $L \coloneqq E(X)$. Consider the following elements of $E^\times$:

$$a \coloneqq 1-x, \quad b \coloneqq x, \quad c \coloneqq y, \quad d \coloneqq 1-y.$$

We have $(a,b) = (c,d) = 0$ in $\mathrm{Br}(E)$ by the Steinberg relations [Ser79, Chapter XIV, Proposition 4(iv)], and hence $(a,b) = (b,c) = 0$ in $\mathrm{Br}(L)$. Moreover, $(b,c) \neq 0$ in $\mathrm{Br}(E)$ because the residue of (b,c) along $x = 0$ is non-zero, while $(b,c) = 0$ in $\mathrm{Br}(L)$ by [GS17, Theorem 5.4.1]. Thus $(a,b) = (b,c) = (c,d) = 0$ in $\mathrm{Br}(L)$. In order to prove Theorem 4.20, it suffices to prove that $\langle a,b,c,d\rangle$ is not defined. We summarize the main steps of the proof.

The first step is to find an equivalent condition for the property "$\langle a,b,c,d\rangle$ is defined".

Proposition 4.21. *Let p be a prime number, let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, and let $a,b,c,d \in F^\times$. The mod p Massey product $\langle a,b,c,d\rangle$ is defined if and only if there exist $u \in F_{a,c}^\times$, $v \in F_{b,d}^\times$ and $w_0 \in F_{b,c}^\times$ such that*

$$N_a(u) \cdot N_d(v) = w_0^p, \qquad (\sigma_b - 1)(\sigma_c - 1)w_0 = \zeta.$$

We refer to [MS23b, Proposition 3.7] for the complete proof of Proposition 4.21. The idea is the following. The Massey product $\langle a,b,c,d\rangle$ is defined if and only if there exists a Galois $\overline{U}_5$-algebra L/F with induced $(\mathbb{Z}/p\mathbb{Z})^4$-algebra $F_{a,b,c,d}/F$. Contemplating the following picture of $\overline{U}_5$

$$\begin{array}{ccccc} 1 & * & * & * & \\ 0 & 1 & * & * & * \\ 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 1 \end{array} \tag{4.1}$$

we see that this is equivalent to the existence of a U_4-algebra inducing $F_{a,b,c}/F$ (top-left 4×4 square), a U_4-algebra inducing $F_{b,c,d}/F$ (bottom-right 4×4 square), and an isomorphism of the induced U_3-algebras (central 3×3 square). The strategy is to parametrize all possibilities for the U_4-algebras, and to impose the condition that they agree on the common U_3 square. Loosely speaking, u corresponds to the upper U_4-square, v to the bottom U_4-square, and w_0 to the fact that the two U_4-squares agree on the common U_3-square.

Once Proposition 4.21 is established, elementary calculations yield the following.

Corollary 4.22. *Let p be a prime, let F be a field of characteristic different from p and containing a primitive p-th root of unity ζ, let $a,b,c,d \in F^\times$, and suppose that $\langle a,b,c,d\rangle$ is defined over F. For every $w \in F_{b,c}^\times$ such that $(\sigma_b - 1)(\sigma_c - 1)w = \zeta$, there exist $u \in F_{a,c}^\times$ and $v \in F_{b,d}^\times$ such that $N_a(u)N_d(v) = w^p$.*

We can rephrase this corollary as follows. Let $\mathcal{T}$ be the kernel of the homomorphism of E-tori

$$R_{a,c}(\mathbb{G}_m) \times R_{b,d}(\mathbb{G}_m) \to R_{b,c}(\mathbb{G}_m), \qquad (u,v) \mapsto N_a(u)N_d(v) = 1.$$

Then $\mathcal{T}$ is an F-torus, that is, it is connected. Given $w \in F_{b,c}^{\times}$ such that $(\sigma_b - 1)(\sigma_c - 1)w = \zeta$, the Massey product $\langle a, b, c, d\rangle$ is defined if and only if the T-torsor $E_w \subset R_{a,c}(\mathbb{G}_m) \times R_{b,d}(\mathbb{G}_m)$ given by $N_a(u)N_d(v) = w^p$ is split.

More generally, suppose that T is a torus over a field F, let K be a Galois field extension of F such that T_K is split, and let $G = \mathrm{Gal}(K/F)$. We have an exact sequence of G-modules

$$1 \to T(K) \to T(K(X)) \xrightarrow{\mathrm{div}} \mathrm{Div}(X_K) \otimes T_* \xrightarrow{\deg} T_* \to 0, \tag{4.2}$$

where T_* denotes the cocharacter lattice of T. We consider the subgroup of unramified torsors

$$H^1(G, T(K(X)))_{\mathrm{nr}} := \mathrm{Ker}[H^1(G, T(K(X))) \xrightarrow{\mathrm{div}} H^1(G, \mathrm{Div}(X_K \otimes T_*))],$$

and the homomorphism

$$\theta \colon H^1(G, T(K(X)))_{\mathrm{nr}} \to \mathrm{Coker}[(\mathrm{Div}(X_K) \otimes T_*)^G \xrightarrow{\deg} (T_*)^G],$$

induced by (4.2). It turns out that it is possible to compute θ explicitly in terms of any short exact sequence

$$1 \to T \to P \to S \to 1$$

where P is a quasi-trivial torus.

In our situation, we have $F = E$, $\mathcal{T} = T$, $K = E_{a,b,c,d}$, and $P = R_{a,c}(\mathbb{G}_m) \times R_{b,d}(\mathbb{G}_m) \to R_{b,c}(\mathbb{G}_m)$. Using the above setup, we show that the T_L-torsor E_w is unramified and that $\theta([E_w]) \neq 0$. In fact, in our example the codomain is $\mathbb{Z}/p\mathbb{Z}$ and $\theta([E_w])$ is a generator. Therefore E_w is non-trivial, and hence $\langle a, b, c, d\rangle$ is not defined.

References

[Dwy75] William G. Dwyer. Homology, Massey products and maps between groups. *J. Pure Appl. Algebra*, 6(2):177–190, 1975. 2, 18

[EM17] Ido Efrat and Eliyahu Matzri. Triple Massey products and absolute Galois groups. *J. Eur. Math. Soc. (JEMS)*, 19(12):3629–3640, 2017. 5

[GMT18] Pierre Guillot, Ján Mináč, and Adam Topaz. Four-fold Massey products in Galois cohomology. *Compos. Math.*, 154(9):1921–1959, 2018. With an appendix by Olivier Wittenberg. 5, 19

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition. 20

[HW15] Michael J. Hopkins and Kirsten G. Wickelgren. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra*, 219(5):1304–1319, 2015. 5, 18

[HW23] Yonatan Harpaz and Olivier Wittenberg. The Massey vanishing conjecture for number fields. *Duke Math. J.*, 172(1):1–41, 2023. 5

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. 6

[Mas58] W. S. Massey. Some higher order cohomology operations. In *Symposium internacional de topología algebraica International symposium on algebraic topology*, pages 145–154. Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958. 1

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[MS22] Alexander Merkurjev and Federico Scavia. Degenerate fourfold Massey products over arbitrary fields. *arXiv preprint arXiv:2208.13011*, 2022. 17, 19

[MS23a] Alexander Merkurjev and Federico Scavia. The massey vanishing conjecture for fourfold massey products modulo 2. *arXiv preprint arXiv:2301.09290*, 2023. 5, 13

[MS23b] Alexander Merkurjev and Federico Scavia. Non-formality of galois cohomology modulo all primes. *arXiv preprint arXiv:2309.17004*, 2023. 19, 20

[MS23c] Alexander Merkurjev and Federico Scavia. On the massey vanishing conjecture and formal hilbert 90. *arXiv preprint arXiv:2308.13682*, 2023. 4

[MT15] Ján Mináč and Nguyen Duy Tân. Triple Massey products over global fields. *Doc. Math.*, 20:1467–1480, 2015. 5

[MT16] Ján Mináč and Nguyen Duy Tân. Triple Massey products vanish over all fields. *J. Lond. Math. Soc. (2)*, 94(3):909–932, 2016. 8

[MT17] Ján Mináč and Nguyen Duy Tân. Triple Massey products and Galois theory. *J. Eur. Math. Soc. (JEMS)*, 19(1):255–284, 2017. 4, 5

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[PS18] Ambrus Pál and Endre Szabó. The strong Massey vanishing conjecture for fields with virtual cohomological dimension at most 1. *arXiv:1811.06192* (2018). 19

[Pos10] Leonid Positselski. Mixed artin-tate motives with finite coefficients. *arXiv preprint arXiv:1006.4343*, 2010. 18

[Pos17] Leonid Positselski. Koszulity of cohomology = $K(\pi, 1)$-ness + quasi-formality. *J. Algebra*, 483:188–229, 2017. 18

[PQ22] Ambrus Pal and Gereon Quick. Real projective groups are formal. *arXiv preprint arXiv:2206.14645*, 2022. 19

[Ros96] Markus Rost. Chow groups with coefficients. *Doc. Math.*, 1:No. 16, 319–393, 1996. 12, 13

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 6, 20

Department of Mathematics, University of California, Los Angeles, CA 90095, United States of America

Email address: merkurev@math.ucla.edu

Institut Galilée, Université Sorbonne Paris Nord, CNRS, 93430, Villetaneuse, France

Email address: scavia@math.univ-paris13.fr