MASSEY PRODUCTS AND ELLIPTIC CURVES

FRAUKE M. BLEHER, TED CHINBURG, AND JEAN GILLIBERT

Abstract. We study the vanishing of Massey products of order at least 3 for absolutely irreducible smooth projective curves over a perfect field with coefficients in $\mathbb{Z}/\ell$. We mainly focus on elliptic curves, for which we obtain a complete characterization of when triple Massey products do not vanish.

1. Introduction

This paper has to do with the vanishing of triple Massey products on $\mathrm{H}^1(X, \mathbb{Z}/\ell)$ when ℓ is an odd prime and X is an absolutely irreducible smooth projective variety over a perfect field F in which ℓ is invertible. When $d = \dim(X) = 0$, Minac and Tan showed in [19] that this triple product always vanishes for arbitrary F, following earlier work by Hopkins and Wickelgren [10], Matzri [14], Efrat and Matzri [6] and others. When $d = 0$ and F is a number field, Harpaz and Wittenberg showed in [9] that all Massey products of order at least 3 vanish. For a more detailed account of the case $d = 0$ see the introduction of [9]. Ekedahl gave an example in [7] showing that the triple Massey product need not vanish when $d = 2$ and $F = \mathbb{C}$.

The present paper arose from the problem of determining when triple Massey products vanish when $d = 1$, i.e. for curves over an arbitrary perfect field F. Our main result classifies exactly which triple Massey products do not vanish when $X = E$ is an elliptic curve over F and the ℓ-torsion of E over an algebraic closure $\overline{F}$ of F is defined over F. We show that the only case in which these do not vanish is when $\ell = 3$ and the three elements of $\mathrm{H}^1(X, \mathbb{Z}/\ell)$ generate the same one-dimensional space (see Lemma 5.1). The classification when $\ell = 3$ of non-vanishing triple Massey products is given in Theorem 5.3. One consequence is the following result, where $G_F^{(3)}$ denotes the pro-3 completion of $\mathrm{Gal}(\overline{F}/F)$:

Theorem 1.1. *Let F be a field whose characteristic is not 3, and let E be an elliptic curve over F such that the 3-torsion of $E(\overline{F})$ is defined over F. There exists a character $\chi \in \mathrm{H}^1(E, \mathbb{Z}/3) = \mathrm{Hom}(\pi_1(E), \mathbb{Z}/3)$ such that $\langle \chi, \chi, \chi \rangle$ does not contain zero if and only if either*

(i) *the action of $G_F^{(3)}$ on $\overline{E}[9]$ is not given by multiplication by scalars in $(\mathbb{Z}/9)^\times$, or*
(ii) *the action of $G_F^{(3)}$ on $\overline{E}[9]$ is given by multiplication by scalars in $(\mathbb{Z}/9)^\times$ and there exists a primitive ninth root $\zeta \in \overline{F}$ such that $\zeta \notin F$ and $F(\zeta)$ is not the only cubic extension of F inside $\overline{F}$.*

As an explicit example, suppose F is a number field containing $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ that does not contain a primitive ninth root of unity. When E is the elliptic curve over F with model $y^2 = x^3 - 1$, there is a character $\chi \in \mathrm{H}^1(E, \mathbb{Z}/3)$ with non-vanishing triple Massey product (see Example 6.2).

We now describe the contents of the paper. In §2 we recall some basic results about Galois and étale cohomology and about Massey products. In §3 we show that higher Massey products on curves over algebraically closed fields always contain 0 provided they are not empty. In §4 we prove some necessary

Date: July 11, 2022.

2010 *Mathematics Subject Classification.* 14F20 (Primary) 55S30, 14H52 (Secondary).

Key words and phrases. Massey products, étale cohomology, smooth projective curves, elliptic curves.

The first author was supported in part by NSF Grant No. DMS-1801328.

The second author was supported in part by NSF SaTC grant No. CNS-1701785.

The third author is the corresponding author. He was supported in part by the CIMI Labex.

conditions for higher Massey products to be non-empty and to not contain 0. In §5 we prove our main results, Theorem 5.3 and Theorem 1.1, concerning triple Massey products when $X = E$ is an elliptic curve. In §6 we analyze two families of examples arising from specializing the Legendre family of elliptic curves and from CM elliptic curves. Finally in §7 we treat arbitrary elliptic curves E when F is a finite field without the assumption that the ℓ-torsion of $E(\overline{F})$ is defined over F.

Acknowledgements. The first and second authors would like to thank the University of Toulouse for its support and hospitality during work on this paper.

2. Preliminaries

Let F be a perfect field with a fixed algebraic closure $\overline{F}$, and let X be a smooth projective geometrically irreducible curve over F. Let ℓ be a prime number that is invertible in F. Let $\pi_1(X, \eta)$ denote the étale fundamental group of X with respect to some geometric base point η on X. We always have a natural isomorphism of first cohomology groups

$$\mathrm{H}^1(X, \mathbb{Z}/\ell) \cong \mathrm{H}^1(\pi_1(X, \eta), \mathbb{Z}/\ell).$$

For higher cohomology groups, we have the following result from [1, §2.1.2] (see also [2, §3]):

Proposition 2.1. *If $X \otimes_F \overline{F}$ is not isomorphic to $\mathbb{P}^1_{\overline{F}}$ then there is a natural isomorphism*

$$\mathrm{H}^i(X, \mathbb{Z}/\ell) \cong \mathrm{H}^i(\pi_1(X, \eta), \mathbb{Z}/\ell)$$

for all $i \geq 1$.

For the remainder of the paper we assume that $\overline{X} = X \otimes_F \overline{F}$ is not isomorphic to $\mathbb{P}^1_{\overline{F}}$, and we identify $\mathrm{H}^i(X, \mathbb{Z}/\ell) = \mathrm{H}^i(\pi_1(X, \eta), \mathbb{Z}/\ell)$ for all $i \geq 1$. Moreover, we let η be a geometric point of $\overline{X}$, which can then also be viewed as a geometric point of X, and we write $\pi_1(X) := \pi_1(X, \eta)$ and $\pi_1(\overline{X}) := \pi_1(\overline{X}, \eta)$ to simplify notation.

We use the following definition of Massey products from [13, §1].

Definition 2.2. Let $t \geq 2$ be an integer, and let $\chi_1, \ldots, \chi_t \in \mathrm{H}^1(X, \mathbb{Z}/\ell) = \mathrm{Hom}(\pi_1(X), \mathbb{Z}/\ell)$. The t-fold Massey product $\langle \chi_1, \ldots, \chi_t \rangle$ is the subset of $\mathrm{H}^2(X, \mathbb{Z}/\ell)$ consisting of the classes of all 2-cocycles ν for which there exists a collection of continuous maps $\kappa_{i,j} : \pi_1(X) \longrightarrow \mathbb{Z}/\ell$, $1 \leq i \leq j \leq t$, $(i, j) \neq (1, t)$, such that

(i) $\kappa_{i,i} = \chi_i$ for $1 \leq i \leq t$, and
(ii) $(\delta\kappa_{i,j})(\sigma, \tau) = -\sum_{r=i}^{j-1} \kappa_{1,r}(\sigma)\, \kappa_{r+1,j}(\tau)$ for all $\sigma, \tau \in \pi_1(X)$, when $1 \leq i < j \leq t$, $(i, j) \neq (1, t)$, and
(iii) $\nu(\sigma, \tau) = -\sum_{r=1}^{t-1} \kappa_{1,r}(\sigma)\, \kappa_{r+1,t}(\tau)$ for all $\sigma, \tau \in \pi_1(X)$.

Any collection of continuous maps $\{\kappa_{i,j}\}$ satisfying (i)-(iii) is called a defining system for $\langle \chi_1, \ldots, \chi_t \rangle$.

Massey products generalize cup products, since if $t = 2$ then the only defining system for $\langle \chi_1, \chi_2 \rangle$ is $\{\chi_1, \chi_2\}$, and $\langle \chi_1, \chi_2 \rangle = \{-\chi_1 \cup \chi_2\}$.

The definition of Massey products can be motivated as follows. Let $U_{t+1}(\mathbb{Z}/\ell)$ be the group of upper triangular unipotent (a.k.a. unitriangular) matrices of dimension $t+1$ with entries in $\mathbb{Z}/\ell$, and let $Z(U_{t+1}(\mathbb{Z}/\ell))$ be its center, which consists of the unitriangular matrices for which all entries above the main diagonal that are not at the $(1, t+1)$ position are zero. The data of a defining system is equivalent to giving a continuous

group homomorphism

$$\begin{array}{rccc} \vartheta: & \pi_1(X) & \longrightarrow & U_{t+1}(\mathbb{Z}/\ell)/Z(U_{t+1}(\mathbb{Z}/\ell)) \\ & & & \\ & \sigma & \mapsto & \begin{pmatrix} 1 & \kappa_{1,1}(\sigma) & \cdots & \kappa_{1,t-1}(\sigma) & * \\ 0 & 1 & \kappa_{2,2}(\sigma) & \cdots & \kappa_{2,t}(\sigma) \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & \kappa_{t,t}(\sigma) \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} \end{array} \tag{2.1}$$

with $\kappa_{i,i}$ being the character χ_i for all i. There is a continuous group homomorphism $\rho = \rho(\vartheta) : \pi_1(X) \longrightarrow U_{t+1}(\mathbb{Z}/\ell)$ lifting ϑ if and only if the 2-cocycle ν is the coboundary of a continuous function $\kappa_{1,t} : \pi_1(X) \longrightarrow \mathbb{Z}/\ell$. Thus $\langle \chi_1, \ldots, \chi_t \rangle$ is not empty if and only if a homomorphism ϑ as in (2.1) exists, and $\langle \chi_1, \ldots, \chi_t \rangle$ contains 0 if and only if there is such a ϑ that has a lift $\rho(\vartheta)$ to $U_{t+1}(\mathbb{Z}/\ell)$. For more details, see [5, Thm. 2.4] and also [18, Lemma 4.2].

We now summarize some useful properties of Massey products.

Let $t \geq 2$, and let $\chi_1, \ldots, \chi_t \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$ be non-zero characters such that the t-fold Massey product $\langle \chi_1, \ldots, \chi_t \rangle$ is not empty.

By [13, (2.3)], we have for all $c_1, \ldots, c_t \in (\mathbb{Z}/\ell)^\times$ that

$$\langle c_1\chi_1, \ldots, c_t\chi_t \rangle \supseteq (c_1 \cdots c_t) \langle \chi_1, \ldots, \chi_t \rangle. \tag{2.2}$$

Writing $\chi_i = c_i^{-1}(c_i\chi_i)$, for $1 \leq i \leq t$, and applying (2.2) again, we obtain

$$\langle c_1\chi_1, \ldots, c_t\chi_t \rangle = (c_1 \cdots c_t) \langle \chi_1, \ldots, \chi_t \rangle. \tag{2.3}$$

In particular, if $\chi \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$ is a single non-zero character and $a_1, \ldots, a_t \in (\mathbb{Z}/\ell)^\times$, then

$$\langle a_1\chi, \ldots, a_t\chi \rangle \quad \text{contains } 0 \quad \text{if and only if} \quad \langle \underbrace{\chi, \ldots, \chi}_{t \text{ copies}} \rangle \quad \text{contains } 0. \tag{2.4}$$

Because of (2.4), it is useful to introduce a "restricted" t-fold Massey product when all characters are the same (see [13, §3]). Namely, when all of $\chi_1, \ldots, \chi_t$ equal a single character χ, then the restricted t-fold Massey product

$$\langle \chi \rangle^t \subseteq \langle \underbrace{\chi, \ldots, \chi}_{t \text{ copies}} \rangle \tag{2.5}$$

is defined to be the subset of $\mathrm{H}^2(X, \mathbb{Z}/\ell)$ consisting of the classes of all 2-cocycles ν as in Definition 2.2 that are associated to defining systems for which the functions $\kappa_{i,j}$ only depend on $i + j$, for $1 \leq i < j \leq t$, $(i, j) \neq (1, t)$. If $t = \ell$, then it follows from [13, Thm. 14] that $\langle \chi \rangle^\ell$ is non-empty and a singleton given by

$$\langle \chi \rangle^\ell = \{-\beta(\chi)\} \tag{2.6}$$

where β is the Bockstein operator associated to the exact sequence

$$0 \longrightarrow \mathbb{Z}/\ell \longrightarrow \mathbb{Z}/\ell^2 \longrightarrow \mathbb{Z}/\ell \longrightarrow 0.$$

In later sections, we will focus on triple Massey products. These are easier to describe than general Massey products, as highlighted in the following remark.

Remark 2.3. Let $\chi_1, \chi_2, \chi_3 \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$. Then the triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is not empty if and only if $\chi_1 \cup \chi_2 = 0 = \chi_2 \cup \chi_3$ in $\mathrm{H}^2(X, \mathbb{Z}/\ell)$. Suppose $\kappa = \{\kappa_{1,1}, \kappa_{1,2}, \kappa_{2,2}, \kappa_{2,3}, \kappa_{3,3}\}$ is a defining system for $\langle \chi_1, \chi_2, \chi_3 \rangle$. In particular, $\kappa_{i,i} = \chi_i$ for $1 \leq i \leq 3$. Then all defining systems can be obtained from κ by

adding a continuous homomorphism $f_{1,2} : \pi_1(X) \longrightarrow \mathbb{Z}/\ell$ to $\kappa_{1,2}$ or by adding a continuous homomorphism $f_{2,3} : \pi_1(X) \longrightarrow \mathbb{Z}/\ell$ to $\kappa_{2,3}$ (or both). This means that the 2-cocycle ν, with

$$\nu(\sigma,\tau) = -\kappa_{1,1}(\sigma)\kappa_{2,3}(\tau) - \kappa_{1,2}(\sigma)\kappa_{3,3}(\tau) = -\chi_1(\sigma)\kappa_{2,3}(\tau) - \kappa_{1,2}(\sigma)\chi_3(\tau)$$

for all $\sigma, \tau \in \pi_1(X)$, gives a single well-defined element $[\nu]$ in the quotient group

$$\frac{\mathrm{H}^2(X,\mathbb{Z}/\ell)}{\mathrm{H}^1(X,\mathbb{Z}/\ell)\cup\chi_3 + \chi_1 \cup \mathrm{H}^1(X,\mathbb{Z}/\ell)}. \tag{2.7}$$

In particular, $\langle \chi_1, \chi_2, \chi_3\rangle$ contains 0 if and only if $[\nu]$ is the identity element of the quotient group (2.7).

In the next remark we summarize some important properties of the group $U_4(\mathbb{Z}/\ell)$ of unitriangular 4×4 matrices over $\mathbb{Z}/\ell$ that we will need in later sections.

Remark 2.4. Let $\ell \geq 3$ and let

$$M = M(a_1,a_2,a_3,u,v,w) := \begin{pmatrix} 1 & a_1 & u & v \\ 0 & 1 & a_2 & w \\ 0 & 0 & 1 & a_3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.8}$$

in $U_4(\mathbb{Z}/\ell)$ for $a_1, a_2, a_3, u, v, w \in \mathbb{Z}/\ell$. It is well known that

$$M^\ell = \begin{pmatrix} 1 & \ell a_1 & \ell u + \binom{\ell}{2} a_1 a_2 & \ell v + \binom{\ell}{2} a_1 w + \binom{\ell}{2} a_3 u + \binom{\ell}{3} a_1 a_2 a_3 \\ 0 & 1 & \ell a_2 & \ell w + \binom{\ell}{2} a_2 a_3 \\ 0 & 0 & 1 & \ell a_3 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.9}$$

In particular, if $\ell > 3$ then every non-identity element of $U_4(\mathbb{Z}/\ell)$ has order ℓ. On the other hand, $U_4(\mathbb{Z}/3)$ contains elements of order 9, which are precisely the matrices M in (2.8) with $a_1a_2a_3 \neq 0$.

For $\ell \geq 3$, we have the following formula of the commutator $[M, \tilde{M}] = M\tilde{M}M^{-1}\tilde{M}^{-1}$ when M is above and $\tilde{M} = M(\tilde{a}_1, \tilde{a}_2, \tilde{a}_3, \tilde{u}, \tilde{v}, \tilde{w})$:

$$[M,\tilde{M}] = \begin{pmatrix} 1 & 0 & a_1\tilde{a}_2 - a_2\tilde{a}_1 & (a_1\tilde{w} - w\tilde{a}_1) - (a_3\tilde{u} - \tilde{a}_3 u) - (a_1\tilde{a}_2 - a_2\tilde{a}_1)(a_3 + \tilde{a}_3) \\ 0 & 1 & 0 & a_2\tilde{a}_3 - a_3\tilde{a}_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.10}$$

In particular, the commutator subgroup H_1 of $U_4(\mathbb{Z}/\ell)$ is the subgroup of matrices M as in (2.8) for which $a_1 = a_2 = a_3 = 0$. It follows from (2.10) that H_1 is an abelian subgroup of $U_4(\mathbb{Z}/\ell)$, which means that the second derived subgroup of $U_4(\mathbb{Z}/\ell)$ is trivial. As usual, the center of $U_4(\mathbb{Z}/\ell)$ consists of all matrices M as in (2.8) with $a_1 = a_2 = a_3 = u = w = 0$.

When $\ell = 3$, we will also need the subgroup H of $U_4(\mathbb{Z}/3)$ consisting of all matrices of the form

$$N = N(a,u,v,w) := \begin{pmatrix} 1 & a & u & v \\ 0 & 1 & a & w \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.11}$$

In particular, $H_1 \leq H$. It follows that the matrices of order 9 in H are precisely the matrices in $H - H_1$. By (2.10), the center of H consists of all matrices N as in (2.11) with $a = 0$ and $u = w$. Moreover, the commutator subgroup H' of H is the subgroup of $Z(H)$ consisting of all matrices N as in (2.11) with $a = 0$ and $u = w = 0$.

The following result on cup products will be important in the next sections.

Lemma 2.5. *Let $\chi, \psi \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$ with restrictions $\overline{\chi}, \overline{\psi}$ to $\mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$. Suppose $\overline{\chi} = 0$, $\chi \neq 0$, and $\chi \cup \psi = 0$. If the ℓ-torsion $\mathrm{Pic}(\overline{X})[\ell]$ is defined over F, then $\overline{\psi} = 0$.*

Proof. Suppose by way of contradiction that $\overline{\psi} \neq 0$. Since $\chi \cup \psi = 0$, there exists a continuous function $\kappa : \pi_1(X) \longrightarrow \mathbb{Z}/\ell$ such that

$$\begin{array}{rccc} \rho: & \pi_1(X) & \longrightarrow & U_3(\mathbb{Z}/\ell) \\ & g & \mapsto & \begin{pmatrix} 1 & \chi(g) & \kappa(g) \\ 0 & 1 & \psi(g) \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

is a continuous group homomorphism. Since $\overline{\chi} = 0$ but $\overline{\psi} \neq 0$, ψ is not in the group of characters generated by χ. Hence the image of ρ surjects onto the quotient of $U_3(\mathbb{Z}/\ell)$ by its center. If ρ is not surjective then the image of ρ has order ℓ^2 so is abelian. Since $U_3(\mathbb{Z}/\ell)$ is generated by this image and its center, this would force $U_3(\mathbb{Z}/\ell)$ to be abelian, which is a contradiction. So ρ is surjective, and in particular the image of ρ is not abelian.

Since $\overline{\chi} = 0$, the image $\rho(\pi_1(\overline{X}))$ lies in an elementary abelian ℓ-subgroup of $U_3(\mathbb{Z}/\ell)$. Since $\pi_1(\overline{X})$ is a normal subgroup of $\pi_1(X)$ and ρ is surjective, it follows that $\rho(\pi_1(\overline{X}))$ is a normal subgroup of $U_3(\mathbb{Z}/\ell)$. Moreover, $\overline{\chi} = 0$ implies that $\#\rho(\pi_1(\overline{X})) \leq \ell^2$. On the other hand, $\overline{\psi} \neq 0$ implies that $\#\rho(\pi_1(\overline{X})) > \ell$ since the only normal subgroup of $U_3(\mathbb{Z}/\ell)$ of order ℓ is its center. Therefore, $\rho(\pi_1(\overline{X}))$ is an elementary abelian subgroup of $U_3(\mathbb{Z}/\ell)$ of order ℓ^2. In particular, ρ is trivial on the subgroup T of $\pi_1(\overline{X})$ generated by commutators and by ℓ^{th} powers, where $\pi_1(\overline{X})/T$ is the maximal elementary abelian ℓ-quotient group of $\pi_1(\overline{X})$. This group is isomorphic to $\mathrm{Pic}(\overline{X})[\ell]$. By our assumption, this latter group is defined over F, which means that $\mathrm{Gal}(\overline{F}/F)$ acts trivially on $\pi_1(\overline{X})/T$. This implies that $\rho(\pi_1(\overline{X}))$ is an elementary abelian subgroup of $\rho(\pi_1(X)) = U_3(\mathbb{Z}/\ell)$ of order ℓ^2, and the quotient group $\rho(\pi_1(X))/\rho(\pi_1(\overline{X}))$ is of order ℓ and acts trivially on $\rho(\pi_1(\overline{X}))$. This forces $\rho(\pi_1(X)) = U_3(\mathbb{Z}/\ell)$ to be abelian, which is not true. The contradiction completes the proof. □

3. Restriction of Massey products on curves to the algebraic closure

We make the same assumptions as in the previous section. In other words, F is a perfect field with a fixed algebraic closure $\overline{F}$, and X is a smooth projective geometrically irreducible curve over F such that $\overline{X} = X \otimes_F \overline{F}$ is not isomorphic to $\mathbb{P}^1_{\overline{F}}$. Moreover, ℓ is a prime number such that ℓ is invertible in F. Let $G_F = \mathrm{Gal}(\overline{F}/F)$.

When F is the algebraic closure of a finite field and $\mathbb{Z}/\ell$ is replaced by $\mathbb{Q}_\ell$, Deligne, Griffiths, Morgan and Sullivan discuss the connection between the Weil conjectures and the vanishing of all higher order Massey products in [4, p. 246].

We now return to the case with coefficients in $\mathbb{Z}/\ell$ over an arbitrary perfect field F.

Proposition 3.1. *Suppose $t \geq 3$, $\chi_1, \ldots, \chi_t \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$, and let $\overline{\chi}_1, \ldots, \overline{\chi}_t$ denote their restrictions to $\mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$. If the t-fold Massey product $\langle \chi_1, \ldots, \chi_t \rangle$ is not empty, then the t-fold Massey product $\langle \overline{\chi}_1, \ldots, \overline{\chi}_t \rangle$ is non-empty and contains* 0.

Proof. If $\overline{\chi}_1 = 0$, then $\langle \overline{\chi}_1, \overline{\chi}_2, \ldots, \overline{\chi}_t \rangle = \langle 0, \overline{\chi}_2, \ldots, \overline{\chi}_t \rangle$ obviously contains 0.

Suppose now that $\overline{\chi}_1 \neq 0$. By our assumption, we have continuous functions $\kappa_{i,j} : \pi_1(X) \longrightarrow \mathbb{Z}/\ell$, for $1 \leq i < j \leq t$, $(i,j) \neq (1,t)$, such that there is a continuous group homomorphism

$$\vartheta : \pi_1(X) \longrightarrow U_{t+1}(\mathbb{Z}/\ell)/Z(U_{t+1}(\mathbb{Z}/\ell))$$

as in (2.1). Then ϑ restricts to a continuous group homomorphism $\pi_1(\overline{X}) \longrightarrow U_{t+1}(\mathbb{Z}/\ell)/Z(U_{t+1}(\mathbb{Z}/\ell))$ by restricting the continuous functions $\kappa_{i,j}$ to $\pi_1(\overline{X})$. We denote these latter restrictions by $\overline{\kappa}_{i,j}$. In particular, $\langle \overline{\chi}_1, \ldots, \overline{\chi}_t \rangle$ contains the class in $\mathrm{H}^2(\overline{X}, \mathbb{Z}/\ell)$ of the two-cocycle $\overline{\nu}$ with

$$\overline{\nu}(\sigma,\tau) = -\overline{\chi}_1(\sigma)\overline{\kappa}_{2,t}(\tau) - \overline{\kappa}_{1,2}(\sigma)\overline{\kappa}_{3,t}(\tau) - \cdots - \overline{\kappa}_{1,t-2}(\sigma)\overline{\kappa}_{t-1,t}(\tau) - \overline{\kappa}_{1,t-1}(\sigma)\overline{\chi}_t(\tau)$$

for all $\sigma, \tau \in \pi_1(\overline{X})$. We are free to add to $\overline{\kappa}_{2,t}$ any element of $\mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$. Since we have assumed that $\overline{\chi}_1 \neq 0$, we can adjust $\overline{\kappa}_{2,t}$ in this way to make the class of $\overline{\nu}$ trivial in $\mathrm{H}^2(\overline{X}, \mathbb{Z}/\ell)$ since the Weil pairing is non-degenerate and $\mathrm{H}^2(\overline{X}, \mathbb{Z}/\ell)$ is one-dimensional over $\mathbb{Z}/\ell$. Note that in this process we may have to add to $\overline{\kappa}_{2,t}$ an element of $\mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$ that is not the restriction of an element of $\mathrm{H}^1(X, \mathbb{Z}/\ell)$, though if $\mathrm{H}^1(X, \mathbb{Z}/\ell) \longrightarrow \mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$ is surjective, we can assume we have such a restriction. □

Corollary 3.2. *Let $t \geq 3$ and $\psi_1, \ldots, \psi_t \in \mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$. If $\langle \psi_1, \ldots, \psi_t \rangle$ is not empty then it contains* 0.

Remark 3.3. For surfaces over an algebraically closed field, the situation is completely different. Ekedahl gave examples in [7] of smooth projective surfaces S over $\mathbb{C}$ and characters $\chi_1, \chi_2, \chi_3 \in \mathrm{H}^1(S, \mathbb{Z}/\ell)$ such that $\langle \chi_1, \chi_2, \chi_3 \rangle$ does not contain 0.

In the situation of Proposition 3.1, the question arises when the Massey product $\langle \chi_1, \ldots, \chi_t \rangle$ contains zero. This question sometimes reduces to the question of when the t-fold Massey product of t characters in $\mathrm{Hom}(G_F, \mathbb{Z}/\ell)$ vanishes. The following definition is useful in this context.

Definition 3.4. We say the t-fold Massey vanishing property holds for F over $\mathbb{Z}/\ell$ if for all $\alpha_1, \ldots, \alpha_t \in \mathrm{H}^1(F, \mathbb{Z}/\ell) = \mathrm{Hom}(G_F, \mathbb{Z}/\ell)$, the t-fold Massey product $\langle \alpha_1, \ldots, \alpha_t \rangle$ contains zero provided it is non-empty.

Remark 3.5. Here are some known instances when the t-fold Massey vanishing property holds for F over $\mathbb{Z}/\ell$:

- If $t = 3$ and F is arbitrary, this holds by [19].
- If $t \geq 4$ and F is a number field, this holds by [9].
- If F is a finite field this holds for all $t \geq 2$ since $\mathrm{H}^2(F, \mathbb{Z}/\ell) = 0$.

Proposition 3.6. *Let $t \geq 3$. Suppose the ℓ-torsion $\mathrm{Pic}(\overline{X})[\ell]$ is defined over F and that the t-fold Massey vanishing property holds for F over $\mathbb{Z}/\ell$. Let $\chi_1, \ldots, \chi_t \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$, and suppose the t-fold Massey product $\langle \chi_1, \ldots, \chi_t \rangle$ is not empty. If $\overline{\chi}_{i_0} = 0$ for some $1 \leq i_0 \leq t$, then $\langle \chi_1, \ldots, \chi_t \rangle$ contains zero.*

Proof. Suppose $\overline{\chi}_{i_0} = 0$ for some i_0. Since $\chi_i \cup \chi_{i+1} = 0$ for $i = 1, \ldots, t-1$ and since the cup product is anti-commutative, it follows from Lemma 2.5 that either $\chi_{i_0} = 0$ for some i_0, or all $\overline{\chi}_1 = \overline{\chi}_2 = \cdots = \overline{\chi}_t = 0$. If $\chi_{i_0} = 0$ then it is obvious that $\langle \chi_1, \ldots, \chi_t \rangle$ contains zero. Otherwise all of $\chi_1, \ldots, \chi_t$ factor through $\mathrm{H}^1(F, \mathbb{Z}/\ell) = \mathrm{Hom}(G_F, \mathbb{Z}/\ell)$. Since we assume that the t-fold Massey vanishing property holds for F over $\mathbb{Z}/\ell$, it follows that $\langle \chi_1, \ldots, \chi_t \rangle$ contains 0. □

4. Necessary conditions for the non-vanishing of Massey products

We make the same assumptions as in the previous section. We obtain the following necessary conditions for the t-fold Massey product to not contain zero.

Proposition 4.1. *Suppose that $\ell, t \geq 3$, and that the ℓ-torsion $\mathrm{Pic}(\overline{X})[\ell]$ is defined over F. Moreover, assume that the t-fold Massey vanishing property holds for F over $\mathbb{Z}/\ell$. Let $\chi_1, \ldots, \chi_t \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$ be such that the t-fold Massey product $\langle \chi_1, \ldots, \chi_t \rangle$ is not empty and does not contain zero. Then the following is true.*

(a) *None of the restrictions $\overline{\chi}_1, \ldots, \overline{\chi}_t$ to $\mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$ are zero.*
(b) *If there exist $a_1, \ldots, a_{t-1} \in (\mathbb{Z}/\ell)^\times$ with $\chi_i = a_i\chi_t$ for all $1 \leq i \leq t-1$ then $t \geq \ell$ provided t is an odd prime number.*

(c) *If X has genus 1 then there are always $a_1, \ldots, a_{t-1}$ as in (b).*

Proof. If one of $\chi_1, \ldots, \chi_t$ is zero, then $\langle \chi_1, \ldots, \chi_t \rangle$ contains zero. Therefore, we have that none of $\chi_1, \ldots, \chi_t$ are zero. Since $t \geq 3$, in order for $\langle \chi_1, \ldots, \chi_t \rangle$ to be not empty, we must have $\chi_i \cup \chi_{i+1} = 0$ for $1 \leq i \leq t-1$. If one of the $\overline{\chi}_i$ is zero, then by Lemma 2.5 and the anti-commutativity of the cup product we conclude that $\overline{\chi}_i = 0$ for $1 \leq i \leq t$. In other words, $\chi_1, \ldots, \chi_t \in \mathrm{H}^1(F, \mathbb{Z}/\ell) = \mathrm{Hom}(G_F, \mathbb{Z}/\ell)$. Since we assume that the t-fold Massey vanishing property holds for F over $\mathbb{Z}/\ell$, it follows that $\langle \chi_1, \ldots, \chi_t \rangle$ contains zero. This implies that none of $\overline{\chi}_1, \ldots, \overline{\chi}_t$ are zero, which is condition (a).

Suppose now that there exist $a_1, \ldots, a_{t-1} \in (\mathbb{Z}/\ell)^\times$ as in (b) and that t is an odd prime number. By (2.4), it follows that $\langle \chi_1, \ldots, \chi_t \rangle$ does not contain zero if and only if the t-fold Massey product $\langle \chi_t, \ldots, \chi_t \rangle$ of t copies of χ_t does not contain zero. By (2.6), $\langle \chi_t \rangle^\ell$ is non-empty, which implies that if $t < \ell$ then $\langle \chi_t \rangle^t$ is non-empty and contains zero. Therefore, the t-fold Massey product $\langle \chi_t, \ldots, \chi_t \rangle$ of t copies of χ_t is non-empty and contains zero if $t < \ell$. Since we have assumed that $\langle \chi_1, \ldots, \chi_t \rangle$ does not contain 0, this implies $t \geq \ell$.

Finally, suppose that X has genus 1, so that $\overline{X}$ is an elliptic curve and $\mathrm{Pic}(\overline{X})[\ell]$ has dimension 2 over $\mathbb{Z}/\ell$. Since $\overline{\chi}_i \cup \overline{\chi}_{i+1} = 0$, for $1 \leq i \leq t-1$, and since $\overline{\chi}_1, \ldots, \overline{\chi}_t$ are non-zero by part (a), the non-degeneracy of the Weil pairing implies that there exist $a_1, \ldots, a_{t-1} \in (\mathbb{Z}/\ell)^\times$ with $\overline{\chi}_i = a_i \overline{\chi}_t$ for all $1 \leq i \leq t-1$. Hence there exist $\psi_1, \ldots, \psi_{t-1} \in \mathrm{H}^1(F, \mathbb{Z}/\ell) = \mathrm{Hom}(G_F, \mathbb{Z}/\ell)$ such that

$$\chi_i = a_i \chi_t + \psi_i \quad \text{for } 1 \leq i \leq t-1.$$

Since $\chi_{t-1} \cup \chi_t = 0$, and $\chi_t \cup \chi_t = 0$ because $\ell \geq 3$, this implies $\psi_{t-1} \cup \chi_t = 0$. But since $\overline{\chi}_t \neq 0$ and $\overline{\psi}_{t-1} = 0$, this is by Lemma 2.5 only possible if $\psi_{t-1} = 0$. By induction on t we obtain $\psi_i = 0$ for all $1 \leq i \leq t-1$. Therefore, there exist $a_1, \ldots, a_{t-1} \in (\mathbb{Z}/\ell)^\times$ with $\chi_i = a_i \chi_t$ for all $1 \leq i \leq t-1$. □

The next result is an immediate consequence of Proposition 4.1 and the Massey vanishing results in [19] (see Remark 3.5).

Corollary 4.2. *Suppose that $\ell \geq 3$, and that the ℓ-torsion $\mathrm{Pic}(\overline{X})[\ell]$ is defined over F. Let $\chi \in \mathrm{H}^1(X, \mathbb{Z}/\ell)$ be such that the triple Massey product $\langle \chi, \chi, \chi \rangle$ does not contain zero. Then $\ell = 3$ and the restriction $\overline{\chi}$ to $\mathrm{H}^1(\overline{X}, \mathbb{Z}/\ell)$ is not zero.*

Remark 4.3. We obtain the following connection to an invariant suggested by M. Kim in [12]. Suppose $\ell = 3$, and that the 3-torsion $\mathrm{Pic}(\overline{X})[3]$ is defined over F. The non-degeneracy and Galois equivariance of the Weil pairing then imply that F contains $\mu_3(\overline{F})$. Let $\chi : \pi_1(X) \longrightarrow \mathbb{Z}/3$ be a character whose restriction $\overline{\chi}$ to $\mathrm{H}^1(\overline{X}, \mathbb{Z}/3)$ is not zero. By (2.6), the restricted triple Massey product $\langle \chi \rangle^3$ is a singleton

$$\langle \chi \rangle^3 = -\beta(\chi) \quad \in \quad \mathrm{H}^2(X, \mathbb{Z}/3)$$

where β is the Bockstein operator associated to the exact sequence

$$0 \longrightarrow \mathbb{Z}/3 \longrightarrow \mathbb{Z}/9 \longrightarrow \mathbb{Z}/3 \longrightarrow 0.$$

Since $\langle \chi \rangle^3 \subseteq \langle \chi, \chi, \chi \rangle$ and since the cup product is anti-commutative, it follows from Remark 2.3 that

$$\langle \chi, \chi, \chi \rangle = -\beta(\chi) + \chi \cup \mathrm{H}^1(X, \mathbb{Z}/3).$$

Since $\chi \cup \chi = 0$, we obtain that

$$\chi \cup \langle \chi, \chi, \chi \rangle = \chi \cup \langle \chi \rangle^3 = -\chi \cup \beta(\chi) \in \mathrm{H}^3(X, \mathbb{Z}/3). \tag{4.1}$$

Suppose now that F is a finite field. Then $\mathrm{H}^3(X, \mu_3)$ is canonically isomorphic to $\mathbb{Z}/3$, so since F contains $\mu_3(\overline{F})$ we get an isomorphism $\mathrm{H}^3(X, \mathbb{Z}/3) = \mu_3(\overline{F})^{\otimes -1} = \mathrm{Hom}(\mu_3(\overline{F}), \mathbb{Z}/3)$. In this case, (4.1) is the negative of the invariant Kim defines at the end of [12, Section 1].

Remark 4.4. Continuing with the hypotheses of Remark 4.3, suppose in addition that X has genus 1 and that F is a finite field. We claim that we have an isomorphism of one-dimensional $\mathbb{Z}/3$ vector spaces

$$\frac{\mathrm{H}^2(X,\mathbb{Z}/3)}{\chi\cup\mathrm{H}^1(X,\mathbb{Z}/3)}\longrightarrow\mathrm{H}^3(X,\mathbb{Z}/3)\cong\mathbb{Z}/3 \tag{4.2}$$

defined by $\beta\mapsto\chi\cup\beta$ for $\beta\in\mathrm{H}^2(X,\mathbb{Z}/3)$. Since F is a finite field containing $\mu_3(\overline{F})$, the cup product

$$\mathrm{H}^1(X,\mathbb{Z}/3)\times\mathrm{H}^2(X,\mathbb{Z}/3)\longrightarrow\mathrm{H}^3(X,\mathbb{Z}/3)$$

is non-degenerate, see [16, Cor. V.2.3]. Hence (4.2) is well-defined and surjective. Since X has genus 1 and $\overline{\chi}$ is not zero, the argument proving the last statement of Proposition 4.1 shows that the only elements $\xi\in\mathrm{H}^1(X,\mathbb{Z}/3)$ such that $\chi\cup\xi=0$ are those ξ that are multiples of χ. So $\chi\cup\mathrm{H}^1(X,\mathbb{Z}/3)$ has dimension

$$\dim_{\mathbb{Z}/3}\mathrm{H}^1(X,\mathbb{Z}/3)-1=\dim_{\mathbb{Z}/3}\mathrm{H}^2(X,\mathbb{Z}/3)-1.$$

This proves both sides of (4.2) have dimension 1, so (4.2) is an isomorphism because it is surjective. The conclusion is that under the above assumptions, the non-triviality of $\langle\chi,\chi,\chi\rangle$ in the group on the left side of (4.2) is equivalent to the non-vanishing of Kim's invariant. We will analyze the χ for which this holds in the next sections.

5. Triple Massey products and elliptic curves

In this section, we make the same assumptions as in the previous section. But we focus on the case when $t=3$ and $X=E$ is an elliptic curve over a field F whose characteristic is not 3. We fix $\chi_1,\chi_2,\chi_3\in\mathrm{H}^1(E,\mathbb{Z}/\ell)$ and we assume that the triple Massey product $\langle\chi_1,\chi_2,\chi_3\rangle$ is not empty. By Remark 2.3, this is equivalent to $\chi_1\cup\chi_2=\chi_2\cup\chi_3=0$. We define $G_F=\mathrm{Gal}(\overline{F}/F)$.

The next result is an immediate consequence of Proposition 4.1 and the Massey vanishing results in [19] (see Remark 3.5).

Lemma 5.1. *Suppose that E is an elliptic curve over a field F of characteristic different from 3. Assume that $\ell\geq 3$, and that the ℓ-torsion $\mathrm{Pic}(\overline{E})[\ell]=\overline{E}[\ell]$ is defined over F. Let $\chi_1,\chi_2,\chi_3\in\mathrm{H}^1(E,\mathbb{Z}/\ell)$ be such that the triple Massey product $\langle\chi_1,\chi_2,\chi_3\rangle$ is not empty and does not contain zero. Then $\ell=3$, none of the restrictions $\overline{\chi}_1,\overline{\chi}_2,\overline{\chi}_3$ to $\mathrm{H}^1(\overline{E},\mathbb{Z}/\ell)$ are zero, and there exist $a,b\in(\mathbb{Z}/\ell)^\times$ with $\chi_2=a\chi_1=b\chi_3$.*

In particular, it follows from Lemma 5.1 that if $\ell\geq 3$ and the ℓ-torsion $\overline{E}[\ell]$ is defined over F, then $\langle\chi_1,\chi_2,\chi_3\rangle$ contains zero unless possibly when $\ell=3$ and χ_1,χ_2,χ_3 all generate the same non-trivial subgroup of $\mathrm{H}^1(E,\mathbb{Z}/3)$. Using (2.4), we see that the only question that remains to be answered is for which characters $\chi:\pi_1(E)\longrightarrow\mathbb{Z}/3$ of order 3, the Massey product $\langle\chi,\chi,\chi\rangle$ does not contain zero.

For $n\geq 1$, let $\overline{E}[3^n]$ be the 3^n-torsion of $\overline{E}=E\otimes_F\overline{F}$. We assume that $\mathrm{Pic}(\overline{E})[3]=\overline{E}[3]$ is defined over F. Since the Weil pairing is non-degenerate and Galois equivariant, it follows that F contains a primitive cubic root ζ_3 of unity. Our goal is to determine all characters $\chi:\pi_1(E)\longrightarrow\mathbb{Z}/3$ such that the restriction $\overline{\chi}$ of χ to $\pi_1(\overline{E})$ is non-zero and the triple Massey product $\langle\chi,\chi,\chi\rangle$ does not contain zero.

Let H be the subgroup of $U_4(\mathbb{Z}/3)$ defined in Remark 2.4 consisting of all matrices of the form $N=N(a,u,v,w)$ as in (2.11). There is a character $\psi:H\longrightarrow\mathbb{Z}/3$ sending each such matrix N to a. Similarly to the discussion following (2.1), we see that $\langle\chi,\chi,\chi\rangle$ does not contain zero if and only if there is no continuous group homomorphism $\rho:\pi_1(E)\longrightarrow H$ with $\chi=\psi\circ\rho$.

The pro-3 completion of $\pi_1(\overline{E})$ is isomorphic to the 3-adic Tate module $T_3(\overline{E})\cong\mathbb{Z}_3^2$. Since $\overline{E}[3]=T_3(\overline{E})/3T_3(\overline{E})$ is defined over F, each $\sigma\in G_F$ acts on $T_3(\overline{E})$ as the identity modulo $3T_3(\overline{E})$. Let $J^{(3)}$ denote the pro-3 completion of a profinite group J.

Lemma 5.2. *Let F be a field whose characteristic is not 3, and let E be an elliptic curve over F such that the 3-torsion $\overline{E}[3]$ is defined over F. There is an exact sequence*

$$0 \longrightarrow T_3(\overline{E}) \longrightarrow \pi_1(E)^{(3)} \longrightarrow G_F^{(3)} \longrightarrow 1. \tag{5.1}$$

Proof. It is clear that $\pi_1(E)^{(3)}$ surjects onto $G_F^{(3)}$ by considering the cover $E \otimes_F F'$ of E when F' is the maximal pro-3 extension of F in an algebraic closure of $F(E)$. Let L be the extension of $F'(E)$ corresponding to the kernel of the resulting homomorphism $\pi_1(E)^{(3)} \longrightarrow G_F^{(3)}$. To prove (5.1) is exact, it will suffice to show that the natural homomorphism $\omega : \pi_1(\overline{E})^{(3)} = T_3(\overline{E}) \longrightarrow \mathrm{Gal}(L/F'(E))$ resulting from restricting automorphisms is an isomorphism. The constant field of L is F' since it is Galois over F and a pro-3 extension of F'. So the base change of $L/F'(E)$ by the extension $\overline{F}/F'$ gives an isomorphism of Galois groups $\mathrm{Gal}(\overline{F}L/\overline{F}(E)) = \mathrm{Gal}(L/F'(E))$. Here $\mathrm{Gal}(\overline{F}L/\overline{F}(E))$ is a quotient of $T_3(\overline{E})$, and this implies ω is surjective. To show ω is injective, we first claim that all of the 3-power torsion of $\overline{E}$ is defined over F'. For this, we use the hypothesis that $\overline{E}[3]$ is defined over F. This implies that the action of G_F on $T_3(\overline{E})$ is via matrices that are congruent to the identity mod 3. Since the multiplicative group of such matrices is a pro-3 group, all the 3-power torsion of $\overline{E}$ is defined over the maximal pro-3 extension F' of F. Now the tower of isogenies over $E \otimes_F F'$ produced by multiplication by powers of 3 gives an extension of $F'(E)$ that is Galois over $F(E)$ and has Galois group $T_3(\overline{E})$ over $F'(E)$. This shows ω is injective and completes the proof of Lemma 5.2. □

Let $\mathfrak{G}_0$ be the decomposition group (inside $\pi_1(E)$) of an inverse system of discrete valuations over the origin of E in a cofinal system of finite étale covers of E. The sequence (5.1) splits since the image of $\mathfrak{G}_0$ inside $\pi_1(E)^{(3)}$ is isomorphic to $G_F^{(3)}$ and disjoint from the image of $T_3(\overline{E})$ in $\pi_1(E)^{(3)}$. Since $9T_3(\overline{E})$ is a characteristic subgroup of $T_3(\overline{E})$, (5.1) leads to an exact sequence

$$0 \longrightarrow \frac{T_3(\overline{E})}{9T_3(\overline{E})} \longrightarrow \frac{\pi_1(E)^{(3)}}{9T_3(\overline{E})} \longrightarrow G_F^{(3)} \longrightarrow 1. \tag{5.2}$$

Let $\sigma \in G_F^{(3)}$. Since σ acts on $T_3(\overline{E})$ as the identity modulo $3T_3(\overline{E})$, we have

$$(\sigma - 1)^2(T_3(\overline{E})) \subset 9T_3(\overline{E}). \tag{5.3}$$

Since

$$(\sigma^9 - 1) \equiv (\sigma - 1)^9 + 3\sigma^3(\sigma - 1)^3 \mod 9\mathbb{Z}[\sigma]$$

we obtain

$$(\sigma^9 - 1)(T_3(\overline{E})) \subset (\sigma - 1)^3(T_3(\overline{E})) + 9T_3(\overline{E}) \subset 9T_3(\overline{E}) \tag{5.4}$$

where the second inclusion follows from (5.3). In (5.2), we view $T_3(\overline{E})/9T_3(\overline{E}) = \overline{E}[9]$ as a (normal) subgroup of $\pi_1(E)^{(3)}/9T_3(\overline{E})$, and we identify $G_F^{(3)}$ with the image of the decomposition group $\mathfrak{G}_0$ inside $\pi_1(E)^{(3)}/9T_3(\overline{E})$. Let $(G_F^{(3)})^9$ be the (normal) subgroup of $G_F^{(3)}$ generated by all 9^{th} powers. By (5.4), the elements of $(G_F^{(3)})^9$ commute with the elements of $\overline{E}[9]$, implying that $(G_F^{(3)})^9$ is a normal subgroup of $\pi_1(E)^{(3)}/9T_3(\overline{E})$ that has trivial intersection with $\overline{E}[9]$. Hence (5.2) leads to an exact sequence

$$0 \longrightarrow \frac{T_3(\overline{E})}{9T_3(\overline{E})} \longrightarrow \frac{\pi_1(E)^{(3)}/9T_3(\overline{E})}{(G_F^{(3)})^9} \longrightarrow \frac{G_F^{(3)}}{(G_F^{(3)})^9} \longrightarrow 1. \tag{5.5}$$

We define

$$\overline{\mathcal{T}} := \frac{T_3(\overline{E})}{9T_3(\overline{E})} = \overline{E}[9], \quad \overline{G} := \frac{\pi_1(E)^{(3)}/9T_3(\overline{E})}{(G_F^{(3)})^9} \quad \text{and} \quad \overline{G}_F := \frac{G_F^{(3)}}{(G_F^{(3)})^9}. \tag{5.6}$$

Letting $\xi : \overline{G}_F \longrightarrow \mathrm{Aut}(\overline{\mathcal{T}}) = \mathrm{GL}_2(\mathbb{Z}/9)$ be the continuous group homomorphism induced by (5.5), $\overline{G}$ is the semidirect product

$$\overline{G} = \overline{\mathcal{T}} \rtimes_\xi \overline{G}_F.$$

We view $\overline{\mathcal{T}}$ as a subgroup of $\overline{G}$ and we identify $\overline{G}_F$ with the image of the decomposition group $\mathfrak{G}_0$ inside $\overline{G}$, which has trivial intersection with $\overline{\mathcal{T}}$.

If $\chi : \pi_1(E) \longrightarrow \mathbb{Z}/3$ is a non-trivial character, then χ factors through the maximal elementary abelian 3-quotient of $\pi_1(E)$, and hence through $\overline{G}$. Since the group H defined in Remark 2.4 has exponent 9, we see that $\langle \chi, \chi, \chi \rangle$ does not contain zero if and only if χ, when viewed as a character from $\overline{G}$ to $\mathbb{Z}/3$, cannot be lifted to a continuous group homomorphism $\rho : \overline{G} \longrightarrow H$ such that $\chi = \psi \circ \rho$.

Theorem 5.3. *Let F be a field whose characteristic is not 3, and let E be an elliptic curve over F such that the 3-torsion $\overline{E}[3]$ is defined over F. Let $\chi : \pi_1(E) \longrightarrow \mathbb{Z}/3$ be a character. Let $\overline{K}_T$ be the image in $\overline{E}[9]$ of the kernel of χ restricted to $T_3(\overline{E})$, and let K_F be the kernel of χ restricted to the decomposition group $\mathfrak{G}_0$. Then $\langle \chi, \chi, \chi \rangle$ does not contain zero if and only if the restriction $\overline{\chi}$ of χ to $\pi_1(\overline{E})$ is non-zero and one of the following two conditions holds:*

1. *there exist elements $a \in \overline{K}_T - 3\overline{E}[9]$ and $\sigma \in G_F^{(3)}$ such that $\sigma(a) \notin (\mathbb{Z}/9)\, a$, or*
2. *the fixed field of K_F inside $\overline{F}$ is a cubic extension of F that does not contain any primitive ninth root ζ of unity, and for all $a \in \overline{K}_T - 3\overline{E}[9]$ and all $b \in \overline{E}[9] - \overline{K}_T$ and all $\iota \in K_F$ with $\iota(\zeta) = \zeta^4$, we have $(\iota - 4)(b) \notin (\mathbb{Z}/9)\, a$.*

Proof. We prove Theorem 5.3 by going through all possible cases and showing that $\langle \chi, \chi, \chi \rangle$ contains zero unless the restriction $\overline{\chi}$ of χ to $\pi_1(\overline{E})$ is non-zero and either condition (1) or condition (2) holds.

If $\overline{\chi}$ is zero, then it follows from the Massey vanishing results in [19] (see Remark 3.5 and Proposition 3.6) that $\langle \chi, \chi, \chi \rangle$ contains zero. For the remainder of the proof, we assume that $\overline{\chi}$ is non-zero.

As noted in the paragraph before the statement of Theorem 5.3, we can and will replace $\pi_1(E)$ by $\overline{G}$ in our arguments. In particular, we will replace $\overline{\chi}$ by the restriction of χ to $\overline{\mathcal{T}} = \overline{E}[9]$ and we will identify $\overline{K}_T$ with the kernel of this restriction. We will also replace K_F by the kernel of χ restricted to $\overline{G}_F$ which we identified with the image of the decomposition group $\mathfrak{G}_0$ inside $\overline{G}$. Moreover, we will replace the statements in conditions (1) and (2) about $G_F^{(3)}$ by the corresponding statements about $\overline{G}_F$ (inside $\overline{G}$). Let $F_\infty \subset \overline{F}$ be such that we can identify $\overline{G}_F = \mathrm{Gal}(F_\infty/F)$.

Suppose first that condition (1) of Theorem 5.3 holds. This means there exist elements $a \in \overline{K}_T - 3\overline{E}[9]$ and $\sigma \in \overline{G}_F$ such that $\sigma(a) \notin (\mathbb{Z}/9)\, a$. Since $\overline{\chi} \neq 0$, there exists an element $b \in \overline{E}[9]$ such that $\chi(b) = 1$. Hence $\{a, b\}$ is a basis of $\overline{E}[9]$ over $\mathbb{Z}/9$, and we can write $\xi(\sigma)$ as a matrix in $\mathrm{GL}_2(\mathbb{Z}/9)$ with respect to this basis. Since $\xi(\sigma)\, a \notin (\mathbb{Z}/9)\, a$, there exist $\mu_1, \mu_2 \in \mathbb{Z}/9$ such that $\mu_2 \not\equiv 0 \bmod 3$ and

$$(\xi(\sigma) - I)\, a = 3\mu_1\, a + 3\mu_2\, b. \tag{5.7}$$

We now want to use the elements a, b, σ to show that χ cannot be lifted to a group homomorphism $\rho : \overline{G} \longrightarrow H$. Suppose to the contrary that such a ρ exists. The entries immediately above the main diagonal of $\rho(a)$, $\rho(b)$ and $\rho(\sigma)$ are 0, 1 and $\chi(\sigma)$, respectively. This means that there exist $r, s, t, u, v, w, x, y, z \in \mathbb{Z}/3$ such that

$$\rho(a) = \begin{pmatrix} 1 & 0 & r & s \\ 0 & 1 & 0 & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} 1 & 1 & u & v \\ 0 & 1 & 1 & w \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\sigma) = \begin{pmatrix} 1 & 0 & x & y \\ 0 & 1 & 0 & z \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rho(b)^{\chi(\sigma)}.$$

Since ρ is a group homomorphism and a and b commute, we must have that $r = t$ by (2.10), which implies that $\rho(a)$ is in the center of H. Moreover, ρ must satisfy

$$[\rho(\sigma), \rho(a)] = \rho(\sigma)\rho(a)\rho(\sigma)^{-1}\rho(a)^{-1} = \rho((\xi(\sigma) - I)\, a).$$

Since $\rho(a)$ is in the center of H, this means that $\rho((\xi(\sigma) - I)\, a)$ must be the identity matrix in H. However, by (5.7), we obtain that

$$\rho((\xi(\sigma) - I)\, a) = \rho(a)^{3\mu_1}\rho(b)^{3\mu_2} = \begin{pmatrix} 1 & 0 & 0 & \mu_2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where the second equation follows from (2.9). Since $\mu_2 \not\equiv 0 \bmod 3$, this is a contradiction, which means ρ does not exist and $\langle \chi, \chi, \chi \rangle$ does not contain zero.

For the remainder of the proof, we assume that condition (1) does not hold, which means that for all $a \in \overline{K}_T - 3\overline{E}[9]$ and all $\sigma \in \overline{G}_F$, we have $\sigma(a) \in (\mathbb{Z}/9)\, a$. Since $\overline{\chi}$ is non-zero, the kernel of χ restricted to $\overline{E}[9]$ has index 3 in $\overline{E}[9]$. Hence there exists an element $a \in \overline{K}_T - 3\overline{E}[9]$. Let b be any element in $\overline{E}[9] - \overline{K}_T$. Then $\{a, b\}$ is a basis of $\overline{E}[9]$ over $\mathbb{Z}/9$ and with respect to this basis, $\xi(\sigma)$ is given by a matrix in $\mathrm{GL}_2(\mathbb{Z}/9)$ of the form

$$\xi(\sigma) = I + 3\begin{pmatrix} \lambda_1(\sigma) & \mu_1(\sigma) \\ 0 & \mu_2(\sigma) \end{pmatrix} \quad \text{for all } \sigma \in \overline{G}_F. \tag{5.8}$$

Suppose first that $K_F = \overline{G}_F$, which means that $\chi(\sigma) = 0$ for all $\sigma \in \overline{G}_F$. We will prove that $\langle \chi, \chi, \chi \rangle$ contains zero by constructing a group homomorphism $\rho : \overline{G} \longrightarrow H$ lifting χ. We define $\rho(a)$ to be the identity in H, and

$$\rho(b) = \begin{pmatrix} 1 & \chi(b) & 0 & 0 \\ 0 & 1 & \chi(b) & 0 \\ 0 & 0 & 1 & \chi(b) \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\sigma) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\mu_2(\sigma) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{for all } \sigma \in \overline{G}_F. \tag{5.9}$$

Then $\rho(a)$ commutes with $\rho(b)$ and $\rho(\sigma)$ for all $\sigma \in \overline{G}_F$. Since $(\xi(\sigma) - I)\, a = 3\lambda_1(\sigma)a$, this implies that ρ satisfies the commutator relation $[\rho(\sigma), \rho(a)] = \rho(a)^{3\lambda_1(\sigma)} = \rho((\xi(\sigma) - I)\, a)$ for all $\sigma \in \overline{G}_F$. On the other hand, (2.9) and (2.10) show that for all $\sigma \in \overline{G}_F$, we have

$$[\rho(\sigma), \rho(b)] = \begin{pmatrix} 1 & 0 & 0 & \mu_2(\sigma)\chi(b) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \rho(a)^{3\mu_1(\sigma)}\rho(b)^{3\mu_2(\sigma)}$$

which implies by (5.8) that ρ satisfies the commutator relation $[\rho(\sigma), \rho(b)] = \rho((\xi(\sigma) - I)\, b)$ for all $\sigma \in \overline{G}_F$. Finally, if $\sigma, \tau \in \overline{G}_F$ then $\xi(\sigma\tau) = \xi(\sigma) \circ \xi(\tau)$, which implies that $\mu_2(\sigma\tau) = \mu_2(\sigma) + \mu_2(\tau)$. Therefore, $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau)$, which shows that ρ is a group homomorphism lifting χ.

For the remainder of the proof, we assume that $K_F \neq \overline{G}_F$, which means that $K_F = \mathrm{Gal}(F_\infty/N)$ for a degree 3 Galois extension N/F. Since F contains a primitive third root of unity, it follows by Kummer theory that $N = F(\sqrt[3]{\alpha})$ for some $\alpha \in F$. Let $\zeta \in \overline{F}$ be a primitive ninth root of unity. Then $F(\zeta)$ is a cyclic extension of F of degree 1 or 3. In particular, $\zeta \in F_\infty$.

Suppose $\zeta \in N$. Let $\sqrt[9]{\alpha} \in \overline{F}$ be a ninth root of α. By Kummer theory, $F(\sqrt[9]{\alpha})$ is a cyclic Galois extension of F of degree 9, so $\sqrt[9]{\alpha} \in F_\infty$. Let $\overline{\tau}$ be the generator of $\mathrm{Gal}(F(\sqrt[9]{\alpha})/F)$ with $\overline{\tau}(\sqrt[9]{\alpha}) = \sqrt[9]{\alpha}\,\zeta$. Since $\mathrm{Gal}(F_\infty/F(\sqrt[9]{\alpha})) \subset K_F$, it follows that χ factors through $\overline{T} \rtimes_{\overline{\xi}} \mathrm{Gal}(F(\sqrt[9]{\alpha})/F)$ where $\overline{\xi}$ is defined by letting

$\overline{\xi}(\overline{\tau}) = \xi(\tau)$ when τ is an extension of $\overline{\tau}$ to $\overline{G}_F$. We will prove that $\langle \chi, \chi, \chi \rangle$ contains zero by constructing a group homomorphism $\rho : \overline{\mathcal{T}} \rtimes_{\overline{\xi}} \mathrm{Gal}(F(\sqrt[9]{\alpha})/F) \longrightarrow H$ lifting χ. We define $\rho(a)$ to be the identity in H, define $\rho(b)$ as in (5.9), and define

$$\rho(\overline{\tau}) = \begin{pmatrix} 1 & \chi(\tau) & 0 & 0 \\ 0 & 1 & \chi(\tau) & -\mu_2(\tau) \\ 0 & 0 & 1 & \chi(\tau) \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{5.10}$$

Then $\rho(a)$ commutes with $\rho(b)$ and $\rho(\overline{\tau})$. We argue as above to see that ρ satisfies the commutator relation $[\rho(\overline{\tau}), \rho(a)] = \rho((\overline{\xi}(\overline{\tau}) - I)\, a)$. Moreover, (2.9) and (2.10) show that

$$[\rho(\overline{\tau}), \rho(b)] = \begin{pmatrix} 1 & 0 & 0 & \mu_2(\tau)\chi(b) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \rho(a)^{3\mu_1(\tau)} \rho(b)^{3\mu_2(\tau)}$$

which implies by (5.8) that ρ satisfies the commutator relation $[\rho(\overline{\tau}), \rho(b)] = \rho((\overline{\xi}(\overline{\tau}) - I)\, b)$. Hence ρ is a group homomorphism lifting χ.

For the remainder of the proof, we assume that $\zeta \notin N$. Let $\bar{\iota}$ be the generator of $\mathrm{Gal}(F(\zeta)/F)$ with $\bar{\iota}(\zeta) = \zeta^4$. Let $\sqrt[9]{\alpha}$ be a ninth root of α in $\overline{F}$. Since $F(\sqrt[9]{\alpha}, \zeta)$ is a splitting field of $x^9 - \alpha$ over F, it is Galois. Let $\bar{\iota}_1 \in \mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F(\sqrt[9]{\alpha}))$ be such that $\bar{\iota}_1(\zeta) = \zeta^4$, so $\bar{\iota}_1$ extends $\bar{\iota}$, and let $\overline{\tau} \in \mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F(\zeta))$ be such that $\overline{\tau}(\sqrt[9]{\alpha}) = \sqrt[9]{\alpha}\,\zeta$. Using Galois theory, we see that $\mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F)$ is generated by $\bar{\iota}_1$ and $\overline{\tau}$ satisfying the relation $\bar{\iota}_1 \circ \overline{\tau} \circ \bar{\iota}_1^{-1} = \overline{\tau}^4$. Notice that $\sqrt[9]{\alpha} \in F_\infty$ because $\mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F)$ is a 3-group. Since $N \subset F(\sqrt[9]{\alpha}, \zeta)$, it follows that χ factors through $\overline{\mathcal{T}} \rtimes_{\overline{\xi}} \mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F)$ where $\overline{\xi}(\bar{\iota}_1) = \xi(\iota_1)$ and $\overline{\xi}(\overline{\tau}) = \xi(\tau)$ when ι_1 and τ are elements in $\overline{G}_F$ that extend $\bar{\iota}_1$ and $\overline{\tau}$, respectively. In particular, $\chi(\iota_1) = 0$ and $\chi(\tau) \neq 0$. The three elements of $\mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/N)$ that extend $\bar{\iota}$ are $\bar{\iota}_1$, $\bar{\iota}_2$ and $\bar{\iota}_3$, where $\bar{\iota}_1(\sqrt[9]{\alpha}) = \sqrt[9]{\alpha}$, $\bar{\iota}_2(\sqrt[9]{\alpha}) = \sqrt[9]{\alpha}\,\zeta^3$ and $\bar{\iota}_3(\sqrt[9]{\alpha}) = \sqrt[9]{\alpha}\,\zeta^6$. It follows that $\bar{\iota}_2 = \overline{\tau}^{-1} \circ \bar{\iota}_1 \circ \overline{\tau}$ and $\bar{\iota}_3 = \overline{\tau} \circ \bar{\iota}_1 \circ \overline{\tau}^{-1}$.

Under the assumptions of the previous paragraph, suppose condition (2) of Theorem 5.3 does not hold. In other words, there exists $a \in \overline{K}_T - 3\overline{E}[9]$ and there exists $b \in \overline{E}[9] - \overline{K}_T$ and there exists $\iota \in K_F$ with $\iota(\zeta) = \zeta^4$ such that $(\iota - 4)(b) \in (\mathbb{Z}/9)\, a$. In particular, we can use $\{a, b\}$ as the basis with respect to which we write the matrices in (5.8). It follows that $\mu_2(\iota) \equiv 1 \bmod 3$ in (5.8). Since ι restricts to one of $\bar{\iota}_1$, $\bar{\iota}_2$ or $\bar{\iota}_3$ in $\mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/N)$ and since the latter three elements are conjugate to each other in $\mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F)$, this implies that also $\mu_2(\iota_1) \equiv 1 \bmod 3$ in (5.8) for any $\iota_1 \in K_F$ extending $\bar{\iota}_1$. We will prove that $\langle \chi, \chi, \chi \rangle$ contains zero by constructing a group homomorphism $\rho : \overline{\mathcal{T}} \rtimes_{\overline{\xi}} \mathrm{Gal}(F(\sqrt[9]{\alpha}, \zeta)/F) \longrightarrow H$ lifting χ. Define $\rho(a)$ to be the identity in H, define $\rho(b)$ as in (5.9), define $\rho(\overline{\tau})$ as in (5.10), and define

$$\rho(\bar{\iota}_1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\mu_2(\iota_1) \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\rho(a)$ commutes with $\rho(b)$, $\rho(\overline{\tau})$ and $\rho(\bar{\iota}_1)$. We argue as above to see that ρ satisfies the commutator relations $[\rho(\overline{\sigma}), \rho(a)] = \rho((\overline{\xi}(\overline{\sigma}) - I)\, a)$ and $[\rho(\overline{\sigma}), \rho(b)] = \rho((\overline{\xi}(\overline{\sigma}) - I)\, b)$ for $\sigma \in \{\iota_1, \tau\}$. It remains to verify the equation $\rho(\bar{\iota}_1)\rho(\overline{\tau})\rho(\bar{\iota}_1^{-1}) = \rho(\overline{\tau}^4)$, which is equivalent to the commutator relation $[\rho(\bar{\iota}_1), \rho(\overline{\tau})] = \rho(\overline{\tau})^3$.

By (2.9) and (2.10), we obtain

$$[\rho(\bar{\iota}_1), \rho(\overline{\tau})] = \begin{pmatrix} 1 & 0 & 0 & \mu_2(\iota_1)\chi(\tau) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\overline{\tau})^3 = \begin{pmatrix} 1 & 0 & 0 & \chi(\tau) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $\mu_2(\iota_1) \equiv 1 \bmod 3$, it follows that ρ is a group homomorphism lifting χ.

Finally suppose that for all $a \in \overline{K}_T - 3\overline{E}[9]$ and all $b \in \overline{E}[9] - \overline{K}_T$ and all $\iota \in K_F$ with $\iota(\zeta) = \zeta^4$, we have $(\iota - 4)(b) \notin (\mathbb{Z}/9)\, a$. In other words, condition (2) of Theorem 5.3 holds. In particular, it follows that $\mu_2(\iota_1) \not\equiv 1 \bmod 3$ in (5.8) for any $\iota_1 \in K_F$ extending $\bar{\iota}_1$. We want to show that χ cannot be lifted to a group homomorphism $\rho : \overline{G} \longrightarrow H$. Suppose to the contrary that such a ρ exists. This means that there exist $r, s, t, u, v, w, x, y, z \in \mathbb{Z}/3$ such that

$$\rho(b) = \begin{pmatrix} 1 & \chi(b) & r & s \\ 0 & 1 & \chi(b) & t \\ 0 & 0 & 1 & \chi(b) \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix} 1 & \chi(\tau) & u & v \\ 0 & 1 & \chi(\tau) & w \\ 0 & 0 & 1 & \chi(\tau) \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\iota_1) = \begin{pmatrix} 1 & 0 & x & y \\ 0 & 1 & 0 & z \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

By (2.9) and (2.10), we obtain

$$[\rho(\iota_1), \rho(\tau)] = \begin{pmatrix} 1 & 0 & 0 & \chi(\tau)(x - z) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\tau)^3 = \begin{pmatrix} 1 & 0 & 0 & \chi(\tau) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $[\iota_1, \tau] = \tau^3$ and ρ is a group homomorphism and since $\chi(\tau) \neq 0$, this forces $x - z \equiv 1 \bmod 3$. On the other hand,

$$[\rho(\iota_1), \rho(b)] = \begin{pmatrix} 1 & 0 & 0 & \chi(b)(x - z) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(a)^{3\mu_1(\iota_1)} \rho(b)^{3\mu_2(\iota_1)} = \begin{pmatrix} 1 & 0 & 0 & \chi(b)\mu_2(\iota_1) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where the second equality follows since $\chi(a) = 0$, which implies that $\rho(a)^3$ is the identiy matrix. Since $[\iota_1, b] = (\xi(\iota_1) - 1)\, b = 3\mu_1(\iota_1)\, a + 3\mu_2(\iota_1)\, b$ and ρ is a group homomorphism and since $\chi(b) \neq 0$, this forces $x - z \equiv \mu_2(\iota_1) \bmod 3$. This is a contradiction, since $\mu_2(\iota_1) \not\equiv 1 \bmod 3$. Therefore, ρ does not exist, which means that $\langle \chi, \chi, \chi \rangle$ does not contain zero. This completes the proof of Theorem 5.3. □

We now proceed to the proof of Theorem 1.1 from the introduction.

Proof of Theorem 1.1. If neither condition (i) nor condition (ii) of Theorem 1.1 are satisfied, it follows from Theorem 5.3 that $\langle \chi, \chi, \chi \rangle$ contains zero for every character $\chi : \pi_1(E) \longrightarrow \mathbb{Z}/3$.

Suppose now that either condition (i) or condition (ii) of Theorem 1.1 holds. As noted in the paragraph before the statement of Theorem 5.3, we can and will replace $\pi_1(E)$ by $\overline{G}$. As before, let $F_\infty \subset \overline{F}$ be such that we can identify $\overline{G}_F = \mathrm{Gal}(F_\infty/F)$.

If condition (i) holds then there exist $a \in \overline{E}[9]$ and $\sigma \in \overline{G}_F$ such that $\sigma(a) \notin (\mathbb{Z}/9)\, a$. In particular, $a \notin 3\overline{E}[9] = \overline{E}[3]$. Let $b \in \overline{E}[9]$ be another element such that $\{a, b\}$ is a basis of $\overline{E}[9]$ over $\mathbb{Z}/9$. We can define a character $\chi : \overline{G} \longrightarrow \mathbb{Z}/3$ by $\chi(a) = 0$, $\chi(b) = 1$ and $\chi(\sigma) = 0$ for all $\sigma \in \overline{G}_F$. By condition (1) of Theorem 5.3, it follows that $\langle \chi, \chi, \chi \rangle$ does not contain zero.

If condition (ii) holds, then $L := F(\zeta)$ is not the only cubic extension of F inside $\overline{F}$. By Kummer theory, there exists $\alpha \in F$ and a cube root $\sqrt[3]{\alpha}$ of α in $\overline{F}$ that does not lie in F such that $F(\sqrt[3]{\alpha}) \neq L$. Moreover,

condition (ii) implies that for each $\sigma \in \overline{G}_F$, there exists a character $h : \overline{G}_F \longrightarrow \mathbb{Z}/9$ such that σ acts on $\overline{E}[9]$ as multiplication by a scalar of the form $\xi(\sigma) = 1 - 3h(\sigma)$. By the non-degeneracy of the Weil pairing, there exist two points $P_1, P_2 \in \overline{E}[9]$ such that the Weil pairing $\langle P_1, P_2 \rangle_{\text{Weil}} = \zeta$. Since the Weil pairing is Galois equivariant and bilinear, we obtain that

$$\sigma(\zeta) = \langle \sigma(P_1), \sigma(P_2) \rangle_{\text{Weil}} = \langle (1 - 3h(\sigma))P_1, (1 - 3h(\sigma))P_2 \rangle_{\text{Weil}} = \zeta^{(1-3h(\sigma))^2} = \zeta^{1+3h(\sigma)}. \tag{5.11}$$

Define a map $\chi : \overline{G} \longrightarrow \mathbb{Z}/3$ by letting the restriction of χ to $\overline{E}[9]$ be a fixed non-zero character, and by letting $\chi(\sigma) = i(\sigma)$ for all $\sigma \in \overline{G}_F$ with $\sigma(\sqrt[3]{\alpha}) = \sqrt[3]{\alpha}\,\zeta^{3i(\sigma)}$. Then χ is a character of $\overline{G}$ since $\chi([\sigma, c]) = \chi((\xi(\sigma) - 1)\, c) = \chi(-3h(\sigma)\, c) = 0$ for all $\sigma \in \overline{G}_F$ and $c \in \overline{E}[9]$. The kernel K_F of χ restricted to $\overline{G}_F$ consists of all $\sigma \in \overline{G}_F$ that fix $\sqrt[3]{\alpha}$. Hence the fixed field of K_F is the cubic extension $F(\sqrt[3]{\alpha})$ of F, which does not contain any primitive ninth root ζ of unity since $F(\sqrt[3]{\alpha}) \neq L$. We have that $\mathrm{Gal}(L/F) = \langle \bar{\iota} \rangle$ where $\bar{\iota}(\zeta) = \zeta^4$. If $\iota \in \overline{G}_F$ is any extension of $\bar{\iota}$, we obtain from (5.11) that $\iota(\zeta) = \zeta^{1+3h(\iota)}$. Since $\iota(\zeta) = \zeta^4$, this implies that $h(\iota) \equiv 1 \bmod 3$. Hence $\xi(\iota) = 1 - 3h(\iota) \equiv 7 \bmod 9$. It follows that $(\iota - 4)(c) = (\xi(\iota) - 4)c = 3c$ for all $c \in \overline{E}[9]$. If $a \in \overline{K}_T - 3\overline{E}[9]$ and $b \in \overline{E}[9] - \overline{K}_T$ then $\{a, b\}$ is a basis for $\overline{E}[9]$ over $\mathbb{Z}/9$, so $3b \notin (\mathbb{Z}/9)\, a$. Hence $(\iota - 4)(b) = 3b \notin (\mathbb{Z}/9)\, a$ for all such a and b. By condition (2) of Theorem 5.3, it follows that $\langle \chi, \chi, \chi \rangle$ does not contain zero. □

6. Non-vanishing triple Massey products for elliptic curves over number fields

Conditions (i) and (ii) of Corollary 1.1 depend on information concerning the action of G_F on the 9-torsion of an elliptic curve E defined over F. In this section we analyze two situations in which one has more control on this action. The first arises from specializations of results of Igusa on Galois actions of generic Legendre elliptic curves. The second arises from the Shimura reciprocity law for CM elliptic curves over number fields.

Example 6.1. We first construct E and F for which condition (i) of Corollary 1.1 is satisfied. Let t be an indeterminate, let n be an odd integer, and let E_t be the generic Legendre elliptic curve, defined over the field $k := \mathbb{Q}(\zeta_n, t)$ by the equation

$$y^2 = x(x-1)(x-t).$$

We denote by $k(\overline{E_t}[n])$ the field obtained from k by adjoining the coordinates of the n-torsion points of $\overline{E_t}$ to k. According to Igusa [11], the Galois representation

$$\mathrm{Gal}(k(\overline{E_t}[n])/k) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n)$$

has image equal to $\mathrm{SL}_2(\mathbb{Z}/n)$. If we set $n = 9$, then by Galois theory we have an exact sequence

$$0 \longrightarrow \mathrm{Gal}(k(\overline{E_t}[9])/k(\overline{E_t}[3])) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/9) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/3) \longrightarrow 0$$

(here we use Igusa's result twice: for $n = 9$ and for $n = 3$). According to Hilbert's irreducibility theorem, these Galois groups remain the same for infinitely many rational specializations t_0 of the parameter t. Therefore, one obtains infinitely many (non-isomorphic) elliptic curves E_{t_0} over $\mathbb{Q}(\zeta_9)$ such that

$$\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_9, \overline{E_{t_0}}[9])/\mathbb{Q}(\zeta_9, \overline{E_{t_0}}[3])) = \frac{\#\,\mathrm{SL}_2(\mathbb{Z}/9)}{\#\,\mathrm{SL}_2(\mathbb{Z}/3)} = 27.$$

If we let $F_{t_0} = \mathbb{Q}(\zeta_9, E_{t_0}[3])$ then the curve E_{t_0} over the field F_{t_0} satisfies condition (i) of Corollary 1.1, since $\#(\mathbb{Z}/9)^\times = 6$ is strictly smaller than 27.

Example 6.2. Suppose F is a number field containing $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ that does not contain a primitive ninth root of unity, and let E be the elliptic curve with model $y^2 = x^3 - 1$. Then $\overline{E}[3]$ is defined over F. Since F does not contain a primitive ninth root of unity, it follows from Corollary 1.1 that there exists an element $\chi \in \mathrm{H}^1(E, \mathbb{Z}/3)$ with non-vanishing triple Massey product.

Note that in Example 6.2 we do not determine which of the conditions (i) or (ii) of Corollary 1.1 holds. Distinguishing which of these holds involves controlling the action of G_F on $\overline{E}[9]$. It is natural then to consider CM elliptic curves and to analyze the information about this Galois action that is provided by the Shimura reciprocity law.

Hypothesis 6.3. Let K be an imaginary quadratic field. Fix an embedding of K into $\mathbb{C}$. Let $\mathcal{O}$ be an order in K. Suppose $\mathcal{A}$ is a non-zero finitely generated $\mathcal{O}$-submodule of K. Fix an isomorphism $\xi : \mathbb{C}/\mathcal{A} \longrightarrow E$, where E is an elliptic curve over $\mathbb{C}$ with CM by $\mathcal{O}$ and this isomorphism is equivariant for the action of $\mathcal{O}$. Let L be the abelian extension of K that is the ring class field of $\mathcal{O}$. For $r = 3, 9$ define F_r to be the extension of L obtained by adjoining the coordinates of the r-torsion points of $\overline{E}$.

Theorem 6.4. *Under Hypothesis* 6.3*, suppose $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{A}$ is a free module over $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{O}$, which is the case if $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{O}$ is étale over $\mathbb{Z}_3$. Then:*

(a) *The curve E over the field F_3 satisfies condition (i) of Corollary* 1.1*.*
(b) *There is a field N such that $F_3 \subset N \subset F_9$ and E satisfies condition (ii) of Corollary* 1.1 *over N.*

Remark 6.5. The elliptic curve $\mathbb{C}/\mathcal{O}$ is isogenous to $E = \mathbb{C}/\mathcal{A}$ and $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{O}$ is clearly free over $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{O}$. So we can always replace $E = \mathbb{C}/\mathcal{A}$ by an isogenous elliptic curve $\mathbb{C}/\mathcal{O}$ to which the conclusions (a) and (b) of Theorem 6.4 apply.

Proof of Theorem 6.4. The Shimura reciprocity law [21, Theorem 5.4] has the following consequence. Let s be an element of the idèle group J_K of K. Let K^{ab} be the maximal abelian extension of K, and let σ be an extension to $\mathbb{C}$ of the element of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ which is the image of s under the Artin map. The ring class field L is by definition the class field associated to the subgroup $K^\times \cdot (\prod_v \mathcal{O}_v^\times \times K_\infty^\times)$ of the idèles of K, where v runs over the finite places in K and $K_\infty = \mathbb{C}$ is the completion of K at the unique infinite place. Suppose $s \in \prod_v \mathcal{O}_v^\times \times K_\infty^\times$, so that σ fixes L and $s^{-1}\mathcal{A} = \mathcal{A}$. By [21, Theorem 5.7], E is defined over L. So the twist E^σ of E by σ is isomorphic to E. The Shimura reciprocity law therefore shows that there is an automorphism $\lambda(\sigma) \in \mathrm{Aut}(E) = \mathcal{O}^\times$ such that the following diagram commutes:

$$\begin{array}{ccc} K/\mathcal{A} & \xrightarrow{\ \xi\ } & E \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/\mathcal{A} & \xrightarrow{\ \lambda(\sigma)\circ\xi\ } & E \end{array} \quad .$$

Here ξ is equivariant with respect to the action of $\mathcal{O}$, so $\lambda(\sigma) \circ \xi = \xi \circ \lambda(\sigma)$ and we can write this diagram as

$$\begin{array}{ccc} K/\mathcal{A} & \xrightarrow{\ \xi\ } & E \\ {\scriptstyle \lambda(\sigma)\cdot s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/\mathcal{A} & \xrightarrow{\ \xi\ } & E \end{array} \quad . \tag{6.1}$$

We first use this to bound the extension F_3 of L generated by the coordinates of the 3-torsion points of $\overline{E}$. Define $\mathcal{O}_3 = \mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{O} \subset \prod_{v|3} \mathcal{O}_v$. Multiplication by elements $s_3 \in (1 + 3\mathcal{O}_3)^\times$ fixes the 3-torsion $3^{-1}\mathcal{A}/\mathcal{A}$ in $K/\mathcal{A}$. Let L_1 be the abelian extension of K which is the class field to $K^\times \cdot (\prod_{3\nmid v} \mathcal{O}_v^\times \times (1 + 3\mathcal{O}_3)^\times \times K_\infty^\times)$, so that $L \subset L_1$. The above diagram for $s \in \prod_{3\nmid v} \mathcal{O}_v^\times \times (1 + 3\mathcal{O}_3)^\times \times K_\infty^\times$ gives $\sigma \in \mathrm{Gal}(\mathbb{C}/L_1)$ and a

commutative square

$$\begin{array}{ccc} 3^{-1}\mathcal{A}/\mathcal{A} & \xrightarrow{\xi} & E \\ {\scriptstyle \lambda(\sigma)}\downarrow & & \downarrow{\scriptstyle \sigma} \\ 3^{-1}\mathcal{A}/\mathcal{A} & \xrightarrow{\xi} & E \end{array} \qquad . \tag{6.2}$$

By hypothesis, $\mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{A}$ is a free rank one $\mathcal{O}_3$-module, so $3^{-1}\mathcal{A}/\mathcal{A}$ is isomorphic to $\mathcal{O}_3/3\mathcal{O}_3 = \mathcal{O}/3\mathcal{O}$. If multiplication by $\lambda(\sigma) \in \mathcal{O}^\times$ is trivial on $3^{-1}\mathcal{A}/\mathcal{A}$, it follows that $\lambda(\sigma) - 1 \in 3\mathcal{O} \subset 3\mathcal{O}_K$. However, $\lambda(\sigma)$ is a root of unity of order dividing 4 or 6, and the only such root of unity for which $\mathrm{Norm}_{K/\mathbb{Q}}(\lambda(\sigma) - 1)$ is divisible by 9 is $\lambda(\sigma) = 1$. It now follows from (6.2) that the map $\sigma \mapsto \lambda(\sigma)$ must be a homomorphism from $\mathrm{Aut}(\mathbb{C}/L_1)$ to the cyclic group $\mathcal{O}^\times$. Let L_2 be the cyclic extension of L_1 which is the fixed field of the kernel of this homomorphism. Then either $[L_2 : L_1]$ divides 4 or else $\mathcal{O}^\times$ has an element of order 3.

We focus for the moment on the case in which $[L_2 : L_1]$ is divisible by 3. Then $\mathcal{O} = \mathbb{Z}[\zeta_3]$ and $K = \mathbb{Q}(\zeta_3) = L$ when ζ_3 is a primitive cube root of unity. The elliptic curve E must be isomorphic to $y^2 = x^3 - 1$, since $\mathcal{O}$ has class number 1. The 3-torsion points of $\overline{E}$ then consist of the point at infinity together with the points with (x, y)-coordinates given by elements of $\{(0, \pm\sqrt{-1}), (4^{1/3}, \pm\sqrt{3}), (\zeta_3 4^{1/3}, \pm\sqrt{3}), (\zeta_3^2 4^{1/3}, \pm\sqrt{3})\}$. Thus $F_3 = K(\sqrt{-1}, 4^{1/3})$ is cyclic of degree 6 over K, totally ramified over the prime $2\mathcal{O}_K$ and unramified over all other primes of $\mathcal{O}_K$. Accordingly, there is a subgroup T of index 6 in the units $\mathcal{O}_{K,2}^\times = \mathcal{O}_2^\times$ of the completion $\mathcal{O}_{K,2}$ of K at $2\mathcal{O}_K$ such that the group $U = K^\times \cdot (T \times \prod_{v \nmid 2\mathcal{O}_K} \mathcal{O}_v^\times \times K_\infty^\times)$ has trivial image under the Artin map to $\mathrm{Gal}(F_3/K)$. We now let s_3 be an element of $(1 + 3\mathcal{O}_3)^\times \subset \mathcal{O}_3^\times$, and we let s be the idèle with component s_3 above 3 and trivial components at all other places. Then $s \in U$, since the component of s at the place over 2 is 1. Hence the automorphism $[s, K] \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ fixes F_3 as well as L_1. Therefore if σ is any extension of $[s, K]$ to $\mathrm{Aut}(\mathbb{C}/F_3L_1)$ we find that $\lambda(\sigma)$ is the identity. Hence (6.1) gives a commutative diagram

$$\begin{array}{ccc} 9^{-1}\mathcal{A}/\mathcal{A} & \xrightarrow{\xi} & E \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ 9^{-1}\mathcal{A}/\mathcal{A} & \xrightarrow{\xi} & E \end{array} \qquad . \tag{6.3}$$

Since $\mathcal{O}_3$ is a discrete valuation ring in this case, $\mathcal{A}_3 = \mathbb{Z}_3 \otimes_{\mathbb{Z}} \mathcal{A}$ is automatically free of rank 1 over $\mathcal{O}_3$. Hence multiplication by the elements of $(1 + 3\mathcal{O}_3)^\times$ produces 9 distinct endomorphisms of $9^{-1}\mathcal{A}/\mathcal{A}$. Thus (6.3) shows that the action of $\mathrm{Gal}(K^{\mathrm{ab}}/F_3L_1)$ on the 9-torsion of $9^{-1}\mathcal{A}/\mathcal{A}$ has image a group of order at least 9. Here $\mathrm{Gal}(K^{\mathrm{ab}}/F_3L_1)$ fixes the 3-torsion $3^{-1}\mathcal{A}/\mathcal{A}$. On picking generators for the 9-torsion, we get a map from $\mathrm{Gal}(K^{\mathrm{ab}}/F_3L_1)$ into the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}/9) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3)$ whose image has order at least 9. Thus this image cannot just consist of scalar matrices, so the curve E over the field F_3 satisfies condition (i) of Corollary 1.1 when $\mathcal{O}^\times$ has order divisible by 3. To produce an N as in part (b) of Theorem 6.4, let N be the class field associated to the subgroup $U' = K^\times \cdot (T \times U_3' \times \prod_{v \nmid 6\mathcal{O}_K} \mathcal{O}_v^\times \times K_\infty^\times)$ where U_3' is the subgroup of elements of $\mathcal{O}_3^\times = \mathcal{O}_{K,3}^\times$ that are congruent to elements of $1 + 3\mathbb{Z}_3$ mod 9. Using the same arguments as above, the elements of $\mathrm{Gal}(K^{\mathrm{ab}}/N)$ act on $\overline{E}[9]$ by multiplication by elements of $1 + 3\mathbb{Z}_3$. Since $(1 + 3)^2 \not\equiv 1 \bmod 9$, the Weil pairing shows $\mathrm{Gal}(K^{\mathrm{ab}}/N)$ acts non-trivially on the ninth roots of unity, so the curve E over N satisfies condition (ii) of Corollary 1.1.

It is interesting to note that in this case, there are elements s_3 of $\mathcal{O}_3^\times$ so that if s is the idèle with component s_3 above 3 and trivial components at all other places, the action of s_3^{-1} on $3^{-1}\mathcal{A}/\mathcal{A}$ is of order 6 but the Artin automorphism $[s, K]$ fixes F_3 since F_3/K is unramified above 3. Thus when $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ extends $[s, K]$, the value of $\lambda(\sigma) \in \mathcal{O}^\times$ in diagram (6.1) must be a sixth root of unity.

From now on we suppose that $\#(\mathcal{O}^\times)$ divides 4. Then $\lambda(\sigma)^4$ is the identity. We conclude that for $s_3 \in (\mathcal{O}_3^\times)^4$ and s the idèle with component s_3 above 3 and component 1 at all other places, the diagram (6.1) becomes

$$\begin{array}{ccc} K/\mathcal{A} & \xrightarrow{\xi} & E \\ {\scriptstyle s^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/\mathcal{A} & \xrightarrow{\xi} & E \end{array} \quad . \tag{6.4}$$

Since $\mathcal{A}$ is an $\mathcal{O}$-module, the subgroup $(1+3\mathcal{O}_3)^\times$ of $\mathcal{O}_3^\times$ acts trivially by multiplication on the 3-torsion $3^{-1}\mathcal{A}/\mathcal{A}$, while $(1+9\mathcal{O}_3)^\times$ acts trivially on $9^{-1}\mathcal{A}/\mathcal{A}$. Here $(1+3\mathcal{O}_3)^\times \subset (\mathcal{O}_3^\times)^4$ since $(1+3\mathcal{O}_3)^\times$ is a pro-3 group, so (6.4) shows σ acts trivially on the 3-torsion of $\overline{E}$ if $s_3 \in (1+3\mathcal{O}_3)^\times$. Thus such σ lie in $\mathrm{Aut}(\mathbb{C}/F_3)$ because F_3 is the extension of L obtained by adjoining the coordinates of the 3-torsion points of $\overline{E}$.

We now use the hypothesis that $\mathbb{Z}_3 \otimes \mathcal{A}$ is a free rank one $\mathcal{O}_3$-module to be able to say that $9^{-1}\mathcal{A}/\mathcal{A}$ is a free rank one module for $\mathcal{O}_3/9\mathcal{O}_3$. This implies that the multiplication by the 9 elements of $(1+3\mathcal{O}_3)^\times/(1+9\mathcal{O}_3)^\times$ give distinct automorphisms of $9^{-1}\mathcal{A}/\mathcal{A}$, each of which fix $3^{-1}\mathcal{A}/\mathcal{A}$ elementwise. The diagram (6.4) together with $(1+3\mathcal{O}_3)^\times \subset (\mathcal{O}_3^\times)^4$ now shows that the elements of $(1+3\mathcal{O}_3)^\times/(1+9\mathcal{O}_3)^\times$ give 9 distinct automorphisms of the field F_9 obtained from F_3 by adjoining the coordinates of the 9-torsion points of $\overline{E}$. Each of these automorphisms fixes F_3, so we have shown $\mathrm{Gal}(F_9/F_3)$ has order at least 9. We now argue as in the case when $\mathcal{O}^\times$ has order divisible by 3 that the curve E over the field F_3 satisfies condition (i) of Corollary 1.1, and that there is a field N as in part (b) of Theorem 6.4. This completes the proof. □

Example 6.6. Let E be the modular curve $X_0(32)$ (which is the strong Weil curve 32A1(B) in Cremona's notation [3]). By [8], E has complex multiplication by $\mathbb{Z}[i]$ with multiplication by i arising from the map $z \mapsto z + \frac{1}{4}$ on the upper half plane, which normalizes $\Gamma_0(32)$. The four rational points are all cusps (and there are four cusps not defined over $\mathbb{Q}$). Note that there is an isomorphism of E with the curve $y^2 = x^4 - 1$, which is the quotient of the Fermat quartic by an involution. The conductor of E is 32 and the complex multiplication of E by $\mathbb{Z}[i]$ is defined over $K = \mathbb{Q}(i)$. Since 32 is prime to 3, E has good reduction above 3 and the hypotheses of Theorem 6.4 are satisfied.

Remark 6.7. Suppose E and F_3 are as in Theorem 6.4. One can show by an easy Cebotarev argument that there are infinitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_{F_3}$ such that the reduction of E at $\mathfrak{p}$ satisfies condition (i) of Corollary 1.1 over the residue field of $\mathfrak{p}$.

7. Triple Massey products and elliptic curves over finite fields

In this section, we assume $\ell \geq 3$ and that E is an elliptic curve over a finite field $F = \mathbb{F}_q$ such that q is not divisible by ℓ. In particular, $G_{\mathbb{F}_q}$ is profinitely generated by a Frobenius automorphism Φ, which we write as $G_{\mathbb{F}_q} = \widehat{\langle \Phi \rangle}$.

Our goal is to classify all characters $\chi_1, \chi_2, \chi_3 : \pi_1(E) \longrightarrow \mathbb{Z}/\ell$ such that the triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ does not contain zero. If $\overline{E}[\ell]$ is defined over $\mathbb{F}_q$, a complete answer is given by Lemma 5.1 and Theorem 5.3. Since $\mathbb{F}_q$ is finite, condition (2) of Theorem 5.3 never holds, which simplifies the statement; see Theorem 7.1 below. Additionally, we will analyze all cases when $\overline{E}[\ell]$ is not defined over $\mathbb{F}_q$. We will see that in these cases $\ell > 3$ is possible.

Recall from Remark 2.4 that if $\ell > 3$ then every element of $U_4(\mathbb{Z}/\ell)$ has order 1 or ℓ. On the other hand, $U_4(\mathbb{Z}/3)$ contains elements of order 9. Define

$$\ell' := \begin{cases} 9 & \text{if } \ell = 3, \text{ and} \\ \ell & \text{if } \ell > 3. \end{cases} \tag{7.1}$$

For $\ell \geq 3$, we have a short exact sequence

$$0 \longrightarrow \pi_1(\overline{E}) \longrightarrow \pi_1(E) \longrightarrow \widehat{\langle \Phi \rangle} \longrightarrow 1.$$

Denote by $\mathbf{P}$ the set of all positive rational primes. Defining

$$\Gamma := \frac{\pi_1(E)}{\prod_{p \in \mathbf{P} - \{\ell\}} T_p(\overline{E})} \tag{7.2}$$

we obtain an exact sequence

$$0 \longrightarrow T_\ell(\overline{E}) \longrightarrow \Gamma \longrightarrow \widehat{\langle \Phi \rangle} \longrightarrow 1. \tag{7.3}$$

As before, let $\mathfrak{G}_0$ be the decomposition group (inside $\pi_1(E)$) of an inverse system of discrete valuations over the origin of E in a cofinal system of finite étale covers of E. The sequence (7.3) splits since the image of $\mathfrak{G}_0$ inside Γ is isomorphic to $\widehat{\langle \Phi \rangle}$ and disjoint from the image of $T_\ell(\overline{E})$ inside Γ.

With ℓ' as in (7.1), we obtain an exact sequence

$$0 \longrightarrow \frac{T_\ell(\overline{E})}{\ell' \, T_\ell(\overline{E})} \longrightarrow \frac{\Gamma}{\ell' \, T_\ell(\overline{E})} \longrightarrow \widehat{\langle \Phi \rangle} \longrightarrow 1. \tag{7.4}$$

We view $T_\ell(\overline{E})/\ell' \, T_\ell(\overline{E}) = \overline{E}[\ell']$ as a (normal) subgroup of $\Gamma/\ell' \, T_\ell(\overline{E})$, and we identify $\widehat{\langle \Phi \rangle}$ with the image of $\mathfrak{G}_0$ inside $\Gamma/\ell' \, T_\ell(\overline{E})$. Let $\widehat{\langle \Phi^{\ell'} \rangle}$ be the subgroup of $\widehat{\langle \Phi \rangle}$ that is profinitely generated by $\Phi^{\ell'}$. By considering the action of $\widehat{\langle \Phi \rangle}$ on $\Gamma/\ell' \, T_\ell(\overline{E})$, we see that the minimal normal subgroup of $\Gamma/\ell' \, T_\ell(\overline{E})$ that contains $\widehat{\langle \Phi^{\ell'} \rangle}$ is profinitely generated by $\Phi^{\ell'}$ together with $(\Phi^{\ell'} - 1)(\overline{E}[\ell'])$. Hence (7.4) leads to an exact sequence

$$0 \longrightarrow \frac{\overline{E}[\ell']}{(\Phi^{\ell'} - 1)(\overline{E}[\ell'])} \longrightarrow \frac{\Gamma/\ell' \, T_\ell(\overline{E})}{(\Phi^{\ell'} - 1)(\overline{E}[\ell']) \cdot \widehat{\langle \Phi^{\ell'} \rangle}} \longrightarrow \frac{\widehat{\langle \Phi \rangle}}{\widehat{\langle \Phi^{\ell'} \rangle}} \longrightarrow 1. \tag{7.5}$$

We define

$$\overline{\mathcal{N}_\ell} := (\Phi^{\ell'} - 1)(\overline{E}[\ell']), \quad \overline{\mathcal{T}_\ell} := \frac{\overline{E}[\ell']}{\overline{\mathcal{N}_\ell}}, \tag{7.6}$$

$$\langle \, \overline{\Phi}_\ell \, \rangle := \frac{\widehat{\langle \Phi \rangle}}{\widehat{\langle \Phi^{\ell'} \rangle}}, \quad \text{and} \quad \overline{G}_\ell := \frac{\Gamma/\ell' \, T_\ell(\overline{E})}{\overline{\mathcal{N}_\ell} \cdot \widehat{\langle \Phi^{\ell'} \rangle}}. \tag{7.7}$$

Letting $\xi_\ell : \langle \overline{\Phi}_\ell \rangle \longrightarrow \mathrm{Aut}(\overline{\mathcal{T}_\ell})$ be the group homomorphism induced by (7.5), $\overline{G}_\ell$ is the semidirect product

$$\overline{G}_\ell = \overline{\mathcal{T}_\ell} \rtimes_{\xi_\ell} \langle \overline{\Phi}_\ell \rangle. \tag{7.8}$$

We view $\overline{\mathcal{T}_\ell}$ as a subgroup of $\overline{G}_\ell$ and we view $\overline{\Phi}_\ell$ as an element of $\overline{G}_\ell$ of order ℓ'. Note that the commutator subgroup $\overline{G}_\ell{}'$ of $\overline{G}_\ell$ is contained in the abelian subgroup $\overline{\mathcal{T}_\ell}$ which implies that $\overline{G}_\ell{}''$ is trivial.

For all $\ell \geq 3$, let H_1 be the subgroup of $U_4(\mathbb{Z}/\ell)$ defined in Remark 2.4 and let

$$(p_1, p_2, p_3) : \quad U_4(\mathbb{Z}/\ell) \longrightarrow (\mathbb{Z}/\ell)^{\oplus 3}$$

be the homomorphism that sends each matrix $M = M(a_1, a_2, a_3, u, v, w)$ in (2.8) to the triple (a_1, a_2, a_3). If $\chi_1, \chi_2, \chi_3 : \pi_1(E) \longrightarrow \mathbb{Z}/\ell$ are non-trivial characters, then they factor through the maximal elementary abelian ℓ-quotient of $\pi_1(E)$, and hence through $\overline{G}_\ell$. Recall that the group $U_4(\mathbb{Z}/\ell)$ has exponent 9 if $\ell = 3$, and it has exponent ℓ if $\ell > 3$. Hence we see, similarly to the discussion following (2.1), that the triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero if and only if $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$ and the map $(\chi_1, \chi_2, \chi_3) : \overline{G}_\ell \longrightarrow (\mathbb{Z}/\ell)^{\oplus 3}$ can be lifted to a continuous group homomorphism $\rho : \overline{G}_\ell \longrightarrow U_4(\mathbb{Z}/\ell)$ such that $(\chi_1, \chi_2, \chi_3) = (p_1, p_2, p_3) \circ \rho$.

7.1. **Suppose the ℓ-torsion $\overline{E}[\ell]$ is defined over $\mathbb{F}_q$.** By (2.4) and Lemma 5.1, we are reduced to the case when $\ell = 3$, $\ell' = 9$, and $\chi_1 = \chi_2 = \chi_3$ is given by a single character $\chi : \overline{G}_3 \longrightarrow \mathbb{Z}/3$. Since $\Phi - 1$ acts trivially on $\overline{E}[3]$, $(\Phi-1)^2$ acts trivially on $\overline{E}[9]$, which implies as in §5 that $\overline{\mathcal{T}_3} = \overline{E}[9]$. Since there is precisely one cubic extension of $\mathbb{F}_q$ inside $\overline{\mathbb{F}_q}$, we get the following simplification of Theorem 5.3.

Theorem 7.1. *Suppose E is an elliptic curve over a finite field $\mathbb{F}_q$ such that q is not divisible by 3 and such that the 3-torsion $\overline{E}[3]$ is defined over $\mathbb{F}_q$. Let $\chi : \overline{G}_3 \longrightarrow \mathbb{Z}/3$ be a character. Then $\langle \chi, \chi, \chi \rangle$ does not contain zero if and only if the restriction of χ to $\overline{E}[9]$ is non-zero and there exists an element $a \in \overline{E}[9] - 3\overline{E}[9]$ such that $\chi(a) = 0$ and $\Phi_3(a) \notin (\mathbb{Z}/9)\, a$.*

7.2. **Suppose the ℓ-torsion $\overline{E}[\ell]$ is not defined over $\mathbb{F}_q$.** This means that the set of fixed points in $\overline{E}[\ell]$ under the action of Φ has either order 1 or ℓ. If this set has order 1, then it follows that the maximal elementary abelian ℓ-quotient group of $\pi_1(E)$ is a group of order ℓ given by $\widehat{\langle\Phi\rangle}/\widehat{\langle\Phi^\ell\rangle}$. Hence all characters in $\mathrm{H}^1(E, \mathbb{Z}/\ell)$ are in $\mathrm{H}^1(\mathbb{F}_q, \mathbb{Z}/\ell)$. Since $\mathrm{H}^2(\mathbb{F}_q, \mathbb{Z}/\ell) = 0$, every triple Massey product that is non-empty contains zero.

For the remainder of this subsection, we assume that the set of fixed points in $\overline{E}[\ell]$ under the action of Φ has order ℓ. We need the following remark.

Remark 7.2. Let $\ell \geq 3$ and let Γ be as in (7.2). Letting $\lambda : \widehat{\langle\Phi\rangle} \longrightarrow \mathrm{Aut}(T_\ell(\overline{E})/\ell\, T_\ell(\overline{E})) = \mathrm{Aut}(\overline{E}[\ell])$ be the group homomorphism induced by the sequence (7.3), $\Gamma/\ell\, T_\ell(\overline{E})$ is the semidirect product

$$\Gamma/\ell\, T_\ell(\overline{E}) = \overline{E}[\ell] \rtimes_\lambda \widehat{\langle\Phi\rangle}. \tag{7.9}$$

Since we assume that the set of fixed points in $\overline{E}[\ell]$ under the action of Φ has order ℓ, there exists a basis $\{\overline{m}_1, \overline{m}_2\}$ of $\overline{E}[\ell]$ over $\mathbb{Z}/\ell$ such that the action of Φ on $\overline{E}[\ell]$ with respect to this basis is given by the matrix $\overline{A}_\Phi \in \mathrm{Aut}(\overline{E}[\ell]) = \mathrm{GL}_2(\mathbb{Z}/\ell)$, where

$$\text{either} \quad \overline{A}_\Phi = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix} \quad \text{for some element } \varepsilon \in (\mathbb{Z}/\ell)^\times - \{1\}, \tag{7.10}$$

$$\text{or} \quad \overline{A}_\Phi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{7.11}$$

In both cases (7.10) and (7.11), the subgroup of $\overline{E}[\ell]$ generated by $\overline{m}_1$ equals the set of fixed points in $\overline{E}[\ell]$ under the action of Φ. In the case (7.10), the image of $(\Phi - 1)$ on $\overline{E}[\ell]$ is given by $(\mathbb{Z}/\ell)\overline{m}_2$, whereas in the case (7.11), the image of $(\Phi - 1)$ on $\overline{E}[\ell]$ is given by $(\mathbb{Z}/\ell)\overline{m}_1$. Therefore, every character $\chi : \Gamma/\ell\, T_\ell(\overline{E}) \longrightarrow \mathbb{Z}/\ell$ satisfies $\chi(\overline{m}_2) = 0$ if $\overline{A}_\Phi$ is as in (7.10) and it satisfies $\chi(\overline{m}_1) = 0$ if $\overline{A}_\Phi$ is as in (7.11).

The following result pins down the structure of $\overline{G}_\ell$ for $\ell \geq 3$.

Lemma 7.3. *Let $\ell \geq 3$, let ℓ' be as in (7.1), and let $\overline{G}_\ell$ be as in (7.8). Extend the action of Φ on $\overline{E}[\ell]$ from (7.9) to an action of the integral group ring $\mathbb{Z}[\Phi]$ on $\overline{E}[\ell]$.*

(a) *If $(\Phi - 1)^2$ does not act as zero on $\overline{E}[\ell]$, i.e. $\overline{A}_\Phi$ is given as in (7.10) with respect to some basis of $\overline{E}[\ell]$ over $\mathbb{Z}/\ell$, then $\overline{\mathcal{T}_\ell} \cong \mathbb{Z}/\ell'$ and*

$$\overline{G}_\ell = (\mathbb{Z}/\ell') \rtimes_{\xi_\ell} \langle\overline{\Phi}_\ell\rangle$$

where $\xi_\ell : \langle\overline{\Phi}_\ell\rangle \longrightarrow (\mathbb{Z}/\ell')^\times$ is given by $\xi_\ell(\overline{\Phi}_\ell) = 1 + \ell\alpha$ for a certain $\alpha \in \mathbb{Z}/\ell'$. If $\ell = 3$ then there is a unique $\alpha \in \{0, 1, 2\}$ such that $\xi_3(\overline{\Phi}_3) = 1 + 3\alpha$, and if $\ell > 3$ then $\xi_\ell(\overline{\Phi}_\ell) = 1$ and we let $\alpha = 0$.

(b) *If $(\Phi - 1)^2$ acts as zero on $\overline{E}[\ell]$, i.e. $\overline{A}_\Phi$ is given as in (7.11) with respect to some basis of $\overline{E}[\ell]$ over $\mathbb{Z}/\ell$, then $\overline{\mathcal{T}_\ell} \cong \overline{E}[\ell']$ and*

$$\overline{G}_\ell = \overline{E}[\ell'] \rtimes_{\xi_\ell} \langle\overline{\Phi}_\ell\rangle$$

where $\xi_\ell : \langle \overline{\Phi}_\ell \rangle \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell')$ *is given by*

$$\xi_\ell(\overline{\Phi}_\ell) = \begin{pmatrix} 1+\ell\alpha & 1+\ell\beta \\ \ell\gamma & 1+\ell\delta \end{pmatrix}$$

for certain $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/\ell'$. *If* $\ell = 3$ *then there are unique such* $\alpha, \beta, \gamma, \delta$ *in* $\{0, 1, 2\}$. *On the other hand, if* $\ell > 3$ *then* $\xi_\ell(\overline{\Phi}_\ell) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *and we let* $\alpha = \beta = \gamma = \delta = 0$.

Proof. Suppose first that we are in part (a), i.e. there exists a basis $\{\overline{m}_1, \overline{m}_2\}$ of $\overline{E}[\ell]$ over $\mathbb{Z}/\ell$ such that the action of Φ on $\overline{E}[\ell]$ with respect to this basis is given by the matrix $\overline{A}_\Phi$ in (7.10).

If $\ell = 3$ then $\ell' = 9$ and $\varepsilon = 2$. In this case, let $\{m_1, m_2\}$ be a basis of $\overline{E}[9]$ that reduces to the basis $\{\overline{m}_1, \overline{m}_2\}$ modulo 3. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/9$ such that the action of Φ on $\overline{E}[9]$ is given by the matrix

$$A_\Phi = \begin{pmatrix} 1+3\alpha & 3\beta \\ 3\gamma & 2+3\delta \end{pmatrix}.$$

Hence $A_\Phi^9 - I = \begin{pmatrix} 0 & 3\beta \\ 3\gamma & 7 \end{pmatrix}$. In particular, we have $\overline{\mathcal{N}_3} = (\mathbb{Z}/9)(3\beta\, m_1 + 7m_2) = (\mathbb{Z}/9)(3\beta\, m_1 + m_2)$ in (7.6), and hence $\overline{\mathcal{T}_3} \cong \mathbb{Z}/9$. Moreover, since $\Phi(m_1) \equiv (1+3\alpha)\, m_1 \mod \overline{\mathcal{N}_3}$, we obtain that $\xi_3(\overline{\Phi}_3) = 1 + 3\alpha$.

If $\ell > 3$ then $\ell' = \ell$. In this case, the action of Φ on $\overline{E}[\ell]$ is given by the matrix $\overline{A}_\Phi$ in (7.10). Hence $\overline{A}_\Phi^\ell - I = \begin{pmatrix} 0 & 0 \\ 0 & \varepsilon - 1 \end{pmatrix}$. Since $\varepsilon - 1 \in (\mathbb{Z}/\ell)^\times$, we have $\overline{\mathcal{N}_\ell} = (\mathbb{Z}/\ell)\overline{m}_2$ in (7.6), and hence $\overline{\mathcal{T}_\ell} \cong \mathbb{Z}/\ell$. Moreover, since $\Phi(m_1) = m_1$, we obtain that $\xi_\ell(\overline{\Phi}_\ell) = 1$. This completes the proof of part (a).

Suppose next that we are in part (b), i.e. there exists a basis $\{\overline{m}_1, \overline{m}_2\}$ of $\overline{E}[\ell]$ over $\mathbb{Z}/\ell$ such that the action of Φ on $\overline{E}[\ell]$ with respect to this basis is given by the matrix $\overline{A}_\Phi$ in (7.11).

If $\ell = 3$ then $\ell' = 9$. In this case, let $\{m_1, m_2\}$ be a basis of $\overline{E}[9]$ that reduces to the basis $\{\overline{m}_1, \overline{m}_2\}$ modulo 3. Then there exist $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/9$ such that the action of Φ on $\overline{E}[9]$ is given by the matrix

$$A_\Phi = \begin{pmatrix} 1+3\alpha & 1+3\beta \\ 3\gamma & 1+3\delta \end{pmatrix}.$$

Hence $A_\Phi^9 - I$ is the zero matrix. It follows that $\overline{\mathcal{N}_3} = 0$ in (7.6), and hence $\overline{\mathcal{T}_3} = \overline{E}[9]$. In particular, $\xi_3(\overline{\Phi}_3)$ has the desired shape.

If $\ell > 3$ then $\ell' = \ell$. In this case, the action of Φ on $\overline{E}[\ell]$ is given by the matrix $\overline{A}_\Phi$ in (7.11). Hence $\overline{A}_\Phi^\ell - I$ is the zero matrix. It follows that $\overline{\mathcal{N}_\ell} = 0$ in (7.6), and hence $\overline{\mathcal{T}_\ell} = \overline{E}[\ell]$. In particular, $\xi_\ell(\overline{\Phi}_\ell)$ has the desired shape. This completes the proof of part (b). □

We have the following result on cup products:

Lemma 7.4. *Let* $\ell \geq 3$. *Suppose* E *is an elliptic curve over a finite field* $\mathbb{F}_q$ *such that* q *is not divisible by* ℓ *and such that the set of fixed points in* $\overline{E}[\ell]$ *under the action of* Φ *has order* ℓ. *Let* $\chi_1, \chi_2 \in \mathrm{H}^1(E, \mathbb{Z}/\ell) = \mathrm{Hom}(\pi_1(E), \mathbb{Z}/\ell)$ *be non-trivial characters.*

(a) *If* $(\Phi - 1)^2$ *does not act as zero on* $\overline{E}[\ell]$, *then* $\chi_1 \cup \chi_2 = 0$ *if and only if there exists* $a \in (\mathbb{Z}/\ell)^\times$ *such that* $\chi_2 = a\chi_1$.

(b) *If* $(\Phi - 1)^2$ *acts as zero on* $\overline{E}[\ell]$, *then we always have* $\chi_1 \cup \chi_2 = 0$.

Proof. Since $\ell \geq 3$, every non-identity element of $U_3(\mathbb{Z}/\ell)$ has order ℓ. It follows that $\chi_1 \cup \chi_2 = 0$ as elements of $\mathrm{H}^1(\pi_1(E), \mathbb{Z}/\ell)$ if and only if this is so when we consider them as elements of $\mathrm{H}^1(\overline{G}_\ell/(\overline{G}_\ell)^\ell, \mathbb{Z}/\ell)$ with cup product in $\mathrm{H}^2(\overline{G}_\ell/(\overline{G}_\ell)^\ell, \mathbb{Z}/\ell)$.

Suppose first that we are in part (a), i.e.

$$\overline{G}_\ell/(\overline{G}_\ell)^\ell \cong \mathbb{Z}/\ell \times \mathbb{Z}/\ell \quad \text{for all } \ell \geq 3.$$

In particular, we write $\overline{G}_\ell/(\overline{G}_\ell)^\ell$ additively. The cup product on $\mathrm{H}^1(\mathbb{Z}/\ell \times \mathbb{Z}/\ell, \mathbb{Z}/\ell)$ is a non-degenerate alternating bilinear form on a two-dimensional vector space over $\mathbb{Z}/\ell$ with values in $\mathrm{H}^2(\mathbb{Z}/\ell \times \mathbb{Z}/\ell, \mathbb{Z}/\ell)$. So it factors through the determinant and vanishes exactly on pairs that span the same space. This proves part (a).

Suppose next that we are in part (b), i.e.

$$\overline{G}_\ell/(\overline{G}_\ell)^\ell \cong \overline{E}[\ell] \rtimes_{\overline{\xi}} \langle \overline{\overline{\Phi}} \rangle \quad \text{for all } \ell \geq 3$$

where $\langle \overline{\overline{\Phi}} \rangle = \widehat{\langle \Phi \rangle}/\widehat{\langle \Phi^\ell \rangle}$ and there exists a basis $\{\overline{m}_1, \overline{m}_2\}$ of $\overline{E}[\ell]$ such that, with respect to this basis, $\overline{\xi}(\overline{\overline{\Phi}}) = \overline{A}_\Phi$ as in (7.11). We want to show that $\chi_1 \cup \chi_2 = 0$, which is equivalent to the statement that there exists a map $\kappa : \overline{G}_\ell/(\overline{G}_\ell)^\ell \longrightarrow \mathbb{Z}/\ell$ such that the map

$$\begin{array}{rccc} \rho: & \overline{G}_\ell/(\overline{G}_\ell)^\ell & \longrightarrow & U_3(\mathbb{Z}/\ell) \\ & \overline{g} & \mapsto & \begin{pmatrix} 1 & \chi_1(\overline{g}) & \kappa(\overline{g}) \\ 0 & 1 & \chi_2(\overline{g}) \\ 0 & 0 & 1 \end{pmatrix} \end{array} \tag{7.12}$$

is a group homomorphism. Since the cup product is alternating and $\mathrm{H}^1(\overline{G}_\ell/(\overline{G}_\ell)^\ell, \mathbb{Z}/\ell)$ has dimension two, it will suffice to consider the case in which $\{\chi_1, \chi_2\}$ is the dual basis over $\mathbb{Z}/\ell$ to the basis for the maximal abelian quotient of $\overline{G}_\ell/(\overline{G}_\ell)^\ell$ formed by the images of $\overline{m}_2$ and $\overline{\overline{\Phi}}$. One then checks by a commutator computation that κ can be defined by

$$\kappa(\overline{m}_1) = \chi_1(\overline{\overline{\Phi}})\chi_2(\overline{m}_2) - \chi_2(\overline{\overline{\Phi}})\chi_1(\overline{m}_2) \quad \text{and} \quad \kappa(\overline{m}_2) = 0 = \kappa(\overline{\overline{\Phi}}).$$

Note that in this case ρ is a group isomorphism, which completes the proof. □

As a consequence, we obtain the following result when $\overline{G}_\ell$ is as in part (a) of Lemma 7.3:

Lemma 7.5. *Suppose $\ell \geq 3$ and that E is an elliptic curve over a finite field $\mathbb{F}_q$ such that q is not divisible by ℓ and such that the set of fixed points in $\overline{E}[\ell]$ under the action of Φ has order ℓ. Moreover, suppose that $(\Phi - 1)^2$ does not act as zero on $\overline{E}[\ell]$. Let $\chi_1, \chi_2, \chi_3 \in \mathrm{H}^1(E, \mathbb{Z}/\ell)$ be characters such that $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$. Then $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero.*

Proof. If any of χ_1, χ_2, χ_3 is trivial, then $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero. Suppose now that none of these characters is trivial. Since $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$, we are, by (2.4) and Lemma 7.4, reduced to consider the case when $\chi_1 = \chi_2 = \chi_3$ is a single character χ. If the restriction $\overline{\chi}$ to $\mathrm{H}^1(\overline{E}, \mathbb{Z}/\ell)$ is trivial, then $\langle \chi, \chi, \chi \rangle$ contains zero since $\mathrm{H}^2(\mathbb{F}_q, \mathbb{Z}/\ell) = 0$.

Suppose now that $\overline{\chi}$ is non-trivial. Using the properties of $U_4(\mathbb{Z}/\ell)$, we can replace $\pi_1(E)$ by $\overline{G}_\ell$ in our arguments and assume that $\chi : \overline{G}_\ell \longrightarrow \mathbb{Z}/\ell$. As in part (a) of Lemma 7.3, we write

$$\overline{G}_\ell = (\mathbb{Z}/\ell') \rtimes_{\xi_\ell} \langle \overline{\Phi}_\ell \rangle$$

where $\xi_\ell(\overline{\Phi}_\ell) = 1 + \ell\alpha$ for some $\alpha \in \mathbb{Z}/\ell'$. Moreover, if $\ell = 3$ then $\ell' = 9$ and we choose $\alpha \in \{0, 1, 2\}$, and if $\ell > 3$ then $\ell' = \ell$ and we choose $\alpha = 0$.

Let m be a generator of $\mathbb{Z}/\ell'$. In particular, since $\overline{\chi} \neq 0$, we have that $\chi(m) \neq 0$. By replacing m by a multiple if necessary, we can assume without loss of generality that $\chi(m) = 1$. Let $\varphi \in \{0, 1, \ldots, \ell - 1\}$ be

such that $\chi(\overline{\Phi}_\ell) \equiv \varphi \mod \ell$. We define a map $\rho : \overline{G}_\ell \longrightarrow U_4(\mathbb{Z}/\ell)$ by

$$\rho(m) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\overline{\Phi}_\ell) = \begin{pmatrix} 1 & 0 & \alpha & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rho(m)^\varphi.$$

Then it follows that

$$[\rho(\overline{\Phi}_\ell), \rho(m)] = [\rho(\overline{\Phi}_\ell)\rho(m)^{-\varphi}, \rho(m)] = \begin{pmatrix} 1 & 0 & 0 & \alpha \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \rho(m)^{\ell\alpha} = \rho((\overline{\Phi}_\ell - 1)\, m)$$

where the second equality follows from (2.10), the third equality follows from (2.9) and our choice of α, and the last equality follows since $(\overline{\Phi}_\ell - 1)\, m = \ell\alpha\, m$. This shows that ρ is a group homomorphism, completing the proof. □

When $\overline{G}_\ell$ is as in part (b) of Lemma 7.3, we obtain the following result:

Proposition 7.6. *Suppose $\ell \geq 3$ and that E is an elliptic curve over a finite field $\mathbb{F}_q$ such that q is not divisible by ℓ and such that the set of fixed points in $\overline{E}[\ell]$ under the action of Φ has order ℓ. Moreover, suppose that $(\Phi - 1)^2$ acts as zero on $\overline{E}[\ell]$. Let $\chi_1, \chi_2, \chi_3 \in \mathrm{H}^1(E, \mathbb{Z}/\ell)$ be characters such that $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$.*

Then $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero if and only if there exists $m \in \overline{E}[\ell']$ whose image $\overline{m} \in \overline{E}[\ell]$ is not fixed by Φ such that the following two conditions hold when we write $x_i = \chi_i(m)$ and $\varphi_i = \chi_i(\overline{\Phi}_\ell)$ for $1 \leq i \leq 3$:

(1) $(\varphi_2 x_3 - \varphi_3 x_2)\, x_1 - (\varphi_1 x_2 - \varphi_2 x_1)\, x_3 \equiv 0 \mod \ell$, *and*
(2) $(\varphi_2 x_3 - \varphi_3 x_2)\, \varphi_1 - (\varphi_1 x_2 - \varphi_2 x_1)\, \varphi_3 \equiv c\, x_1 x_2 x_3 \mod \ell$,
where $c \in \mathbb{Z}$, $c = 0$ if $\ell > 3$, and $(\Phi - 1)^2(m) \equiv 3\, c\, m \mod \langle\, 3(\Phi - 1)(m) \,\rangle$ if $\ell = 3$.

Proof. Let $m \in \overline{E}[\ell']$ be such that its image $\overline{m} \in \overline{E}[\ell]$ is not fixed by Φ. Define $m' := (\Phi - 1)(m)$, so the image $\overline{m'} \in \overline{E}[\ell]$ is not zero. Since the action of $(\Phi - 1)^2$ is zero on $\overline{E}[\ell]$, it follows that $\overline{m'}$ is fixed by Φ. In particular, $\chi_i(m') = 0$ for all $1 \leq i \leq 3$ by Remark 7.2, implying that $\{m', m\}$ is a basis of $\overline{E}[\ell']$ over $\mathbb{Z}/\ell'$. It follows, as in part (b) of Lemma 7.3, that the action of Φ on $\overline{E}[\ell']$ with respect to this basis $\{m', m\}$ is given by a matrix of the form

$$\xi_\ell(\overline{\Phi}_\ell) = \begin{pmatrix} 1 + \ell\alpha & 1 + \ell\beta \\ \ell\gamma & 1 + \ell\delta \end{pmatrix} \tag{7.13}$$

for certain $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/\ell'$. Moreover, if $\ell = 3$ then $\ell' = 9$ and we choose $\alpha, \beta, \gamma, \delta \in \{0, 1, 2\}$, and if $\ell > 3$ then $\ell' = \ell$ and we choose $\alpha = \beta = \gamma = \delta = 0$. Hence, we obtain

$$(\Phi - 1)^2(m) = (\Phi - 1)(m') = \begin{cases} 3(\alpha + \delta)\, m' + 3\gamma\, m & \text{if } \ell = 3, \\ 0 & \text{if } \ell > 3. \end{cases} \tag{7.14}$$

Define

$$c = \begin{cases} \gamma & \text{if } \ell = 3, \\ 0 & \text{if } \ell > 3. \end{cases} \tag{7.15}$$

In particular, $(\Phi - 1)^2(m) \equiv 3\, c\, m \mod \langle\, 3(\Phi - 1)(m) \,\rangle$ if $\ell = 3$.

The Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero if and only if there exists a group homomorphism $\rho : \overline{G}_\ell \longrightarrow U_4(\mathbb{Z}/\ell)$ such that

$$\rho(m') = \begin{pmatrix} 1 & 0 & r & s \\ 0 & 1 & 0 & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \rho(m) = \begin{pmatrix} 1 & x_1 & u & v \\ 0 & 1 & x_2 & w \\ 0 & 0 & 1 & x_3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \rho(\overline{\Phi}) = \begin{pmatrix} 1 & \varphi_1 & d & e \\ 0 & 1 & \varphi_2 & f \\ 0 & 0 & 1 & \varphi_3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

for certain $r, s, t, u, v, w, d, e, f \in \mathbb{Z}/\ell$. Using (7.13), such a ρ exists if and only if the following three relations are satisfied in $U_4(\mathbb{Z}/\ell)$:

$$[\rho(m'), \rho(m)] = I_4, \tag{7.16}$$

$$[\rho(\overline{\Phi}), \rho(m')] = \rho(m')^{\ell\alpha}\rho(m)^{\ell\gamma} = \rho(m)^{\ell\gamma}, \tag{7.17}$$

$$[\rho(\overline{\Phi}), \rho(m)] = \rho(m')^{1+\ell\beta}\rho(m)^{\ell\delta} = \rho(m')\rho(m)^{\ell\delta}, \tag{7.18}$$

where I_4 is the identity matrix in $U_4(\mathbb{Z}/\ell)$ and the second equality in both (7.17) and (7.18) follows since $\rho(m')$ has order ℓ in $U_4(\mathbb{Z}/\ell)$ for all $\ell \geq 3$. Using (2.9) and (2.10), we see that equations (7.16), (7.17) and (7.18) are equivalent to the following equalities in $\mathbb{Z}/\ell$:

$$rx_3 = tx_1, \tag{7.19}$$

$$\gamma\, x_1x_2x_3 = t\varphi_1 - r\varphi_3, \tag{7.20}$$

$$r = \varphi_1x_2 - \varphi_2x_1, \tag{7.21}$$

$$t = \varphi_2x_3 - \varphi_3x_2, \tag{7.22}$$

$$s + \delta\, x_1x_2x_3 = (\varphi_1w - fx_1) - (\varphi_3u - dx_3) - (\varphi_1x_2 - \varphi_2x_1)(\varphi_3 + x_3). \tag{7.23}$$

It follows that $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero if and only if there exists at least one choice of $r, s, t, u, v, w, d, e, f \in \mathbb{Z}/\ell$ such that all equations (7.19) - (7.23) are satisfied. Letting $u = w = d = f = 0$ and $s = -\delta\, x_1x_2x_3 - (\varphi_1x_2 - \varphi_2x_1)(\varphi_3 + x_3)$ satisfies (7.23). Since (7.19) - (7.22) only involve r and t, we see that $\langle \chi_1, \chi_2, \chi_3 \rangle$ contains zero if and only if there exist $r, t \in \mathbb{Z}/\ell$ such that all equations (7.19) - (7.22) are satisfied. Since, by (7.15), $c \equiv \gamma \mod 3$ if $\ell = 3$ and since $c = \gamma = 0$ if $\ell > 3$, substituting (7.21) and (7.22) into (7.19) and (7.20) finishes the proof of Proposition 7.6. □

References

[1] P. Achinger, *$K(\pi, 1)$-Spaces in Algebraic Geometry*, Thesis (Ph.D.) – University of California, Berkeley, 2015.

[2] P. Achinger, *$K(\pi, 1)$-neighborhoods and comparison theorems*, Compos. Math. 151 (2015), no. 10, 1945–1964.

[3] J. E. Cremona, *Elliptic Curve Data*, `https://johncremona.github.io/ecdata/`.

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

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

[6] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. 19 (2017), no. 12, 3629–3640.

[7] T. Ekedahl, *Two examples of smooth projective varieties with non-zero Massey products*, in: Algebra, algebraic topology and their interactions (Stockholm, 1983), 128–132, Lecture Notes in Math., 1183, Springer, Berlin, 1986.

[8] N. D. Elkies, *Elliptic Curves in Nature*, `https://people.math.harvard.edu/~elkies/nature.html`.

[9] Y. Harpaz and O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Math. J., 2022, in press.

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

[11] J.-I. Igusa, *Fibre Systems of Jacobian Varieties: (III. Fibre Systems of Elliptic Curves)*, Amer. J. Math. 81 (1959), 453–476.

[12] M. Kim *Arithmetic Chern-Simons theory I*, Galois covers, Grothendieck-Teichmüller Theory and Dessins d'Enfants, pp. 155–180, Springer Proc. Math. Stat., 330, Springer, Cham, 2020.
[13] D. Kraines, *Massey higher products*, Trans. Amer. Math. Soc. 124 (1966), 431–449.
[14] E. Matzri *Triple Massey products in Galois cohomology*, ArXiv:1411.4146, preprint 2014.
[15] J. McCleary, *A user's guide to spectral sequences*, second edition. Cambridge Studies in Advanced Mathematics, 58. Cambridge University Press, Cambridge, 2001.
[16] J. Milne, *Etale cohomology*. Princeton University Press, 1980.
[17] J. Milne, *Arithmetic Duality Theorems*, second edition. Academic Press, 2006.
[18] J. Mináč and N. D. Tân, *Triple Massey products over global fields*, Doc. Math. 20 (2015), 1467–1480.
[19] J. Mináč and N. D. Tân, *Triple Massey products vanish over all fields*, J. Lond. Math. Soc. (2) 94 (2016), no. 3, 909–932.
[20] R. Sharifi, *Massey Products and Ideal Class Groups*, J. reine angew. Math. 603 (2007), 1–33.
[21] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, reprint of the 1971 original, Princeton University Press, Princeton, NJ, 1994.

F.B.: Department of Mathematics, University of Iowa, 14 MacLean Hall, Iowa City, IA 52242-1419, U.S.A.
Email address: frauke-bleher@uiowa.edu

T.C.: Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, U.S.A.
Email address: ted@math.upenn.edu

J. G.: Institut de Mathématiques de Toulouse, CNRS UMR 5219, 118, route de Narbonne, 31062 Toulouse Cedex, France.
Email address: Jean.Gillibert@math.univ-toulouse.fr