THE GALOIS ACTION ON THE LOWER CENTRAL SERIES OF THE FUNDAMENTAL GROUP OF THE FERMAT CURVE

RACHEL DAVIS, RACHEL PRIES, AND KIRSTEN WICKELGREN

Abstract. Information about the absolute Galois group G_K of a number field K is encoded in how it acts on the étale fundamental group π of a curve X defined over K. In the case that $K = \mathbb{Q}(\zeta_n)$ is the cyclotomic field and X is the Fermat curve of degree $n \geq 3$, Anderson determined the action of G_K on the étale homology with coefficients in $\mathbb{Z}/n\mathbb{Z}$. The étale homology is the first quotient in the lower central series of the étale fundamental group. In this paper, we determine the structure of the graded Lie algebra for π. As a consequence, this determines the action of G_K on all degrees of the associated graded quotient of the lower central series of the étale fundamental group of the Fermat curve of degree n, with coefficients in $\mathbb{Z}/n\mathbb{Z}$.
MSC2010: 11D41, 11R18, 13A50, 14F20, 14F35, 14H30
Keywords: Fermat curve, cyclotomic field, étale fundamental group, homology, lower central series, 2-nilpotent quotient, Galois module.

1. Introduction

Let X be the Fermat curve of degree n, where $n \geq 3$. Consider the cyclotomic field $K = \mathbb{Q}(\zeta_n)$; let $\overline{K}$ be its algebraic closure and let G_K be its absolute Galois group. Anderson described the action of G_K on the étale homology $\mathrm{H}_1(X; \mathbb{Z}/n\mathbb{Z})$ with coefficients in $\mathbb{Z}/n\mathbb{Z}$ of the base change $X_{\overline{K}}$ of X to $\overline{K}$ (the base change is suppressed in the notation $\mathrm{H}_1(X; \mathbb{Z}/n\mathbb{Z})$); more precisely, he analyzed the G_K-action on the relative homology $\mathrm{H}_1(U, Y; \mathbb{Z}/n\mathbb{Z})$ of the open affine Fermat curve $U = \{(x, y) : x^n + y^n = 1\}$ relative to the set Y of the $2n$ cusps with $xy = 0$.

The main result of [DPSW16, Sections 4 & 5] is that Anderson's description uniquely determines the action of G_K on $\mathrm{H}_1(U, Y; \mathbb{Z}/n\mathbb{Z})$ when n is prime. In [DPSW18, Theorem 1.1], the authors find an explicit formula for the action of each $\sigma \in G_K$ on $\mathrm{H}_1(U, Y; \mathbb{Z}/n\mathbb{Z})$ when n is a prime satisfying Vandiver's conjecture.

Let $\pi = [\pi]_1 = \pi_1(X)$ be the étale fundamental group of $X_{\overline{K}}$, and for $m \geq 2$, let $[\pi]_m$ be the mth subgroup of the lower central series $\pi = [\pi]_1 \supset [\pi]_2 \supset [\pi]_3 \supset \cdots$, defined so that $[\pi]_m = \overline{[\pi, [\pi]_{m-1}]}$ is the closure of the subgroup generated by commutators of elements of π with elements of $[\pi]_{m-1}$. For example, there is a canonical isomorphism of G_K-modules $\mathrm{H}_1(X; \mathbb{Z}/n\mathbb{Z}) \cong \pi/[\pi]_2 \otimes \mathbb{Z}/n\mathbb{Z}$, and as a group $\pi/[\pi]_2 \otimes \mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$, where $g = (n-1)(n-2)/2$ is the genus of the Fermat curve.

In this paper, we describe the action of G_K on each of the higher graded quotients $[\pi]_m/[\pi]_{m+1} \otimes \mathbb{Z}/n\mathbb{Z}$ in the lower central series filtration of π, with coefficients in $\mathbb{Z}/n\mathbb{Z}$; when n is prime, this description determines the action uniquely. One motivation for this work is that it sheds light on the 2-nilpotent quotient of the étale fundamental group of the Fermat curve, because of the exact sequence:

$$1 \to [\pi]_2/[\pi]_3 \otimes \mathbb{Z}/n\mathbb{Z} \to \pi/[\pi]_3 \otimes \mathbb{Z}/n\mathbb{Z} \to \pi/[\pi]_2 \otimes \mathbb{Z}/n\mathbb{Z} \to 1. \tag{1.a}$$

To state the results more precisely, consider the graded Lie algebra $\mathrm{gr}(\pi) = \oplus_{m \geq 1} [\pi]_m/[\pi]_{m+1}$ associated with the lower central series for π, [Laz54, Ser65], which is equipped with its G_K-action. The group $\mu_n \times \mu_n$ acts on X by multiplying x and y by nth roots of unity, and therefore acts G_K-equivariantly on π. Let F

We would like to thank AIM for support for this project through a Square collaboration grant. We would like to thank Vesna Stojanoska for earlier collaboration and Richard Hain for helpful comments. We would like to thank the anonymous referee for thoughtful comments. Pries was supported by NSF grants DMS-15-02227 and DMS-19-01819. Wickelgren was supported by an American Institute of Mathematics five year fellowship and NSF grants DMS-1406380 and DMS-1552730.

be the free profinite group on $2g$ generators and consider its graded Lie algebra $\mathrm{gr}(F) = \oplus_{m\geq 1}\mathrm{gr}_m(F)$. It follows from work of Labute in [Lab70, Theorem, page 17] that there is an element ρ of weight 2 such that

$$\mathrm{gr}(\pi) \cong \mathrm{gr}(F)/\overline{\langle\rho\rangle}.$$

We use the Galois action on the left hand side to equip the right hand side with such an action.

In Theorem 1.1, we determine the isomorphism class of $\mathrm{gr}(\pi)$ as a graded Lie group with action of $\mu_n \times \mu_n$. Since $\mathrm{gr}(F)$ is generated in degree 1, it suffices to obtain a complete description of the ideal $\overline{\langle\rho\rangle} \subset \mathrm{gr}(F)$ and the action of $\mu_n \times \mu_n$ on it.

Furthermore, when n is prime, we determine the isomorphism class of $\mathrm{gr}(\pi)\otimes \mathbb{Z}/n\mathbb{Z}$ as a graded Lie algebra with $\mu_n \times \mu_n \times G_K$-action. This gives the stated application of determining the action of G_K on each of the higher graded quotients $[\pi]_m/[\pi]_{m+1} \otimes \mathbb{Z}/n\mathbb{Z}$. For this, it suffices to use the description of the ideal $\overline{\langle\rho\rangle} \subset \mathrm{gr}(F)$ from Theorem 1.1 together with the action of G_K on $[\pi]_1/[\pi]_2 \otimes \mathbb{Z}/n\mathbb{Z}$ from our earlier result in [DPSW18, Theorem 1.1].

To find the ideal $\overline{\langle\rho\rangle} \subset \mathrm{gr}(F)$, we use the isomorphism of G_K-modules [Hai97, Corollary 8.3]

$$[\pi]_2/[\pi]_3 \cong (\mathrm{H}_1(X) \wedge \mathrm{H}_1(X))\,/\mathrm{Im}(\mathscr{C}),$$

where

$$\mathscr{C} : \mathrm{H}_2(X) \to \mathrm{H}_1(X) \wedge \mathrm{H}_1(X) \tag{1.b}$$

is the dual map to the cup product $\mathrm{H}^1(X) \wedge \mathrm{H}^1(X) \to \mathrm{H}^2(X)$.

The image $\mathrm{Im}(\mathscr{C})$ is cyclic since $\mathrm{H}_2(X) \cong \mathbb{Z}(1)$. We use the basis of $H_1(X)$ of [Ejd19, Theorem 1.2], see (4.l), which interacts well with the $\mu_n \times \mu_n$-action. This basis gives an isomorphism $\mathrm{gr}_1(F) \cong H_1(X)$, which in turn induces an isomorphism $\mathrm{gr}_2(F) \cong \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$. We may therefore compute ρ as an element of $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$, and any generator of $\mathrm{Im}(\mathscr{C})$ is a valid choice for ρ.

We note that $\mathrm{H}_1(X)$ is a quotient of $\mathrm{H}_1(U)$, which is a subspace of the relative homology $\mathrm{H}_1(U, Y)$. For all integers $n \geq 3$, we determine ρ as the image of an element Δ in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$, with the result expressed in terms of a convenient basis $\{[E_{i,j}]\}$ for $\mathrm{H}_1(U)$ defined in Section 4.1, Lemma 4.1.

Theorem 1.1. *For $n \geq 3$, a generator ρ for $\mathrm{Im}(\mathscr{C})$ is given by the image in $\mathrm{H}_1(X)\wedge\mathrm{H}_1(X)$ of the following element Δ of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$:*

$$\Delta = \sum_{\substack{1\leq i_1\leq i_2\leq n-1 \\ 1\leq j_1,j_2\leq n-1 \\ (i_1,j_1)\neq(i_2,j_2)}} \epsilon(i_1, j_1, i_2, j_2)[E_{i_1,j_1}] \wedge [E_{i_2,j_2}],$$

where

$$\epsilon(i_1, j_1, i_2, j_2) = \begin{cases} 1 & \text{if } j_2 - j_1 \equiv i_2 - i_1 \not\equiv 0 \mod n-1 \\ -1 & \text{if } j_2 - j_1 + 1 \equiv i_2 - i_1 \not\equiv 0 \mod n-1 \\ 0 & \text{otherwise.} \end{cases}$$

The action of the absolute Galois group G_K on the homology of the Fermat curve is the subject of several foundational papers, including [Iha86], [And87], [AI88], [And89], and [Col89]. Let $n = p$ be an odd prime. Let L be the splitting field of $1 - (1 - x^p)^p$. In [And87, Section 10.5], Anderson proved that the action of G_K on the relative homology $\mathrm{H}_1(U, Y; \mathbb{Z}/p\mathbb{Z})$ factors through the finite Galois extension L/K and gave a theoretical formulation for the action of $q \in Q = \mathrm{Gal}(L/K)$. From [And87, Section 10.5] and the result of Labute quoted above, it follows that the action of G_K on $[\pi]_m/[\pi]_{m+1}\otimes\mathbb{Z}/p\mathbb{Z}$ factors through $Q = \mathrm{Gal}(L/K)$, for any $m \geq 2$.

In [DPSW18, Theorem 1.1] and [DPSW16, Theorem 1.1], we made a completely explicit calculation of the Q-action on $\mathrm{H}_1(U, Y; \mathbb{Z}/p\mathbb{Z})$ when p is an odd prime satisfying Vandiver's conjecture.* Our main motivation for Theorem 1.1 is that the G_K-module $[\pi]_2/[\pi]_3$ occurs as the coefficient group in a map that measures an

*Vandiver's Conjecture states that p does not divide the order of the class group of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. It is true for all regular primes p and all primes less than 163 million.

obstruction for rational points: $\delta_2 : \mathrm{H}^1(G_K, \mathrm{H}_1(X)) \to \mathrm{H}^2(G_K, [\pi]_2/[\pi]_3)$. For this reason, we highlight the following result.

Corollary 1.2. *Combining* [DPSW18, Theorem 1.1] *with Theorem 1.1 yields an explicit computation of* $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z}$ *as a* G_K*-module when* p *is an odd prime satisfying Vandiver's conjecture.*

Section 7 contains several applications. In Section 7.1, we give an independent verification for the formula for ρ if $p = 5$, using the fact that ρ satisfies certain invariance properties under the action of $\mathrm{Aut}(X)$ and $\mathrm{Gal}(L/\mathbb{Q})$. Using these invariance properties, if $p = 5$, we also compute that the dimension of the $G_{\mathbb{Q}}$-invariant subspace of $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ is 2, see Example 7.6. This provides a new proof of a result of Tzermias [Tze97, Corollary 2].

In Section 7.3, we consider the short exact sequence

$$0 \to (\mathbb{Z}/p\mathbb{Z})\rho \to \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \to [\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z} \to 0.$$

Since Q fixes ρ, this yields a long exact sequence

$$0 \to (\mathbb{Z}/p\mathbb{Z})\rho \to \mathrm{H}^0(Q; \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z})) \to \mathrm{H}^0(Q; [\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\delta} \mathrm{H}^1(Q; (\mathbb{Z}/p\mathbb{Z})\rho). \tag{1.c}$$

If $p = 5$, as an application of Corollary 1.2, we compute that the dimension of the G_K-invariant subspace of $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ (resp. $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/5\mathbb{Z}$) is 35 (resp. 34). This shows that the coboundary map δ in (1.c) is trivial if $p = 5$, see Example 7.7.

2. The fundamental group of the Fermat curve

Let $\zeta = \zeta_n = e^{2\pi i/n}$ (resp. $\epsilon = e^{\pi i/n}$) be a primitive nth (resp. $2n$th) root of unity.

Consider the Fermat curve X of exponent n with equation $x^n + y^n = z^n$. Let Z_0 be the set of n points where $z = 0$. Consider the open affine subset $U = X - Z_0$. In Sections 2-4, we work over $X := X(\mathbb{C})$ and $U := U(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 \mid x^n + y^n = 1\}$.

2.1. The fundamental group and the definition of Δ.

Note that U is a real surface of genus $g = \binom{n-1}{2}$ with n punctures. We choose the base point $b = (0, 1)$. There exist loops a_i, b_i for $1 \le i \le g$ and c_j for $0 \le j \le n-1$, with base point b, such that $\pi_1(U)$ has a presentation

$$\pi_1(U) = \langle a_i, b_i, c_j : i = 1, \ldots, g,\ j = 0, \ldots, n-1 \rangle / \prod_{i=1}^{g} [a_i, b_i] \prod_{j=0}^{n-1} c_j. \tag{2.d}$$

Let $\bar{a}_i, \bar{b}_i, \bar{c}_j$ denote the images of a_i, b_i, c_j in $\mathrm{H}_1(U)$. Furthermore, we can suppose that

(1) the loop c_j circles the puncture $[\zeta^j : \epsilon : 0] \in Z_0$;

(2) each $\bar{c}_j$ pairs trivially with $\bar{a}_i, \bar{b}_i$; each $\bar{c}_j$ pairs trivially with $\bar{c}_i$ for $i \ne j$;

(3) and $\bar{a}_i, \bar{b}_i$ in $\mathrm{H}_1(U)$ form a symplectic basis.

The set $\{\bar{c}_j\}$ generates the kernel of $\mathrm{H}_1(U) \to \mathrm{H}_1(X)$. Define

$$\Delta = \sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U). \tag{2.e}$$

Let $[\pi_1(U)]_2 = \overline{[\pi_1(U), \pi_1(U)]}$ and $[\pi_1(U)]_3 = \overline{[\pi_1(U), [\pi_1(U)]_2]}$. Consider the map

$$C : \mathrm{H}_1(U) \wedge \mathrm{H}_1(U) \to [\pi_1(U)]_2/[\pi_1(U)]_3,$$

which takes the simple wedge $a \wedge b$ to the (equivalance class of the) commutator of a lift of a and a lift of b to elements of $\pi_1(U)$. Since U is not proper, C is an isomorphism. Recall the definition of $\mathscr{C}$ from (1.b).

Lemma 2.1. *The image of* Δ *under the map* $\wedge^2(\mathrm{H}_1(U) \to \mathrm{H}_1(X))$ *is a generator of* $\mathrm{Im}(\mathscr{C})$.

Proof. By definition, $\mathscr{C}$ is the dual of the cup product pairing. Since $\bar{a}_i, \bar{b}_i$ satisfy the standard symplectic pairing, the image of $\mathscr{C}$ is generated by the image of $\sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i$ under the map $\wedge^2(\mathrm{H}_1(U) \to \mathrm{H}_1(X))$, which is the image of Δ by definition. □

Lemma 2.1 shows that the image of Δ under the map $\wedge^2(\mathrm{H}_1(U) \to \mathrm{H}_1(X))$ is a valid choice for ρ, and we henceforth let ρ denote this image.

2.2. **The second graded quotient in the lower central series.** By (2.e), $\Delta = \sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i$. Our goal is to determine Δ in terms of a basis of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ for which we know the action of the absolute Galois group. In order to do this, we investigate the element $T := \prod_{i=1}^{g} [a_i, b_i]$ in $\pi_1(U)$. Note that $T = (c_0 \circ c_1 \circ \cdots c_{n-1})^{-1}$.

The next lemma shows that Δ does not depend on the representation as a product of commutators.

Lemma 2.2. *Suppose $r_1, \ldots, r_N, s_1 \ldots, s_N$ are loops in U, with images $\bar{r}_i, \bar{s}_i$ in $\mathrm{H}_1(U)$. If*

$$T \text{ is homotopic to } [r_1, s_1] \circ \cdots \circ [r_N, s_N],$$

then $\sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i = \sum_{i=1}^{N} \bar{r}_i \wedge \bar{s}_i$ in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$.

Proof. By hypothesis, in $\pi_1(U)$,

$$[a_1, b_1] \circ \cdots \circ [a_g, b_g] = [r_1, s_1] \circ \cdots \circ [r_N, s_N]. \tag{2.f}$$

Note that both sides of the equation are elements of $[\pi_1(U)]_2$. Therefore (2.f) holds in $[\pi_1(U)]_2/[\pi_1(U)]_3$. Under the inverse of the isomorphism C, (2.f) becomes $\sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i = \sum_{i=1}^{N} \bar{r}_i \wedge \bar{s}_i$ in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$. □

The next lemma is key for simplifying later calculations.

Lemma 2.3. *Suppose $\alpha, \beta, \gamma \in \pi_1(U)$.*

(1) If $\alpha\gamma \in [\pi_1(U)]_2$, then $\gamma\alpha \in [\pi_1(U)]_2$ and $\alpha\gamma$ and $\gamma\alpha$ have the same image in $[\pi_1(U)]_2/[\pi_1(U)]_3$.

(2) If $\gamma^{-1}\alpha\gamma\beta \in [\pi_1(U)]_2$, then $\alpha\beta \in [\pi_1(U)]_2$ and the difference between the images of $\gamma^{-1}\alpha\gamma\beta$ and $\alpha\beta$ in $[\pi_1(U)]_2/[\pi_1(U)]_3$ is $\gamma \wedge (-\alpha)$.

Proof. (1) Note that $\gamma\alpha = \alpha^{-1}(\alpha\gamma)\alpha$. If $\alpha\gamma \in [\pi_1(U)]_2$, then $\gamma\alpha \in [\pi_1(U)]_2$ because the commutator subgroup is normal. Also $\alpha\gamma$ and $\gamma\alpha$ have the same image in $[\pi_1(U)]_2/[\pi_1(U)]_3$ because conjugation acts trivially on $[\pi_1(U)]_2/[\pi_1(U)]_3$.

(2) In $\pi_1(U)$,

$$[\gamma^{-1}\alpha\gamma, \gamma] = (\gamma^{-1}\alpha\gamma)\gamma(\gamma^{-1}\alpha^{-1}\gamma)\gamma^{-1} = \gamma^{-1}\alpha\gamma\alpha^{-1} = [\gamma^{-1}, \alpha].$$

So $[\gamma^{-1}\alpha\gamma, \gamma]\alpha\beta = \gamma^{-1}\alpha\gamma\beta$. In particular, if $\gamma^{-1}\alpha\gamma\beta$ is in $[\pi_1(U)]_2$, then so is $\alpha\beta$.

Since U is affine, $[\pi_1(U)]_2/[\pi_1(U)]_3 \cong \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$. In $[\pi_1(U)]_2/[\pi_1(U)]_3$, the difference between the images of $\gamma^{-1}\alpha\gamma\beta$ and $\alpha\beta$ is the image of $[\gamma^{-1}\alpha\gamma, \gamma]$. Since $[\gamma^{-1}\alpha\gamma, \gamma] = [\gamma^{-1}, \alpha]$, this image is $-\gamma \wedge \alpha$, which equals $\gamma \wedge (-\alpha)$.

□

2.3. **Elements of the fundamental groupoid.** We compute in the fundamental groupoid of $U := U(\mathbb{C}) = \{(x, y) \mid x^n + y^n = 1\}$ where the base points are taken to be the $2n$ points such that $xy = 0$. Let β be the path in U, which begins at the base point $b_0 = b = (0, 1)$ and ends at $d_0 = (1, 0)$, given by

$$\beta = (\sqrt[n]{t}, \sqrt[n]{1-t}) \text{ for } t \in [0, 1]. \tag{2.g}$$

Throughout this section, let $0 \le i \le n-1$ and $0 \le j \le n-1$. Let $b_j = (0, \zeta^j)$ and $d_i = (\zeta^i, 0)$. Consider the automorphisms $\epsilon_0, \epsilon_1 \in \mathrm{Aut}(U)$ defined by $\epsilon_0(x, y) = (\zeta x, y)$ and $\epsilon_1(x, y) = (x, \zeta y)$. Consider the path in U, which begins at b_j and ends at d_i, given by

$$e_{i,j} = \epsilon_0^i \epsilon_1^j \beta. \tag{2.h}$$

Note that $e_{i,j}$ depends only on the values of i and j modulo n.

Consider the loop $E_{i,j}$ in U, formed by the composition of four paths, where path composition is written from left to right:

$$E_{i,j} = e_{0,0} \circ (e_{0,j})^{-1} \circ e_{i,j} \circ (e_{i,0})^{-1}.$$

Then $E_{i,j}$ proceeds through the following points:

$$b_0 \mapsto d_0 \mapsto b_j \mapsto d_i \mapsto b_0.$$

If $ij = 0$, then $E_{i,j}$ is trivial in the fundamental groupoid. The converse is also true; see Lemma 4.1 below.

3. A formula for the classifying element

In this section, we analyze the class, in the fundamental groupoid, of the boundary of a disk in the Fermat curve which contains the n cusps where $z = 0$. This allows us to describe

$$T = \prod_{i=1}^{g} [a_i, b_i] = (c_0 \circ c_1 \circ \cdots c_{n-1})^{-1}$$

as a product of loops of the form $E_{i,j}$. We analyze the ordering of the loops in this product combinatorially. Using the material in Section 2.2, this allows us to find an explicit formula for the element $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ whose image in $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ is ρ, in terms of a basis on which we understand the action of the absolute Galois group.

3.1. Sheets of a cover.

Let $V = \mathbb{A}^1(\mathbb{C})$. Consider the map $\wp : U \to V$ given by $(x, y) \mapsto x$. Let $\zeta = e^{2\pi i/n}$. Then $\wp$ is a μ_n-Galois cover, where the generator ζ of μ_n acts via $\zeta(x, y) = (x, \zeta y)$.

The cover $\wp$ is ramified at $\{(x, y) = (\zeta^i, 0) \mid i = 0, \ldots, n-1\}$ and branched at $\{x = \zeta^i \mid i = 0, \ldots, n-1\}$. Let w_i be the path in V given by $x = \zeta^i \sqrt[n]{t}$ for $t \in [0, 1]$. Let $V^\circ = V - \{w_i \mid 0 \leq i \leq n-1\}$. Let $U^\circ = \wp^{-1}(V^\circ)$. The restriction of $\wp$ to U° is unbranched and U° is a disjoint union of n sheets $\{U_k \mid 0 \leq k \leq n-1\}$.

In order to label these sheets, we define the following notation, for $0 \leq i \leq n-1$. Let r_i be the ray $x = \zeta^i \sqrt[n]{t}$ for $t \in [0, \infty)$. Let R_i be the intersection of a small neighborhood of $x = 0$ in V° with the segment of V° bounded by $r_{i-1 \bmod n}$ and r_i. In other words, for some small $\epsilon_\circ \in \mathbb{R}^{>0}$,

$$R_i = \{x = re^{I\theta} \in V^\circ \mid (i-1)\frac{2\pi}{n} < \theta < i\frac{2\pi}{n},\ 0 < r < \epsilon_\circ\}.$$

For $0 \leq i, j \leq n-1$, we denote by $\tilde{R}_{i,j}$ the intersection of a small neighborhood of $b_j = (0, \zeta^j)$ with $U^\circ \cap \wp^{-1}(R_i)$. We label by U_k the sheet containing $\tilde{R}_{k,0}$.

Thus our small neighborhood of $b_j = (0, \zeta^j)$ intersected with U° is the disjoint union of the n neighborhoods $\tilde{R}_{i,j}$ for $0 \leq i \leq n-1$. Since we are free to base fundamental groups at a point b_j or at a simply connected neighborhood of b_j, we can think of b_j as a base point divided into n pieces, one piece on each sheet U_k.

Note that $U^\circ = U - \{e_{i,j} \mid 0 \leq i, j \leq n-1\}$. There is exactly one way to glue the sheets U_k together along the paths $e_{i,j}$ to obtain a ramified cover of Riemann surfaces.

3.2. The cusps with $z = 0$.

Recall that Z_0 is the set of n points of X where $z = 0$. Let $\epsilon = e^{\pi I/n}$ be a primitive nth root of -1. The points of Z_0 have projective coordinates $z_k = [\zeta^k : \epsilon : 0]$ for $0 \leq k \leq n-1$. The unramified cover $U^\circ \to V^\circ$ extends to an unramified cover $U^\circ \cup Z_0 \to V^\circ \cup \{\infty\}$. The boundary of the sheet U_k contains exactly one point of Z_0.

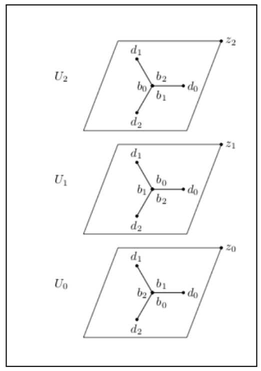
Lemma 3.1. *The point z_k is contained in the boundary of the sheet U_k.*

Proof. Consider the ray Q_k in U° given by $(x, y) = (\epsilon^{-1}\zeta^k \sqrt[n]{t}, \sqrt[n]{1+t})$ for $t \in (0, \infty)$. As $t \to 0$, it approaches $b = (0, 1)$ and it is contained in the sheet U_k. As $t \to \infty$, the value of x/y on Q_k approaches

$$\lim_{t\to\infty} \epsilon^{-1}\zeta^k \sqrt[n]{t} / \sqrt[n]{1+t} = \epsilon^{-1}\zeta^k.$$

The point z_k is at the end of the ray Q_k and is thus contained in the sheet U_k. □

FIGURE 1.



3.3. **The inertia type.** The inertia type of $\wp$ is $\vec{1}$, because $y^n = f(x)$ where $f(x) = -\prod_{i=0}^{n-1}(x - \zeta^i)^1$ is separable. This means that the canonical generator of inertia at each ramification point is ζ. Consider a loop L_i in V, with starting point $x = 0$, which makes a counterclockwise circle around the path w_i, starting in the region R_i and ending in R_{i+1}. Note that L_i depends only on the value of i modulo n. Let $L_{i,j}$ be the lift of L_i to a path in U° which starts at the point $(x,y) = (0, \zeta^j)$. By the definition of the inertia type, $L_{i,j}$ ends at the point $(x,y) = (0, \zeta^{j+1})$.

Lemma 3.2. *With notation as above, $\tilde{R}_{i,j} \subset U_k$ if and only if $i - j = k$.*

Proof. By definition, $\tilde{R}_{k,0} \subset U_k$. The path $L_{i,j}$ is contained in a unique sheet. Since $L_{i,j}$ starts in $\tilde{R}_{i,j}$ and ends in $\tilde{R}_{i+1,j+1}$, then these neighborhoods are contained in the same sheet. □

Note that $L_{i,j}$ is homotopic to the composition of paths

$$L_{i,j} = e_{i,j} \circ (e_{i,j+1})^{-1} \colon (0, \zeta^j) \mapsto (\zeta^i, 0) \mapsto (0, \zeta^{j+1}).$$

3.4. **Lifting of a star shape.** Recall that path composition is written from left to right. For $0 \le \ell \le n-1$, define a loop in V by:

$$S_\ell = L_{n-\ell} \circ L_{n-\ell+1} \circ \cdots \circ L_{n-\ell+(n-1)}. \tag{3.i}$$

Each loop S_ℓ traces in a counterclockwise direction along the outside of the slits $\{w_i\}$ and forms an n-pointed star shape. Each is homotopic to a large circle in V traced in a counterclockwise direction.

Definition 3.3. For $0 \le \ell \le n-1$, let $\tilde{S}_\ell$ denote the unique lift under $\wp$ of S_ℓ to a loop in U with starting point $b_0 = (0,1)$. Let $\tilde{S} := \tilde{S}_0 \circ \tilde{S}_1 \cdots \circ \tilde{S}_{n-1}$.

Note that $\tilde{S}_\ell$ is contained in $U_{n-\ell}$. Later, we will see that $\tilde{S} \in [\pi_1(U)]_2$, see Remark 4.5.

Lemma 3.4. *For $0 \le \ell \le n-1$, the loop $\tilde{S}_\ell$ is homotopic to*

$$\tilde{S}_\ell = e_{-\ell,0} \circ (e_{-\ell,1})^{-1} \circ e_{-\ell+1,1} \circ (e_{-\ell+1,2})^{-1} \circ \cdots \circ e_{-\ell+n-1,n-1} \circ (e_{-\ell+n-1,0})^{-1}.$$

Proof. The loop $\tilde{S}_\ell$ is homotopic to the composition of $2n$ of the edges $e_{i,j}$ and $(e_{i,j})^{-1}$. Because of the inertia type of $\wp$, this composition involves loops of the form $L_{i,j} = e_{i,j} \circ (e_{i,j+1})^{-1}$. The condition that $\tilde{S}_\ell$ is contained in $U_{n-\ell}$ implies that its initial edge is the path $e_{-\ell,0}$ from $(0,1)$ to $(\zeta^{-\ell}, 0)$. Thus the initial loop is $L_{-\ell,0} = e_{-\ell,0} \circ (e_{-\ell,1})^{-1}$. Consider the loop $L_{i',j'}$ coming after the loop $L_{i,j}$. Then $i' = i+1$ because $\tilde{S}_\ell$ circles counterclockwise around the point $(\zeta^i, 0)$. Also $j' = j+1$ because the starting point $(0, \zeta^{j'})$ of $L_{i',j'}$ is the same as the ending point $(0, \zeta^{j+1})$ of $L_{i,j}$. □

For example, $\tilde{S}_0$ passes around the points in this order:

$$(0,1) \to (1,0) \to (0,\zeta) \to (\zeta, 0) \to (0, \zeta^2) \to \cdots \to (\zeta^{n-1}, 0) \to (0,1),$$

and

$$\tilde{S}_0 = e_{0,0} \circ (e_{0,1})^{-1} \circ e_{1,1} \circ (e_{1,2})^{-1} \circ \cdots \circ e_{n-1,n-1} \circ (e_{n-1,0})^{-1}.$$

3.5. **Comparison with loops around cusps with $z = 0$.** We prove that $\tilde{S}$ is path homotopic to the boundary of a disk containing the n cusps of Z_0 and that $\tilde{S}_\ell$ can be taken to be the loop $(c_{n-\ell})^{-1}$ in a standard presentation of $\pi_1(U)$ (a presentation of the form (2.d)). For $0 \le j \le n-1$, let $z_j = [\zeta^j : \epsilon : 0]$.

Proposition 3.5. *The loop $\tilde{S}_\ell$ is homotopic to the clockwise loop bounding a disk containing $z_{n-\ell}$.*

Proof. Note that V° is homeomorphic to $\mathbb{A}^1 - \{0\}$ and S_ℓ is homotopic to a counterclockwise loop around 0. Thus S_ℓ is homotopic to a clockwise loop around ∞. By definition, the lift $\tilde{S}_\ell$ of S_ℓ is a loop in $U_{n-\ell}$. The restriction of $\wp$ to $U_{n-\ell}$ yields a homeomorphism $U_{n-\ell} \to V^\circ$. Thus $\tilde{S}_\ell$ is a clockwise loop around the point missing from $U_{n-\ell}$. By Lemma 3.1, this point is $z_{n-\ell}$. □

Proposition 3.6. *The loop $\tilde{S}$ is homotopic to the boundary of a disk in the Fermat curve which contains the n points where $z = 0$; it follows that we may take a presentation of the form (2.d) where $\tilde{S}_\ell = (c_{n-\ell})^{-1}$ and $\tilde{S} = (c_1 \circ \cdots \circ c_{n-1} \circ c_0)^{-1}$.*

In the following proof, it is convenient to use a small ball around b_0 as our basepoint b_0 (which we may do because balls are simply connected). The intersection of this ball with $\tilde{R}_{i,0}$ will then be called *the fractional point of b_0 in the region $\tilde{R}_{i,0}$*.

Proof. The loop $\tilde{S}_0$ in U_0 starts and ends at the fractional point b_0 in the region $\tilde{R}_{0,0}$. With a small homotopy adjustment, the end of $\tilde{S}_0$ can cross the path $e_{n-1,0}$ rather than return to the point b_0. Since the sheet U_0 is glued to the sheet U_{n-1} along the edge $e_{n-1,0}$, this yields an ending point in the region $\tilde{R}_{n-1,0}$ near the fractional point b_0 in the sheet U_{n-1}.

The loop $\tilde{S}_1$ in U_{n-1} starts and ends at the fractional point b_0 in the region $\tilde{R}_{n-1,0}$. With a small homotopy adjustment, the end of $\tilde{S}_1$ can cross the path $e_{n-2,0}$ rather than return to the point b_0. Since the sheet U_{n-1} is glued to the sheet U_{n-2} along the edge $e_{n-2,0}$, this yields an ending point in the region $\tilde{R}_{n-2,0}$ near the fractional point b_0 in the sheet U_{n-2}.

We continue in this way through all the loops $\tilde{S}_0 \circ \tilde{S}_1 \circ \cdots \circ \tilde{S}_{n-1}$. Finally, with a small homotopy adjustment, the end of $\tilde{S}_{n-1}$ crosses the path $e_{0,0}$ and returns to the region $\tilde{R}_{0,0}$ in U_0. Thus $\tilde{S}$ is path homotopic to a loop in the Fermat curve X composed of n paths each contained on a single U_k of the form shown in Figure 2 for $n = 3$.

This path divides X into an external and internal piece, where the internal piece contains the ramification points $\{d_i \mid 0 \le i \le n-1\}$, and the external piece contains Z_0 and is homeomorphic to a disk. (To see that the external piece is homeomorphic to a disk, note the following. The external piece is the union of n pieces, each homotopic to a wedge, which are glued together along the edges of the wedges. The picture for $n = 3$ is illustrated in Figure 2.)

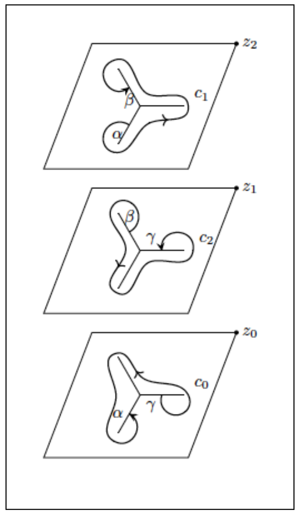
Applying Proposition 3.5, it follows that we can take a presentation of the form (2.d) where $\tilde{S}_\ell = (c_{n-\ell})^{-1}$. Thus $\tilde{S} = (c_0)^{-1} \circ (c_{n-1})^{-1} \circ \cdots \circ (c_1)^{-1} = (c_1 \circ \cdots \circ c_{n-1} \circ c_0)^{-1}$. □

The difference between $(c_0 \circ c_1 \circ \cdots c_{n-1})^{-1}$ and $(c_1 \circ \cdots \circ c_{n-1} \circ c_0)^{-1}$ is not significant by Lemma 2.3(1).

Lemma 3.7. *Let S^* (resp. S^*_ℓ) be the element of $\pi_1(U)$ obtained by substituting $E_{i,j}$ for the path $e_{i,j}$ in $\tilde{S}$ (resp. $\tilde{S}_\ell$). Then S^* and $\tilde{S}$ (resp. S^*_ℓ and $\tilde{S}_\ell$) are homotopic in $\pi_1(U)$.*

Proof. We fix the path $e_{0,0} \circ e_{0,j}^{-1}$ from b_0 to b_j, the initial point of $e_{i,j}$. We fix the path $e_{i,0}$ from b_0 to d_i, the final point of $e_{i,j}$. In the composition of paths, after completing each path $e_{i,j}$, we return to the base point b_0 and then return to the initial point of the next path. This does not change the homotopy class. □

FIGURE 2.



3.6. Combinatorial analysis.

Lemma 3.8. *The loop $\tilde{S}$ is the composition of $2n^2$ paths, with each path $e_{i,j}$ and each path $(e_{i,j})^{-1}$ occuring exactly once.*

Proof. Immediate from Lemma 3.4. □

We begin a combinatorial analysis of the ordering of the elements $E_{i,j}$ and $E_{i,j}^{-1}$ in S^*, viewed as a cycle, rather than a word. For $1 \leq j \leq n-1$ and $0 \leq a \leq n-2$, let $\overline{j+a}$ be the unique value in $\{1, \dots, n-1\}$ congruent to $j+a$ modulo $n-1$.

Proposition 3.9. *The ordering of the elements $E_{i,j}$ and $E_{i,j}^{-1}$ in the cycle S^* satisfies the following:*

(1) *The edges between $E_{1,1}^{-1}$ and $E_{1,1}$ are:*
$$f_1 := E_{2,1} \circ (E_{2,2})^{-1} \circ \cdots \circ E_{n-1,n-2} \circ (E_{n-1,n-1})^{-1}.$$

(2) *The edges between $E_{1,j}^{-1}$ and $E_{1,j}$ are:*
$$f_j := E_{2,\overline{j}} \circ (E_{2,\overline{j+1}})^{-1} \circ \cdots \circ E_{n-1,\overline{j+n-3}} \circ (E_{n-1,\overline{j+n-2}})^{-1}.$$

(3) *For $1 \leq i, j \leq n-1$, the edges $E_{i',j'}$ between $E_{i,j}^{-1}$ and $E_{i,j}$ with $i' \geq i$ are:*
$E_{i',j'}$ with $i < i' \leq n-1$ and $i' - j' \equiv i - j + 1 \bmod n-1$; and
$(E_{i',j'})^{-1}$ with $i < i' \leq n-1$ and $i' - j' \equiv i - j \bmod n-1$.

Proof. Item (1) is a special case of (2), which is a special case of (3), which follows from Lemma 3.4. □

4. The homology of the Fermat curve

The homology of the Fermat curve has been studied from many perspectives, see e.g., [Gro78, appendix] and [Lim91, Section 4]. By [Gro78, Theorem 1, appendix], $\mathrm{H}_1(X)$ is a cyclic Λ_1-module, where $\Lambda_1 = \mathbb{Z}[\mu_n \times \mu_n]$, and the annihilator of $\mathrm{H}_1(X)$ in Λ_1 can be found in [Gro78, page 210] and [Lim91, Proposition 4.1]. The facts about the structure of $\mathrm{H}_1(U)$ and $\mathrm{H}_1(X)$ in this section will be familiar to the experts.

In this paper, we follow an approach which is compatible with the results in [And87], [DPSW16], and [DPSW18] about the étale homology with coefficients in $\mathbb{Z}/n\mathbb{Z}$ and the action of the absolute Galois group upon it, see Section 6.

To study $\mathrm{H}_1(U)$, we use the homomorphism from the fundamental groupoid to $\mathrm{H}_1(U, Y)$, which sends composition to addition.

4.1. **A basis for the homology of X.** Let $\Lambda_1 = \mathbb{Z}[\mu_n \times \mu_n]$ and let $[\epsilon]_0$ and $[\epsilon]_1$ denote the generators of $\mu_n \times \mu_n$. Let $A_1 = \langle ([\epsilon]_0 - 1)([\epsilon]_1 - 1)\rangle \subset \Lambda_1$ denote the augmentation ideal.

Let $[e_{i,j}]$ (resp. $[E_{i,j}]$) denote the class of $e_{i,j}$ (resp. $E_{i,j}$) in the relative homology $\mathrm{H}_1(U, Y)$. Note that $[e_{i,j}] = [\epsilon]_0^i[\epsilon]_1^j\beta$. Also

$$[E_{i,j}] = [e_{0,0}] - [e_{i,0}] - [e_{0,j}] + [e_{i,j}]. \tag{4.j}$$

Using modular symbols, Ejder proves in [Ejd19, Theorem 1.2] that a basis for $\mathrm{H}_1(X)$ is given by

$$\{[\epsilon]_0^i[\epsilon]_1^j(1 - [\epsilon]_0)(1 - [\epsilon]_1)\beta \mid 1 \le i \le n - 2,\ 0 \le j \le n - 2\}. \tag{4.k}$$

In our notation, that means that a basis for $\mathrm{H}_1(X)$ is given by

$$\{[\epsilon]_0^i[\epsilon]_1^j[E_{1,1}] \mid 1 \le i \le n - 2,\ 0 \le j \le n - 2\}. \tag{4.l}$$

4.2. **Facts about the homology of the affine curve.** Next we find a basis for $\mathrm{H}_1(U)$.

Lemma 4.1. *The elements $[E_{i,j}]$ from (4.j) are in $\mathrm{H}_1(U)$ and the set $\{[E_{i,j}] \mid 1 \le i, j \le n - 1\}$ is a basis for $\mathrm{H}_1(U)$.*

Proof. The first claim is true because $[E_{i,j}]$ is the image of a path in the fundamental groupoid starting and ending at the same point.

We first show that $\{[E_{i,j}] \mid 1 \le i, j \le n - 1\}$ is a basis for $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$. There is an isomorphism $\mathrm{H}_1(U, Y; \mathbb{Z}/n\mathbb{Z}) \cong \Lambda_1 \otimes (\mathbb{Z}/n\mathbb{Z})$, taking $\beta \mapsto 1$, [And87, Theorem 6]. Thus $\{[e_{i,j}] \mid 0 \le i, j \le n - 1\}$ is a basis for $\mathrm{H}_1(U, Y; \mathbb{Z}/n\mathbb{Z})$.

Consider the augmentation ideal $A_1 \otimes \mathbb{Z}/n\mathbb{Z} \subset \Lambda_1 \otimes \mathbb{Z}/n\mathbb{Z}$. If $\alpha \in \Lambda_1 \otimes \mathbb{Z}/n\mathbb{Z}$, write $\alpha = \sum_{i,j} a_{i,j}[\epsilon]_0^i[\epsilon]_1^j$. One can check that $\alpha \in A_1 \otimes \mathbb{Z}/n\mathbb{Z}$ if and only if the rows and columns of the matrix $[a_{i,j}]$ sum to 0 modulo n. By [DPSW16, Proposition 6.2], $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z}) \cong A_1 \otimes \mathbb{Z}/n\mathbb{Z}$.

The element $[e_{i,j}]$ appears in $[E_{i',j'}]$ if and only if $i' = i$ and $j' = j$. It follows that $\{[E_{i,j}] \mid 1 \le i, j \le n - 1\}$ is a set of linearly independent elements in $\mathrm{H}_1(U, Y; \mathbb{Z}/n\mathbb{Z})$, and thus also in $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$. Their span contains $n^{((n-1)^2)}$ elements of $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$. Since $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$ has rank $(n - 1)^2$, this span is the entirety of $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$. This completes the proof that $\{[E_{i,j}] \mid 1 \le i, j \le n - 1\}$ is a basis for $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$.

It follows that $\{[E_{i,j}] \mid 1 \le i, j \le n-1\}$ is a set of linearly independent elements in $\mathrm{H}_1(U)$. Consider the span of the image of this set in $\mathrm{H}_1(X)$. This span contains $[E_{1,1}]$ and is a Λ_1-module, thus contains $[\epsilon]_0^i[\epsilon]_1^j[E_{1,1}]$. By (4.l), the image of this set spans $\mathrm{H}_1(X)$.

To complete the proof, we need to show that $\{[E_{i,j}] \mid 1 \le i, j \le n - 1\}$ spans the kernel of $\mathrm{H}_1(U) \to \mathrm{H}_1(X)$. A basis for the kernel is $\{\bar{c_j} \mid 0 \le j \le n - 1\}$. By Proposition 3.5, the loop $\tilde{S}_\ell$ is homotopic to the clockwise loop bounding a disk containing $z_{n-\ell}$. Thus a basis for the kernel is the set of images of $\tilde{S}_\ell$ in $\mathrm{H}_1(U)$. By Lemma 3.4, $\tilde{S}_\ell$ is homotopic to a loop with a formula written in terms of $e_{i,j}$. By Lemma 3.7, the same is true after replacing $e_{i,j}$ by $E_{i,j}$. Also $E_{i,j} = 0$ if $ij = 0$. Thus the set of images of $\tilde{S}_\ell$ in $\mathrm{H}_1(U)$ is generated by $\{[E_{i,j}] \mid 1 \le i, j \le n - 1\}$. This completes the proof. □

By Lemma 4.1, there is an injection $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U) \to \Lambda_1 \wedge_{\mathbb{Z}} \Lambda_1$ and an isomorphism

$$\mathrm{H}_1(U) \wedge \mathrm{H}_1(U) \to A_1 \wedge_{\mathbb{Z}} A_1.$$

Lemma 4.2. *Consider the index set*

$$I = \{(i_1, j_1, i_2, j_2) \mid 1 \le i_1, i_2, j_1, j_2 \le n - 1,\ i_1 \le i_2,\ \text{and if } i_1 = i_2 \text{ then } j_1 < j_2\}. \tag{4.m}$$

Then $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ is a free $\mathbb{Z}$-module with basis $\{[E_{i_1,j_1}] \wedge [E_{i_2,j_2}] \mid (i_1, j_1, i_2, j_2) \in I\}$.

Proof. By Lemma 4.1, $\mathrm{H}_1(U)$ is a free $\mathbb{Z}$-module of rank $m := (n-1)^2$ with basis $\{[E_{i_1,j_1}] \mid 1 \le i_1, j_1 \le n-1\}$. Then $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ is a free $\mathbb{Z}$-module of rank $\binom{m}{2}$. Because $z \wedge w = -w \wedge z$ and $z \wedge z = 0$, a basis is given by the set of simple wedges $[E_{i_1,j_1}] \wedge [E_{i_2,j_2}]$ with $i_1 \le i_2$ and $(i_1, j_1) \ne (i_2, j_2)$, which is indexed by I. □

4.3. **Facts about the homology of the projective curve.** We characterize $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ as a quotient of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ both for theoretical reasons and for the computational applications in Sections 7.1-7.3.

Lemma 4.3. *Suppose S is the kernel of $\mathrm{H}_1(U) \to \mathrm{H}_1(X)$. Then the kernel of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U) \to \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ equals $S \wedge \mathrm{H}_1(U)$.*

Proof. Since $\mathrm{H}_1(X)$ is a free module, the quotient map $\mathrm{H}_1(U) \to \mathrm{H}_1(X)$ splits, giving a direct sum decomposition $\mathrm{H}_1(U) \cong \mathrm{H}_1(X) \oplus S$, where S, $\mathrm{H}_1(X)$ and $\mathrm{H}_1(U)$ are all free modules. The wedge of the direct sum decomposes as $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U) \cong (\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)) \oplus (\mathrm{H}_1(X) \wedge S) \oplus (S \wedge S)$, showing the claim. □

We need an explicit description of $\mathrm{H}_1(X)$ as a quotient of $\mathrm{H}_1(U)$ for the computational applications in Sections 7.1-7.3. Define $\gamma_i \in \Lambda_1$ by the formula

$$\gamma_i = [\epsilon]_0^{-i}(1 - [\epsilon]_1)(1 + [\epsilon]_0[\epsilon]_1 + \cdots + [\epsilon]_0^{n-1}[\epsilon]_1^{n-1}). \tag{4.n}$$

Lemma 4.4. *The set $\{\gamma_i\beta \mid 1 \le i \le n-1\}$ is a basis for $\mathrm{Ker}(\mathrm{H}_1(U) \to \mathrm{H}_1(X))$.*

Proof. By Proposition 3.5, a basis for the kernel of $\mathrm{H}_1(U) \to \mathrm{H}_1(X)$ is the set of images of $\tilde{S}_\ell$ in $\mathrm{H}_1(U)$. Using Lemma 3.4, one can check that $\gamma_\ell\beta$ is the image of $\tilde{S}_\ell$ under the map $\pi_1(U) \to \mathrm{H}_1(U)$. Thus $\{\gamma_i\beta \mid 1 \le i \le n-1\}$ is a basis for the kernel of $\mathrm{H}_1(U) \to \mathrm{H}_1(X)$. □

Remark 4.5. Since $\gamma_\ell\beta$ is the image of $\tilde{S}_\ell$, one can see that the image of $\tilde{S}$ is $\sum_{\ell=0}^{n-1} \gamma_\ell\beta = 0$. Thus $\tilde{S} \in [\pi_1(U)]_2$.

4.4. **Properties of the classifying element ρ.** The classifying element $\rho \in \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ satisfies the following invariance property for the geometric action of automorphisms in $\mathrm{Aut}(X)$. See Proposition 6.2 for an invariance property for the arithmetic action of automorphisms in the absolute Galois group $G_{\mathbb{Q}}$.

Proposition 4.6. *Let ρ be a generator for the image of $\mathrm{H}_2(X) \to \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$. If $\phi \in \mathrm{Aut}(X)$, then $\phi(\rho) = \rho$.*

Proof. Every algebraic automorphism ϕ of $X(\mathbb{C})$ is orientation-preserving and preserves the fundamental class in $\mathrm{H}_2(X(\mathbb{C}))$. It follows that ϕ preserves the fundamental class in $\mathrm{H}_2(X)$. □

By [Tze95], or [Leo96], if $n \ge 4$, then $|\mathrm{Aut}(X)| = 6n^2$. We will apply Proposition 4.6 to:

(1) the automorphisms $\phi_0([x : y : z]) = [\zeta x : y : z]$ and $\phi_1([x : y : z]) = [x : \zeta y : z]$ which act on $\mathrm{H}_1(U, Y)$ via multiplication by $[\epsilon]_0$ and $[\epsilon]_1$ respectively. So ρ is invariant under the action of Λ_1.

(2) the transposition $\tau([x : y : z]) = [y : x : z]$, which acts on $\mathrm{H}_1(U, Y)$ by the ring automorphism of Λ_1 that switches $[\epsilon]_0$ and $[\epsilon]_1$. So ρ is symmetric.

(3) the 3-cycle $\omega([x : y : z]) = [z : -x : y]$; this automorphism does not stabilize U and Y.

5. Main result

In this section, we complete the analysis of the structure of $\mathrm{gr}(\pi)$ as a graded Lie algebra, by finding a formula for the element $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ that maps to $\rho \in \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$. Then we give some examples for $n = 3, 4, 5$.

5.1. **Proof of the main result.** By Lemma 4.2, with I defined as in (4.m), $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ is a free $\mathbb{Z}$-module with basis $\{[E_{i_1,j_1}] \wedge [E_{i_2,j_2}] \mid (i_1, j_1, i_2, j_2) \in I\}$. Thus there exist $\epsilon(i_1, j_1, i_2, j_2) \in \mathbb{Z}$, such that $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ can be uniquely represented as the linear combination

$$\Delta = \sum_{(i_1,j_1,i_2,j_2)\in I} \epsilon(i_1, j_1, i_2, j_2)[E_{i_1,j_1}] \wedge [E_{i_2,j_2}].$$

Theorem 1.1 follows immediately from the next result.

Theorem 5.1. *In $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$, the coefficient $\epsilon(i_1, j_1, i_2, j_2)$ of the basis element $[E_{i_1,j_1}] \wedge [E_{i_2,j_2}]$ in Δ is*

$$\epsilon(i_1, j_1, i_2, j_2) = \begin{cases} 1 & \text{if } j_2 - j_1 \equiv i_2 - i_1 \not\equiv 0 \bmod n-1, \\ -1 & \text{if } j_2 - j_1 + 1 \equiv i_2 - i_1 \not\equiv 0 \bmod n-1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Recall that $T = \prod_{i=1}^{g}[a_i, b_i] = (c_0 \circ c_1 \circ \cdots c_{n-1})^{-1}$. By Lemma 2.2, if $r_1, \dots, r_N, s_1 \dots, s_N \in \pi_1(U)$ are such that $T = [r_1, s_1] \circ \cdots \circ [r_N, s_N]$, then $\Delta = \sum_{i=1}^{N} \bar{r}_i \wedge \bar{s}_i$ in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$. By Proposition 3.6, $\tilde{S}$ is homotopic to $(c_1 \circ \cdots \circ c_{n-1} \circ c_0)^{-1}$. By Lemma 2.3(1), $\tilde{S}$ and T have the same image in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$. By Lemma 3.7, S^* is homotopic to $\tilde{S}$. It thus suffices to express $\tilde{S}$ as a product of commutators.

By Lemma 2.3(1), the image of S^* in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ depends only its equivalence class as a cycle rather than a word. By Proposition 3.9, the ordering of the elements $E_{i,j}$ and $E_{i,j}^{-1}$ in S^* is:

$$(E_{1,1}^{-1} \circ f_1 \circ E_{1,1}) \circ (E_{1,2}^{-1} \circ f_2 \circ E_{1,2}) \circ \cdots \circ (E_{1,n-1}^{-1} \circ f_{n-1} \circ E_{1,n-1}),$$

where f_j is defined in Proposition 3.9.

By Lemma 2.3(2), Δ is the sum of

$$[E_{1,1}] \wedge (-f_1) + \cdots + [E_{1,n-1}] \wedge (-f_{n-1}), \tag{5.o}$$

and the image of $\tilde{f} := f_1 \circ \cdots \circ f_{n-1}$ in $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$.

Note that $E_{1,j}$ and $E_{1,j}^{-1}$ do not appear in $\tilde{f}$ for any j. Thus the coefficient of $[E_{1,j}] \wedge [E_{i_2,j_2}]$ is zero unless E_{i_2,j_2} or its inverse appears in f_j. In particular, it is zero if $i_2 = 1$. For $i_2 \neq 1$, by the definition of f_j, the coefficient of $[E_{1,j}] \wedge [E_{i_2,j_2}]$ is $+1$ if $j_2 - i_2 = j - 1$ and is -1 if $j_2 - i_2 = j - 2$. This is equivalent to the coefficient being $+1$ if $j_2 - j_1 \equiv i_2 - 1 \not\equiv 0 \bmod n-1$ and being -1 if $j_2 - j_1 + 1 \equiv i_2 - i_1 \not\equiv 0 \bmod n-1$, which is the claimed statement for $i_1 = 1$.

Furthermore, the ordering of the edges in the cycle $\tilde{f}$ is the same as for the cycle S^*, except the edges $e_{1,j}$ and $e_{1,j}^{-1}$ do not appear. Using Proposition 3.9(3) and repeating the argument shows that the statement is true for $i = 2$. The result follows by induction. □

Remark 5.2. For $p = 5$, we were able to independently verify using Magma [BCP97] that the image of Δ generates $\langle\rho\rangle$ in $\mathrm{H}_1(X)\wedge\mathrm{H}_1(X)$; see Section 7.1. This uses the invariance properties from Propositions 4.6 and 6.2 and the explicit formulas for the Galois action from [DPSW18, Theorem 1.1], [DPSW16, Theorem 1.1].

Remark 5.3. The combinatorial description of $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ can be related with the ring of cliques as follows. Consider the graph whose vertices are indexed by the $(n-1)^2$ elements $[E_{i,j}]$ of the basis of $\mathrm{H}_1(U)$. Place these vertices on $n-1$ levels indexed by the value of $j-i \bmod n-1 \in \{0, \dots, n-2\}$. Elements $[E_{i_1,j_1}] \wedge [E_{i_2,j_2}]$ of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ can be indexed by a subset of edges in this graph. The elements in Δ yield the complete graph K_{n-1} on each level; also each vertex on level i is connected to $n-2$ vertices from levels $i-1 \bmod n-1$ and $i+1 \bmod n-1$.

5.2. **Examples.** In Sections 5.2.1-5.2.3, we illustrate the process of finding Δ when $n = 3, 4, 5$; of course, the results match the formula for Δ found in Theorem 1.1.

5.2.1. *The case* $n = 3$. Let $\zeta = e^{2\pi I/3}$. By Lemma 3.4:

$$\begin{aligned}
\tilde{S}_0 &= (0,1) \mapsto (1,0) \mapsto (0,\zeta) \mapsto (\zeta,0) \mapsto (0,\zeta^2) \mapsto (\zeta^2,0) \mapsto (0,1) \\
&= e_{0,0} \circ e_{0,1}^{-1} \circ e_{1,1} \circ e_{1,2}^{-1} \circ e_{2,2} \circ e_{2,0}^{-1};
\end{aligned}$$

$$\begin{aligned}
\tilde{S}_1 &= (0,1) \mapsto (\zeta^2,0) \mapsto (0,\zeta) \mapsto (1,0) \mapsto (0,\zeta^2) \mapsto (\zeta,0) \mapsto (0,1) \\
&= e_{2,0} \circ e_{2,1}^{-1} \circ e_{0,1} \circ e_{0,2}^{-1} \circ e_{1,2} \circ e_{1,0}^{-1}; \text{ and}
\end{aligned}$$

$$\begin{aligned}
\tilde{S}_2 &= (0,1) \mapsto (\zeta,0) \mapsto (0,\zeta) \mapsto (\zeta^2,0) \mapsto (0,\zeta^2) \mapsto (1,0) \mapsto (0,1) \\
&= e_{1,0} \circ e_{1,1}^{-1} \circ e_{2,1} \circ e_{2,2}^{-1} \circ e_{0,2} \circ e_{0,0}^{-1}.
\end{aligned}$$

By Lemma 3.7,

$$\begin{aligned}
S^* &= E_{0,0} \circ E_{0,1}^{-1} \circ E_{1,1} \circ E_{1,2}^{-1} \circ E_{2,2} \circ E_{2,0}^{-1} \circ \\
&\quad E_{2,0} \circ E_{2,1}^{-1} \circ E_{0,1} \circ E_{0,2}^{-1} \circ E_{1,2} \circ E_{1,0}^{-1} \circ \\
&\quad E_{1,0} \circ E_{1,1}^{-1} \circ E_{2,1} \circ E_{2,2}^{-1} \circ E_{0,2} \circ E_{0,0}^{-1} \\
&= E_{1,1} \circ E_{1,2}^{-1} \circ E_{2,2} \circ E_{2,1}^{-1} \circ E_{1,2} \circ E_{1,1}^{-1} \circ E_{2,1} \circ E_{2,2}^{-1}.
\end{aligned}$$

By Lemma 2.3(1), in $[\pi_1(U)]_2/[\pi_1(U)]_3$, the image of S^* is the same as the image of

$$(E_{1,1}^{-1} \circ E_{2,1} \circ E_{2,2}^{-1} \circ E_{1,1}) \circ (E_{1,2}^{-1} \circ E_{2,2} \circ E_{2,1}^{-1} \circ E_{1,2}).$$

By Lemma 2.3(2),

$$\begin{aligned}
\Delta &= E_{1,1} \wedge (E_{2,2} - E_{2,1}) + E_{1,2} \wedge (E_{2,1} - E_{2,2}) \\
&= E_{1,1} \wedge E_{2,2} - E_{1,1} \wedge E_{2,1} + E_{1,2} \wedge E_{2,1} - E_{1,2} \wedge E_{2,2}.
\end{aligned}$$

5.2.2. *The case* $n = 4$. Let $\zeta = e^{2\pi I/4}$. By Lemma 3.4:

$$\begin{aligned}
\tilde{S}_0 &= (0,1) \mapsto (1,0) \mapsto (0,\zeta) \mapsto (\zeta,0) \mapsto (0,\zeta^2) \mapsto (\zeta^2,0) \mapsto (0,\zeta^3) \mapsto (\zeta^3,0) \mapsto (0,1) \\
&= e_{0,0} \circ e_{0,1}^{-1} \circ e_{1,1} \circ e_{1,2}^{-1} \circ e_{2,2} \circ e_{2,3}^{-1} \circ e_{3,3} \circ e_{3,0}^{-1};
\end{aligned}$$

$$\begin{aligned}
\tilde{S}_1 &= (0,1) \mapsto (\zeta^3,0) \mapsto (0,\zeta) \mapsto (1,0) \mapsto (0,\zeta^2) \mapsto (\zeta,0) \mapsto (0,\zeta^3) \mapsto (\zeta^2,0) \mapsto (0,1) \\
&= e_{3,0} \circ e_{3,1}^{-1} \circ e_{0,1} \circ e_{0,2}^{-1} \circ e_{1,2} \circ e_{1,3}^{-1} \circ e_{2,3} \circ e_{2,0}^{-1};
\end{aligned}$$

$$\begin{aligned}
\tilde{S}_2 &= (0,1) \mapsto (\zeta^2,0) \mapsto (0,\zeta) \mapsto (\zeta^3,0) \mapsto (0,\zeta^2) \mapsto (1,0) \mapsto (0,\zeta^3) \mapsto (\zeta,0) \mapsto (0,1) \\
&= e_{2,0} \circ e_{2,1}^{-1} \circ e_{3,1} \circ e_{3,2}^{-1} \circ e_{0,2} \circ e_{0,3}^{-1} \circ e_{1,3} \circ e_{1,0}^{-1}; \text{ and}
\end{aligned}$$

$$\begin{aligned}
\tilde{S}_3 &= (0,1) \mapsto (\zeta,0) \mapsto (0,\zeta) \mapsto (\zeta^2,0) \mapsto (0,\zeta^2) \mapsto (\zeta^3,0) \mapsto (0,\zeta^3) \mapsto (1,0) \mapsto (0,1) \\
&= e_{1,0} \circ e_{1,1}^{-1} \circ e_{2,1} \circ e_{2,2}^{-1} \circ e_{3,2} \circ e_{3,3}^{-1} \circ e_{0,3} \circ e_{0,0}^{-1}.
\end{aligned}$$

By Lemma 3.7,

$$\begin{aligned}
S^* &= E_{1,1} \circ E_{1,2}^{-1} \circ E_{2,2} \circ E_{2,3}^{-1} \circ E_{3,3} \circ E_{3,1}^{-1} \circ E_{1,2} \circ E_{1,3}^{-1} \circ E_{2,3} \circ \\
&\quad E_{2,1}^{-1} \circ E_{3,1} \circ E_{3,2}^{-1} \circ E_{1,3} \circ E_{1,1}^{-1} \circ E_{2,1} \circ E_{2,2}^{-1} \circ E_{3,2} \circ E_{3,3}^{-1}.
\end{aligned}$$

By Lemma 2.3(1), in $[\pi_1(U)]_2/[\pi_1(U)]_3$, the image of S^* is the same as the image of

$$\begin{aligned}
&(E_{1,1}^{-1} \circ E_{2,1} \circ E_{2,2}^{-1} \circ E_{3,2} \circ E_{3,3}^{-1} \circ E_{1,1}) \circ \\
&(E_{1,2}^{-1} \circ E_{2,2} \circ E_{2,3}^{-1} \circ E_{3,3} \circ E_{3,1}^{-1} \circ E_{1,2}) \circ \\
&(E_{1,3}^{-1} \circ E_{2,3} \circ E_{2,1}^{-1} \circ E_{3,1} \circ E_{3,2}^{-1} \circ E_{1,3}).
\end{aligned}$$

By Lemma 2.3(2),

$$\begin{aligned}\Delta &= E_{1,1}\wedge(E_{2,2}-E_{2,1}+E_{3,3}-E_{3,2})+\\ &E_{1,2}\wedge(E_{2,3}-E_{2,2}+E_{3,1}-E_{3,3})+\\ &E_{1,3}\wedge(E_{2,1}-E_{2,3}+E_{3,2}-E_{3,1})+\\ &E_{2,1}\wedge(E_{3,2}-E_{3,1})+\\ &E_{2,2}\wedge(E_{3,3}-E_{3,2})+\\ &E_{2,3}\wedge(E_{3,1}-E_{3,3}).\end{aligned}$$

5.2.3. *The case* $n=5$. Let $\zeta=e^{2\pi I/5}$. By Lemma 3.4:

$$\begin{aligned}\tilde{S}_0 &= (0,1)\mapsto(1,0)\mapsto(0,\zeta)\mapsto(\zeta,0)\mapsto(0,\zeta^2)\mapsto(\zeta^2,0)\mapsto(0,\zeta^3)\mapsto(\zeta^3,0)\mapsto(0,\zeta^4)\mapsto(\zeta^4,0)\mapsto(0,1)\\ &= e_{0,0}\circ e_{0,1}^{-1}\circ e_{1,1}\circ e_{1,2}^{-1}\circ e_{2,2}\circ e_{2,3}^{-1}\circ e_{3,3}\circ e_{3,4}^{-1}\circ e_{4,4}\circ e_{4,0}^{-1};\end{aligned}$$

$$\begin{aligned}\tilde{S}_1 &= (0,1)\mapsto(\zeta^4,0)\mapsto(0,\zeta)\mapsto(1,0)\mapsto(0,\zeta^2)\mapsto(\zeta,0)\mapsto(0,\zeta^3)\mapsto(\zeta^2,0)\mapsto(0,\zeta^4)\mapsto(\zeta^3,0)\mapsto(0,1)\\ &= e_{4,0}\circ e_{4,1}^{-1}\circ e_{0,1}\circ e_{0,2}^{-1}\circ e_{1,2}\circ e_{1,3}^{-1}\circ e_{2,3}\circ e_{2,4}^{-1}\circ e_{3,4}\circ e_{3,0}^{-1};\end{aligned}$$

$$\begin{aligned}\tilde{S}_2 &= (0,1)\mapsto(\zeta^3,0)\mapsto(0,\zeta)\mapsto(\zeta^4,0)\mapsto(0,\zeta^2)\mapsto(1,0)\mapsto(0,\zeta^3)\mapsto(\zeta,0)\mapsto(0,\zeta^4)\mapsto(\zeta^2,0)\mapsto(0,1)\\ &= e_{3,0}\circ e_{3,1}^{-1}\circ e_{4,1}\circ e_{4,2}^{-1}\circ e_{0,2}\circ e_{0,3}^{-1}\circ e_{1,3}\circ e_{1,4}^{-1}\circ e_{2,4}\circ e_{2,0}^{-1};\end{aligned}$$

$$\begin{aligned}\tilde{S}_3 &= (0,1)\mapsto(\zeta^2,0)\mapsto(0,\zeta)\mapsto(\zeta^3,0)\mapsto(0,\zeta^2)\mapsto(\zeta^4,0)\mapsto(0,\zeta^3)\mapsto(1,0)\mapsto(0,\zeta^4)\mapsto(\zeta,0)\mapsto(0,1)\\ &= e_{2,0}\circ e_{2,1}^{-1}\circ e_{3,1}\circ e_{3,2}^{-1}\circ e_{4,2}\circ e_{4,3}^{-1}\circ e_{0,3}\circ e_{0,4}^{-1}\circ e_{1,4}\circ e_{1,0}^{-1};\ \text{and}\end{aligned}$$

$$\begin{aligned}\tilde{S}_4 &= (0,1)\mapsto(\zeta,0)\mapsto(0,\zeta)\mapsto(\zeta^2,0)\mapsto(0,\zeta^2)\mapsto(\zeta^3,0)\mapsto(0,\zeta^3)\mapsto(\zeta^4,0)\mapsto(0,\zeta^4)\mapsto(1,0)\mapsto(0,1)\\ &= e_{1,0}\circ e_{1,1}^{-1}\circ e_{2,1}\circ e_{2,2}^{-1}\circ e_{3,2}\circ e_{3,3}^{-1}\circ e_{4,3}\circ e_{4,4}^{-1}\circ e_{0,4}\circ e_{0,0}^{-1}.\end{aligned}$$

By Lemma 3.7,

$$\begin{aligned}S^* &= E_{1,1}\circ E_{1,2}^{-1}\circ E_{2,2}\circ E_{2,3}^{-1}\circ E_{3,3}\circ E_{3,4}^{-1}\circ E_{4,4}\circ\\ &E_{4,1}^{-1}\circ E_{1,2}\circ E_{1,3}^{-1}\circ E_{2,3}\circ E_{2,4}^{-1}\circ E_{3,4}\circ\\ &E_{3,1}^{-1}\circ E_{4,1}\circ E_{4,2}^{-1}\circ E_{1,3}\circ E_{1,4}^{-1}\circ E_{2,4}\circ\\ &E_{2,1}^{-1}\circ E_{3,1}\circ E_{3,2}^{-1}\circ E_{4,2}\circ E_{4,3}^{-1}\circ E_{1,4}\circ\\ &E_{1,1}^{-1}\circ E_{2,1}\circ E_{2,2}^{-1}\circ E_{3,2}\circ E_{3,3}^{-1}\circ E_{4,3}\circ E_{4,4}^{-1}.\end{aligned}$$

By Lemma 2.3(1)-(2), in $[\pi_1(U)]_2/[\pi_1(U)]_3$, the image of S^* is

$$\begin{aligned}\Delta &= E_{1,1}\wedge(-E_{2,1}+E_{2,2}-E_{3,2}+E_{3,3}-E_{4,3}+E_{4,4})\\ &+E_{1,2}\wedge(-E_{2,2}+E_{2,3}-E_{3,3}+E_{3,4}-E_{4,4}+E_{4,1})\\ &+E_{1,3}\wedge(-E_{2,3}+E_{2,4}-E_{3,4}+E_{3,1}-E_{4,1}+E_{4,2})\\ &+E_{1,4}\wedge(-E_{2,4}+E_{2,1}-E_{3,1}+E_{3,2}-E_{4,2}+E_{4,3})\\ &+E_{2,1}\wedge(-E_{3,1}+E_{3,2}-E_{4,2}+E_{4,3})\\ &+E_{2,2}\wedge(-E_{3,2}+E_{3,3}-E_{4,3}+E_{4,4})\\ &+E_{2,3}\wedge(-E_{3,3}+E_{3,4}-E_{4,4}+E_{4,1})\\ &+E_{2,4}\wedge(-E_{3,4}+E_{3,1}-E_{4,1}+E_{4,2})\\ &+E_{3,1}\wedge(-E_{4,1}+E_{4,2})\\ &+E_{3,2}\wedge(-E_{4,2}+E_{4,3})\\ &+E_{3,3}\wedge(-E_{4,3}+E_{4,4})\\ &+E_{3,4}\wedge(E_{4,1}-E_{4,4}).\end{aligned}$$

6. The étale homology and action of the absolute Galois group

Let $K = \mathbb{Q}(\zeta_n)$. We consider X and U as curves over K. Let $Y \subset U$ be the set of $2n$ points where $xy = 0$. In this section, we denote the étale fundamental group by $\pi_1(U)$, the étale homology by $\mathrm{H}_1(U)$, and the relative étale homology by $\mathrm{H}_1(U, Y)$.

Remark 6.1. After choosing an embedding $K \subset \mathbb{C}$ and applying Riemann's Existence Theorem, we may identify the profinite completion of $\mathrm{H}_1(U(\mathbb{C}))$ with the étale homology $\mathrm{H}_1(U)$, and may identify $\mathrm{H}_1(U(\mathbb{C}); \mathbb{Z}/n\mathbb{Z})$ with $\mathrm{H}_1(U; \mathbb{Z}/n\mathbb{Z})$. Similarly, we may identify the profinite completion of $\pi_1(U(\mathbb{C}))$ with the étale fundamental group $\pi_1(U)$.

We therefore can consider the elements $a_i, b_i, c_j, T, E_{i,j}$ to be in $\pi_1(U)$ and $\bar{a}_i, \bar{b}_i, \bar{c}_j, [E_{i,j}]$ to be in $\mathrm{H}_1(U)$. Similarly, we may consider $\beta, e_{i,j}$ to be in the étale fundamental groupoid and $[e_{i,j}]$ to be in $\mathrm{H}_1(U, Y)$. Likewise, we can consider Δ to be an element of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ and its image ρ to be an element of $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$.

The results in Sections 2-5 about these elements remain true in this context as well. In particular, Theorem 1.1 is true in the context of the étale homology.

6.1. An arithmetic property of the action.

Proposition 6.2. *If $\sigma \in G_{\mathbb{Q}}$, then σ acts on ρ via the cyclotomic character: if $\sigma(\zeta) = \zeta^i$, then $\sigma(\rho) = \zeta^i \rho$. In particular, if $\sigma \in G_K$, then σ acts trivially on ρ.*

Proof. Recall that ρ is a generator for the image of $\mathrm{H}_2(X) \to \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$. The map $\mathrm{H}_2(X) \to \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ is $G_{\mathbb{Q}}$-equivariant. By the Weil conjectures, $\sigma \in G_{\mathbb{Q}}$ acts on $\mathrm{H}_2(X)$ via the cyclotomic character. The cyclotomic character is trivial when restricted to G_K. □

6.2. Explicit formulas for the action.

Let $n = p$ be a prime satisfying Vandiver's conjecture. In this section, we collect some information about the action of $G_{\mathbb{Q}}$ on $\mathrm{H}_1(U, Y; \mathbb{Z}/p\mathbb{Z})$.

By [And87, Section 10.5], the action of $\sigma \in G_K$ on the generator β for $\mathrm{H}_1(U, Y; \mathbb{Z}/p)$ factors through $Q = \mathrm{Gal}(L/K)$. For $q \in Q$, in [DPSW18, Theorem 1.1], the authors provide a completely explicit formula for the element $B_q \in \Lambda_1 \otimes \mathbb{Z}/p\mathbb{Z}$ such that $q \circ \beta = B_q \beta$.

Here is some partial information about how $\mathrm{Gal}(K/\mathbb{Q})$ acts on β. Let a be a primitive root modulo p. Let $\xi_a \in \mathrm{Gal}(K/\mathbb{Q})$ be the automorphism such that $\xi_a(\zeta_p) = \zeta_p^a$. It generates $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$. By [DPSW18, Lemma 2.2], $\mathrm{Gal}(L/\mathbb{Q})$ is a semi-direct product of the form $Q \rtimes (\mathbb{Z}/p\mathbb{Z})^*$. We fix the lifting $(1, \xi_a)$ of ξ_a in $\mathrm{Gal}(L/\mathbb{Q})$ and denote it also by ξ_a.

Since $\mathrm{H}_1(U, Y)$ is $G_{\mathbb{Q}}$-invariant, there exists $R_a \in \Lambda_1$ such that $\xi_a(\beta) = R_a \beta$. Modifying the lifting of ξ_a by $q \in Q$ changes R_a by multiplication by the element $B_q \in \Lambda_1$ from [DPSW18, Theorem 1.1]. By [And87, Theorem 7], R_a is symmetric. By [And87, Section 9.6], $R_a - 1$ is in the augmentation ideal $\langle y_0 y_1 \rangle$. This is because $\xi_a(\beta)$ and β have the same endpoints and so $R_a \beta - \beta$ is in $\mathrm{H}_1(U) = \langle y_0 y_1 \rangle \beta$. Also $R_a R_b = R_{ab}$.

Proposition 6.2 implies that $\xi_a(\rho) = a\rho$. To state one more property of R_a, we consider the permutation action on Λ_1 given by $\mathrm{perm}_a(\epsilon_0^i \epsilon_1^j) = \epsilon_0^{ai} \epsilon_1^{aj}$.

Lemma 6.3. *Let p be an odd prime and let a be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Then $\prod_{i=0}^{(p-1)/2-1} \mathrm{perm}_a^i(R_a) = 1$.*

Proof. The automorphism $\xi_a^{(p-1)/2}$ is the restriction of complex conjugation to K. This fixes β, since β is defined over $\mathbb{R}$. By induction, we check that $\xi_a^j(\beta) = (\prod_{i=0}^{j-1} \mathrm{perm}_a^i(R_a))\beta$. Thus

$$\beta = \xi_a^{(p-1)/2}(\beta) = \left(\prod_{i=0}^{(p-1)/2-1} \mathrm{perm}_a^i(R_a) \right) \beta.$$

□

If $p = 5$, the properties above determine the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z})$; see Section 7.1.

7. Examples

In Section 7.1, if $n = 5$, we verify the formula through an independent method using invariance properties. This method provides additional information that allows us to determine the action of $G_{\mathbb{Q}}$ on $\mathrm{H}_1(X)$ if $n = 5$, see Section 7.2. As a final application of the formula if $n = 5$, in Section 7.3, we compute the dimension of the G_K-invariant subspace of $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/5\mathbb{Z}$ and use it to show a coboundary map is trivial.

7.1. **An independent verification of the formula for ρ if $n = 5$.** In this section, we build on Section 4.4 to study the subspace of $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ which is invariant under $\mathrm{Aut}(X)$ and G_K. We use some additional information about the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{H}_1(X)$ to verify that the subspace $\langle\rho\rangle$ is uniquely determined by these invariance properties if $n = 5$.

The actions of $\phi \in \mathrm{Aut}(X)$ and $\sigma \in G_{\mathbb{Q}}$ on $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ can be computed from the corresponding actions on $\mathrm{H}_1(X)$ using the exterior wedge product. The following result is immediate from Propositions 4.6 and 6.2 and Lemma 4.3.

Proposition 7.1. *Let $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ be as in (2.e).*

(1) Then $[\epsilon]_0\Delta - \Delta$, $[\epsilon]_1\Delta - \Delta$, and $\tau\Delta - \Delta$ are in $S \wedge \mathrm{H}_1(U)$.

(2) If $\sigma \in G_K$, then $(\sigma - 1)\Delta \in S \wedge \mathrm{H}_1(U)$.

The actions of the automorphisms $[\epsilon]_0, [\epsilon]_1, \tau$ on $\mathrm{H}_1(U)$ and thus on $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ are straight-forward to compute using Magma.

For the 3-cycle $\omega \in \mathrm{Aut}(X)$, it is more complicated to determine the action of ω on $\mathrm{H}_1(X)$ since ω does not stabilize $\mathrm{H}_1(U)$. To check invariance under ω, we use a basis for $\mathrm{H}_1(X)$ found in [Ejd19, Theorem 1.2], together with information about how ω acts on $\mathrm{H}_1(X)$ found in [Ejd19, Section 4.3 and Proposition 5.1].

If n is a prime p satisfying Vandiver's conjecture, the action of $\sigma \in G_K$ on $\mathrm{H}_1(U)$ can be calculated. As explained in the introduction, the reason is that the action of σ factors through $Q = \mathrm{Gal}(L/K)$. In [DPSW18, Theorem 1.1], we gave an explicit formula for the action of each $q \in Q$ on $\mathrm{H}_1(U)$. This yields an explicit formula for the action of $q \in Q$ on $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ which can computed using Magma.

Let a be a primitive root modulo p. Consider the automorphism $\xi_a \in \mathrm{Gal}(L/\mathbb{Q})$ from Section 4.4 having the property that $\xi_a(\zeta) = \zeta^a$. Recall that $\xi_a(\beta) = R_a\beta$ for some $R_a \in \Lambda_1$ such that:
(i) $R_a - 1$ is in the augmentation ideal $\langle y_0y_1\rangle$;
(ii) R_a is symmetric; and
(iii) $\prod_{i=0}^{(p-1)/2-1} \mathrm{perm}_a^i(R_a) = 1$ (Lemma 6.3).
For $p > 3$, properties (i)-(iii) do not determine R_a but they do give partial information.

The invariance property for ρ under ξ_a is equivalent to

$$\xi_a(\Delta) - a\Delta \in S \wedge \mathrm{H}_1(U). \tag{7.p}$$

To compute ξ_a on an element $\alpha \in \mathrm{H}_1(U)\wedge\mathrm{H}_1(U)$, we write α as a sum of simple tensors $\alpha = \sum_{t\in\mathcal{T}} \alpha'_t\beta\wedge\alpha''_t\beta$, where $\mathcal{T}$ is a finite index set and $\alpha'_t, \alpha''_t \in \Lambda_1$. Then $\xi_a(\alpha) = \sum_{t\in\mathcal{T}} \mathrm{perm}_a(\alpha'_t)R_a\beta \wedge \mathrm{perm}_a(\alpha''_t)R_a\beta$.

If $p = 5$ and $a = 2$, we found all possible pairs (α, R_a) satisfying these conditions. Despite the ambiguity for R_a, we found that these conditions uniquely determine $\langle\rho\rangle$.

Definition 7.2. Let $\mathcal{A}$ be the subset of $\alpha \in \mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ which satisfy these properties:

(1) α is invariant under the action of G_K;

(2) α is invariant under the automorphisms $\phi_0, \phi_1, \tau, \omega$ of X.

Let $\mathcal{A}'$ be $\mathcal{A} \setminus \{\overline{0}\}$.

Definition 7.3. Let $\mathcal{R}$ be the set of $R_a \in \Lambda_1$ satisfying conditions (i)-(iii).

Proposition 7.4. *Let $n = 5$ and $a = 2$. There are exactly $n - 1 = 4$ values of $\alpha \in \mathcal{A}'$ for which there is an $R_a \in \mathcal{R}$ such that the pair (α, R_a) satisfies (7.p). These $\alpha \in \mathcal{A}'$ are exactly the non-zero multiples of the image in $\mathrm{H}_1(X) \wedge \mathrm{H}_1(X)$ of the element $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ found in Theorem 1.1.*

Proof. This is a Magma calculation [BCP97]. For $p = 5$, $\mathcal{A}$ is a 2-dimensional subspace of $H_1(X) \wedge H_1(X)$ and $\mathcal{R}$ is a set of size 125. Checking all pairs (α, R_a) for $\alpha \in \mathcal{A}'$ and $R_a \in \mathcal{R}$, there are 100 pairs satisfying (7.p). The same 25 possibilities for $R_a \in \mathcal{R}$ each appear 4 times as the second coordinate of the pair. ☐

We do not know if the analogue of Proposition 7.4 is true for $p > 5$.

7.2. **The action of $G_{\mathbb{Q}}$.** Furthermore, if $n = 5$ and $a = 2$, we have enough information about $R_a \in \mathcal{R}$ to determine the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathrm{H}_1(X)$.

Proposition 7.5. *Let $n = 5$ and $a = 2$. There are 25 possibilities for $R_a \in \mathcal{R}$ from the calculation in 7.4. Each of the 25 elements $R_a - 1$ has the same action on $H_1(X)$.*

Proof. Magma calculation [BCP97] ☐

Here is one of the possibilities for R_a:

$$\begin{aligned} R_{a,0} &= 4[\epsilon]_0^4[\epsilon]_1^3 + 4[\epsilon]_0^4[\epsilon]_1^2 + 2[\epsilon]_0^4[\epsilon]_1 + 3[\epsilon]_0^3[\epsilon]_1^2 + 4[\epsilon]_0^3[\epsilon]_1 + 4[\epsilon]_0^2[\epsilon]_1 + 4[\epsilon]_0^3 + 4[\epsilon]_0^2 \\ &+ 4[\epsilon]_0^3[\epsilon]_1^4 + 4[\epsilon]_0^2[\epsilon]_1^4 + 2[\epsilon]_0[\epsilon]_1^4 + 3[\epsilon]_0^2[\epsilon]_1^3 + 4[\epsilon]_0[\epsilon]_1^3 + 4[\epsilon]_0[\epsilon]_1^2 + 4[\epsilon]_1^3 + 4[\epsilon]_1^2 + 3. \end{aligned}$$

Write $y_0 = [\epsilon]_0 - 1$ and $y_1 = [\epsilon]_1 - 1$. Then

$$\begin{aligned} R_{a,0} &= 4y_0^4y_1^3 + y_0^4y_1^2 + 2y_0^4y_1 + y_0^3y_1^2 + 4y_0^3y_1 + 4y_0^2y_1 \\ &+ 4y_0^3y_1^4 + y_0^2y_1^4 + 2y_0y_1^4 + y_0^2y_1^3 + 4y_0y_1^3 + 4y_0y_1^2 + 2y_0^3y_1^3 + 2y_0y_1 + 1. \end{aligned}$$

The set of 25 possibilities for R_a in Proposition 7.5 is $\{R_{a,0} + iv_1 + jv_2 \mid i, j \in \{0, \ldots, 4\}\}$, where:

$$\begin{aligned} v_1 &= 2y_0^4y_1^4 + 3y_0^4y_1^2 + 3y_0^3y_1^3 + 3y_0^2y_1^4, \\ v_2 &= 2y_0^4y_1^4 + 3y_0^4y_1^3 + 2y_0^4y_1^2 + 3y_0^3y_1^4 + 2y_0^2y_1^4. \end{aligned}$$

Recall from Section 4.4 that R_a is well-defined after making a choice of automorphism ξ_a in $\mathrm{Gal}(L/\mathbb{Q})$ lifting the automorphism $\xi_a \in \mathrm{Gal}(K/\mathbb{Q})$. Changing ξ_a by $q \in Q$ changes R_a by multiplication by the element $B_q \in \Lambda_1$ found in [DPSW18, Theorem 1.1].

Suppose $\delta \in \mathrm{H}_1(X)^{G_K}$. Then δ is fixed by any automorphism $q \in \mathrm{Gal}(L/K)$. By definition, the action of q on δ is given by multiplication by B_q. Then $B_qR_a\delta = R_aB_q\delta = R_a\delta$ for any $q \in \mathrm{Gal}(L/K)$. This means that the action of $\mathrm{Gal}(L/\mathbb{Q})$ on $\mathrm{H}_1(X)^{G_K}$ does not depend on the choice involved in the definition for R_a.

Let J_5 be the Jacobian of the Fermat curve of degree 5. In [Tze97, Proposition, Corollary 2], Tzermias proved that $\dim_{\mathbb{Z}/5\mathbb{Z}}(J_5(\mathbb{Q}(\zeta_5))) = 8$ and $\dim_{\mathbb{Z}/5\mathbb{Z}}(J_5(\mathbb{Q})) = 2$. Since $J_5(L) \cong \mathrm{H}_1(X, \mathbb{Z}/5\mathbb{Z})^{G_L}$ for a number field L, our work allows us to give a new proof of these results of Tzermias.

Example 7.6. *If $n = 5$, the G_K-invariant subspace of $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ has dimension 8 and the $G_{\mathbb{Q}}$-invariant subspace of $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ has dimension 2.*

Proof. The action of G_K on $\mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z})$ factors through the field extension L/K where L is the splitting field of $1 - (1 - x^p)^p$. If $p = 5$, there are 3 generators τ_0, τ_1, τ_2 for $Q = \mathrm{Gal}(L/K)$. The formula for the action of each of these on $\mathrm{H}_1(U; \mathbb{Z}/5\mathbb{Z})$ can be found in [DPSW18, Example 3.8].

Let $\mathrm{Fix}([\epsilon]_0[\epsilon]_1) = \{\alpha \in \mathrm{H}_1(U; \mathbb{Z}/5\mathbb{Z}) \mid [\epsilon]_0[\epsilon]_1\alpha = \alpha\}$.

By [DPSW16, Proposition 6.3],

$$\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z}) = \mathrm{H}_1(U; \mathbb{Z}/5\mathbb{Z})/S \tag{7.q}$$

where $S = \mathrm{Fix}([\epsilon]_0[\epsilon]_1)$ †

† In [DPSW16, Proposition 6.3], we used the notation $\mathrm{Stab}([\epsilon]_0[\epsilon]_1)$ instead.

In Magma [BCP97] we computed the action of τ_0, τ_1, τ_2 on $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$. To determine the G_K-invariant subspace of $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$, we computed the intersection of the kernels of the 3 operators $\tau_i - 1$ for $i = 0, 1, 2$. For the $G_{\mathbb{Q}}$-invariant subspace, we computed the subspace of this intersection which is fixed by multiplication by R_a. □

7.3. **An application.** Let p be a prime satisfying Vandiver's Conjecture and let $K = \mathbb{Q}(\zeta_p)$. In [DPSW18, Theorem 1.1], we gave an explicit formula for the action of G_K on $\mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) = \pi/[\pi]_2 \otimes \mathbb{Z}/p\mathbb{Z}$. From the results in this paper, we obtain an explicit action of G_K on the higher quotients $[\pi]_m/[\pi]_{m+1} \otimes \mathbb{Z}/p\mathbb{Z}$ as well.

We would like to thank the referee for bringing this idea to our attention. Consider the short exact sequence

$$0 \to (\mathbb{Z}/p\mathbb{Z})\rho \to \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \to [\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z} \to 0.$$

Since Q fixes ρ, this yields a long exact sequence

$$(7.r) \quad 0 \to (\mathbb{Z}/p\mathbb{Z})\rho \to \mathrm{H}^0(Q; \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z})) \to \mathrm{H}^0(Q; [\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\delta} \mathrm{H}^1(Q; (\mathbb{Z}/p\mathbb{Z})\rho).$$

The fact that Q fixes ρ also implies that $\mathrm{H}^1(Q; (\mathbb{Z}/p\mathbb{Z})\rho) \cong \mathrm{Hom}(Q, \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^{(p+1)/2}$. Given a Q-invariant element α of $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z}$, consider a lift of α to $\tilde{\alpha} \in \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z})$. If $q \in Q$, then $q(\tilde{\alpha}) = \tilde{\alpha} + s_q\rho$ for some $s_q \in \mathbb{Z}/p\mathbb{Z}$. Then $\delta(\alpha)$ can be identified with the homomorphism $Q \to \mathbb{Z}/p\mathbb{Z}$ given by $q \mapsto s_q$.

Recall that X has genus $g = (p-1)(p-2)/2$ and so $\mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/p\mathbb{Z})$ has dimension $\binom{2g}{2}$. Thus $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/p\mathbb{Z}$ has dimension $\binom{2g}{2} - 1$. If $p = 5$, then $g = 6$ and $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/5\mathbb{Z}$ has dimension 65.

Example 7.7. *If $p = 5$, then the G_K-invariant subspace of $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ has dimension 35; the G_K-invariant subspace of $[\pi]_2/[\pi]_3 \otimes \mathbb{Z}/5\mathbb{Z}$ has dimension 34; and thus the coboundary map δ in (7.r) is trivial.*

Proof. From the computation in Example 7.6, we know the action of τ_i on $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ for $i = 0, 1, 2$. From this, we computed the action of τ_i on $\mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z}) \wedge \mathrm{H}_1(X; \mathbb{Z}/5\mathbb{Z})$ (resp. on the quotient of this by ρ). We then computed the dimension of the intersection of the kernels of the 3 operators $\tau_i - 1$ for $i = 0, 1, 2$. This dimension, which is 35 (resp. 34), is the dimension of the G_K-invariant subspace.

The fact that the coboundary map is trivial follows from the exact sequence in (7.r) but we also verified it computationally. □

References

[AI88] G. Anderson and Y. Ihara, *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293. MR 960948 2

[And87] G. W. Anderson, *Torsion points on Fermat Jacobians, roots of circular units and relative singular homology*, Duke Math. J. **54** (1987), no. 2, 501–561. MR 899404 (89g:14012) 2, 8, 9, 14

[And89] ———, *The hyperadelic gamma function*, Invent. Math. **95** (1989), no. 1, 63–131. MR 969414 2

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478 11, 16, 17

[Col89] R. F. Coleman, *Anderson-Ihara theory: Gauss sums and circular units*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 55–72. MR 1097609 (92f:11159) 2

[DPSW16] Rachel Davis, Rachel Pries, Vesna Stojanoska, and Kirsten Wickelgren, *Galois action on the homology of Fermat curves*, Directions in number theory, Assoc. Women Math. Ser., vol. 3, Springer, [Cham], 2016, pp. 57–86. MR 3596577 1, 2, 8, 9, 11, 16

[DPSW18] ———, *The Galois action and cohomology of a relative homology group of Fermat curves*, J. Algebra **505** (2018), 33–69. MR 3789905 1, 2, 3, 8, 11, 14, 15, 16, 17

[Ejd19] Özlem Ejder, *Modular symbols for Fermat curves*, Proc. Amer. Math. Soc. **147** (2019), no. 6, 2305–2319. MR 3951413 2, 9, 15

[Gro78] Benedict H. Gross, *On the periods of abelian integrals and a formula of Chowla and Selberg*, Invent. Math. **45** (1978), no. 2, 193–211, With an appendix by David E. Rohrlich. MR 0480542 8

[Hai97] Richard Hain, *Infinitesimal presentations of the Torelli groups*, J. Amer. Math. Soc. **10** (1997), no. 3, 597–651. MR 1431828 2

[Iha86] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106. MR 825839 (87c:11055) 2

[Lab70] John P. Labute, *On the descending central series of groups with a single defining relation*, J. Algebra **14** (1970), 16–23. MR 0251111 2

[Laz54] Michel Lazard, *Sur les groupes nilpotents et les anneaux de Lie*, Ann. Sci. Ecole Norm. Sup. (3) **71** (1954), 101–190. MR 0088496 1

[Leo96] Heinrich-Wolfgang Leopoldt, *Über die Automorphismengruppe des Fermatkörpers*, J. Number Theory **56** (1996), no. 2, 256–282. MR 1373551 10

[Lim91] Chong-Hai Lim, *Endomorphisms of Jacobian varieties of Fermat curves*, Compositio Math. **80** (1991), no. 1, 85–110. MR 1127061 8

[Ser65] Jean-Pierre Serre, *Lie algebras and Lie groups*, Lectures given at Harvard University, vol. 1964, W. A. Benjamin, Inc., New York-Amsterdam, 1965. MR 0218496 1

[Tze95] Pavlos Tzermias, *The group of automorphisms of the Fermat curve*, J. Number Theory **53** (1995), no. 1, 173–178. MR 1344839 10

[Tze97] ———, *Mordell-Weil groups of the Jacobian of the 5th Fermat curve*, Proc. Amer. Math. Soc. **125** (1997), no. 3, 663–668. MR 1353401 3, 16

University of Wisconsin-Madison

E-mail address: rachel.davis@wisc.edu

Colorado State University

E-mail address: pries@math.colostate.edu

Georgia Institute of Technology

E-mail address: kwickelgren3@math.gatech.edu