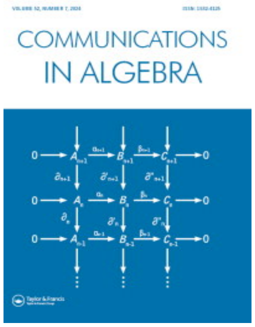

Taylor & Francis
Taylor & Francis Group

Communications in Algebra

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/lagb20

The classifying element for quotients of Fermat curves

Juanita Duque-Rosero & Rachel Pries

To cite this article: Juanita Duque-Rosero & Rachel Pries (06 May 2024): The classifying element for quotients of Fermat curves, Communications in Algebra, DOI: 10.1080/00927872.2024.2346299

To link to this article: https://doi.org/10.1080/00927872.2024.2346299

Published online: 06 May 2024.

COMMUNICATIONS IN ALGEBRA®
https://doi.org/10.1080/00927872.2024.2346299

Taylor & Francis
Taylor & Francis Group

Check for updates

The classifying element for quotients of Fermat curves

Juanita Duque-Rosero[a] and Rachel Pries[b]

[a]Boston University, Boston, MA; [b]Colorado State University, Fort Collins, CO

ABSTRACT
Suppose C is a cyclic Galois cover of the projective line branched at the three points 0, 1, and ∞. Under a mild condition on the ramification, we determine the structure of the graded Lie algebra of the lower central series of the fundamental group of C in terms of a basis which is well-suited to studying the action of the absolute Galois group of $\mathbb{Q}$.

ARTICLE HISTORY
Received 12 December 2023
Communicated by Daniel Erman

KEYWORDS
Absolute Galois group; Belyi curve; classifying element; covering; curve; Fermat curve; fundamental group; Galois module; graded Lie algebra; homology; lower central series; modular symbol

2020 MATHEMATICS SUBJECT CLASSIFICATION
Primary: 11D41; 11G32; 14F35; 14H30; 17B70; Secondary: 11F06; 11F67; 11G30; 13A50; 14F20

1. Introduction

In this companion paper to [3], the main goal is to determine information about the étale fundamental group of a cyclic Belyi curve using its lower central series. To explain the meaning of this, we first provide some background.

Suppose X is a smooth projective curve of genus g defined over a number field K. Let $\bar{K}$ be the algebraic closure of K and suppose that $X_{\bar{K}}$ is connected. Let $\pi = [\pi]_1 = \pi_1(X)$ be the étale fundamental group and let $\mathrm{H}_1(X)$ be the étale homology group of $X_{\bar{K}}$.

For $m \geq 2$, let $[\pi]_m$ be the mth subgroup of the lower central series $\pi = [\pi]_1 \supset [\pi]_2 \supset [\pi]_3 \supset \cdots$; specifically, $[\pi]_m = \overline{[\pi, [\pi]_{m-1}]}$ is the closure of the subgroup generated by commutators of elements of π with elements of $[\pi]_{m-1}$. Then $\mathrm{H}_1(X) \cong [\pi]_1/[\pi]_2$.

Consider the graded Lie algebra $\mathrm{gr}(\pi) = \oplus_{m\geq 1}[\pi]_m/[\pi]_{m+1}$ of the lower central series for π, [7, 11]. Let F be the free profinite group on $2g$ generators and consider its graded Lie algebra $\mathrm{gr}(F) = \oplus_{m\geq 1}\mathrm{gr}_m(F)$. By [6, Theorem, p. 17], there is an element ρ of weight 2 such that

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

Thus $\mathrm{gr}(\pi)$ is determined by the subgroup $\langle\rho\rangle$. By [5, Corollary 8.3],

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

where

$$\mathscr{C}: \mathrm{H}_2(X) \to \mathrm{H}_1(X) \wedge \mathrm{H}_1(X) \tag{1.1}$$

CONTACT Rachel Pries pries@colostate.edu Colorado State University, Fort Collins, CO.

is the dual map to the cup product map $\mathrm{H}^1(X) \wedge \mathrm{H}^1(X) \to \mathrm{H}^2(X)$. Since $\mathrm{H}_2(X) \cong \mathbb{Z}(1)$, the image $\mathrm{Im}(\mathscr{C})$ is cyclic. A generator Δ for $\mathrm{Im}(\mathscr{C})$ is called a *classifying element*.

There is a formula for Δ in terms of a set of generators of the fundamental group of X that satisfies certain properties; see (2.3) for details. In the context of étale homology groups, we would like additional information, specifically the following.

Goal 1.1. Find a formula for a classifying element using a basis for $\mathrm{H}_1(X)$ which is well-suited for studying the action of the absolute Galois group G_K and the action of $\mathrm{Aut}(X)$.

In [3], the authors realized this goal when $X = X_n : x^n + y^n = z^n$ is the Fermat curve of degree n, for any integer $n \geq 3$. When $n = p$ is an odd prime satisfying Vandiver's conjecture, and $K = \mathbb{Q}(\zeta_p)$ is the cyclotomic field, then the information about the action of G_K on $\mathrm{H}_1(X_p, \mathbb{Z}/p\mathbb{Z})$ comes from [1] and [2].

In this paper, we realize Goal 1.1 when $X = W_{n,k}$ is a cyclic Belyi curve, namely a curve with affine equation

$$v^n = u(1-u)^k, \tag{1.2}$$

for any odd integer n and integer k with $1 \leq k \leq n-2$. This curve admits a Galois μ_n-cover $\phi\colon W_{n,k} \to \mathbb{P}^1$ branched at 3 points 0, 1, and ∞. We restrict to the case that the cover is totally ramified at the ramification points η_0, η_1, and η_∞; this is true if and only if $\gcd(n, k(k+1)) = 1$; in particular, it is true for all $1 \leq k \leq n-2$ if n is prime.

The main result of the paper is Theorem 3.5; writing $W = W_{n,k}$, we determine a classifying element $\Delta \in \mathrm{H}_1(W) \wedge \mathrm{H}_1(W)$ for all such pairs (n,k). This determines the isomorphism class of $\mathrm{gr}(\pi)$ as a graded Lie group with the action of $\mu_n \subset \mathrm{Aut}(W)$.

Here is some notation needed to state the result. Let $U = W - \eta_\infty$, where η_∞ is the unique point not on the affine chart (1.2). In Section 2, we define some loops $E_1, \ldots, E_{n-1}$ in the fundamental group $\pi_1(U)$ (2.6). Let $[E_1], \ldots, [E_{n-1}]$ denote the images of $E_1, \ldots, E_{n-1}$ in the homology group $\mathrm{H}_1(U)$. In Corollary 4.5, we prove that these form a basis for $\mathrm{H}_1(U)$. This basis for $\mathrm{gr}_1(F) \cong \mathrm{H}_1(W) \cong \mathrm{H}_1(U)$ yields a basis for $\mathrm{gr}_2(F) \cong \mathrm{H}_1(W) \wedge \mathrm{H}_1(W)$ given by $\{[E_i] \wedge [E_j] \mid 1 \leq i < j \leq n-1\}$. We state our main result in terms of that basis.

Theorem A (Theorem 3.5). *Suppose $1 \leq k \leq n-2$ and $\gcd(n, k(k+1)) = 1$. Let W be the smooth projective curve with affine equation $v^n = u(1-u)^k$.*

Let c be the integer such that $1 \leq c \leq n-1$ and c is the multiplicative inverse of $k+1$ modulo n. Then a classifying element Δ for W is given by

$$\Delta = \sum_{1 \leq I < J \leq n-1} c_{I,J} [E_I] \wedge [E_J],$$

where

$$c_{I,J} = \begin{cases} -1 & \text{if } J - I \equiv j(k+1) - 1 \bmod n, \text{ or} \\ +1 & \text{if } J - I \equiv j(k+1) \bmod n, \end{cases}$$

for some j such that $1 \leq j \leq c-1$; and $c_{I,J} = 0$ otherwise.

For the proof, we first rely on Lemma 2.1, which states that a formula for Δ can be found by expressing a loop L around η_∞ as a product of commutators of elements in $\pi_1(U)$. Then the main ingredients of the proof are the topology and Galois theory of branched coverings. In Section 3, we use these to find a combinatorial formula for L; the formula is first described using edges that generate the fundamental groupoid of U with respect to $\{\eta_0, \eta_1\}$, and then re-expressed in terms of the loops $E_1, \ldots, E_{n-1}$.

In Section 5, we provide examples for arbitrary odd n and certain values of k.

Remark 1.2. The motivation for studying covers of $\mathbb{P}^1$ branched at three points originates with Grothendieck's program for understanding the absolute Galois group of $\mathbb{Q}$. The cyclic Belyi curves play an important role in the study of Galois theory, Hurwitz spaces, and abelian varieties with complex multiplication. Since $W = W_{n,k}$ is a quotient of the Fermat curve X_n, it might be possible to prove Theorem A with a top-down approach, using the result of [3]. In working on this problem, we realized that there are many advantages with the direct approach, see Remark 2.4.

Remark 1.3. Theorem A is valid both for the homology with coefficients in $\mathbb{Z}$ and for the étale homology which has coefficients in a finite or ℓ-adic ring. In Section 4, the proof relies on the modular symbols of Manin [8] (and a result of Ejder [4]). However, we follow an approach which is compatible with the results in [1] and [2] about the étale homology with coefficients in $\mathbb{Z}/n\mathbb{Z}$ and the action of the absolute Galois group upon it, because this will be important in future applications.

After choosing an embedding $\mathbb{Q} \subset \mathbb{C}$ and applying Riemann's Existence Theorem, we may identify the profinite completion of $\mathrm{H}_1(U(\mathbb{C}))$ with the étale homology $\mathrm{H}_1(U)$. Similarly, we may identify the profinite completion of $\pi_1(U(\mathbb{C}))$ with the étale fundamental group $\pi_1(U)$. Thus we can consider the elements $E_1, \ldots, E_{n-1}$ to be in the topological fundamental group or in the étale fundamental group; similarly, we can consider the elements $[E_1], \ldots, [E_{n-1}]$ to be in the simplicial homology or in the étale homology. A similar comparison holds for other objects in the paper.

2. The fundamental group of cyclic Belyi curves

We describe the geometry of cyclic Belyi curves and their relationship to Fermat curves. We state some facts about the fundamental group and the classifying element Δ.

Let $n \geq 3$ be a positive integer. Let $\zeta = e^{2\pi i/n}$ be a fixed primitive nth root of unity. Fix an integer k, with $1 \leq k \leq n-2$. For simplicity, we assume throughout the paper that $\gcd(n, k(k+1)) = 1$; this assumption is true if n is prime, which is the situation of future applications of this paper.

2.1. The geometry of cyclic Belyi curves

Let $W = W_{n,k}$ be the smooth projective curve having affine equation:

$$v^n = u(1-u)^k. \tag{2.1}$$

Let η_0 be the point $(u, v) = (0, 0)$; let η_1 be the point $(u, v) = (1, 0)$. The hypothesis that $\gcd(n, k+1) = 1$ implies that there is a unique point η_∞ on W which is not on this affine chart. Consider the open affine subset $U = W - \eta_\infty$.

There is a μ_n-Galois cover $\phi\colon W \to \mathbb{P}^1$, given by $\phi(u, v) \mapsto u$. The Galois group is generated by the automorphism $\epsilon \in \mathrm{Aut}(W)$ of order n that acts by $\epsilon((u, v)) = (u, \zeta v)$. The cover ϕ is totally ramified at the points η_0, η_1, and η_∞, which lie over the branch points $u = 0, 1$, and ∞ respectively.

By the Riemann-Hurwitz formula, the genus of W is $g = (n-1)/2$.

Any μ_n-cover of $\mathbb{P}^1$ branched at three points, which is totally ramified at one point, admits an equation of the form (2.1) for some k with $1 \leq k \leq n-2$. The condition of being totally ramified over the other two branch points is equivalent to $\gcd(n, k(k+1)) = 1$.

2.2. The fundamental group

Throughout the paper, composition of paths and loops is denoted by the symbol $\cdot$ and written from left to right. Note that $U \subset W$ is a real surface of genus $g = (n-1)/2$ with 1 puncture. We choose the base point η_1. There exist loops a_i, b_i for $1 \leq i \leq g$ and c_∞, with base point η_1, such that $\pi_1(U)$ has a presentation

$$\pi_1(U) = \langle a_i, b_i, c_\infty \mid i = 1, \dots, g\rangle / \prod_{i=1}^{g} [a_i, b_i] c_\infty. \tag{2.2}$$

Without loss of generality, we choose the loop c_∞ to circle the puncture η_∞ and to have no set-theoretic intersection with the loops a_i, b_i for $1 \leq i \leq g$. This can be arranged using a standard gluing of a 1-punctured polygon with $4g$ sides, with the sides labeled consecutively by $a_1, b_1, a_1^{-1}, b_1^{-1}, \dots, a_g, b_g, a_g^{-1}, b_g^{-1}$.

The homology group $\mathrm{H}_1(U)$ is equipped with an intersection pairing, defined using Poincaré duality and the cup product on compactly supported cohomology. Let $\bar{a}_i, \bar{b}_i, \bar{c}_\infty$ denote the images of a_i, b_i, c_∞ in $\mathrm{H}_1(U)$. Note that $\bar{c}_\infty$ is trivial.

Without loss of generality, we can suppose that the images of $\bar{a}_i, \bar{b}_i$ in $\mathrm{H}_1(U)$ form a standard symplectic basis. Since U has only one puncture, there is an isomorphism $\mathrm{H}_1(U) \cong \mathrm{H}_1(W)$. These two facts imply that a generator of $\mathrm{Im}(\mathscr{C})$ as in (1.1) can be identified with:

$$\Delta_W = \sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U). \tag{2.3}$$

2.3. The second graded quotient in the lower central series

By (2.3), $\Delta_W = \sum_{i=1}^{g} \bar{a}_i \wedge \bar{b}_i$. We would like to determine Δ_W in terms of a basis of $\mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$ for which we have information about the action of the absolute Galois group. To do this, we investigate the element $T := \prod_{i=1}^{g} [a_i, b_i] = c_\infty^{-1}$ in $\pi_1(U)$.

We need the following two results. The first shows that Δ_W does not depend on the representation as a product of commutators.

Lemma 2.1. *[3, Lemma 2.2] Suppose $r_1, \dots, r_N, s_1 \dots, s_N$ are loops in U, with images $\bar{r}_i, \bar{s}_i$ in $\mathrm{H}_1(U)$. If*

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

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

The next lemma will help simplify later calculations.

Lemma 2.2. *[3, 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 the quotient $[\pi_1(U)]_2/[\pi_1(U)]_3$.
(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 $\gamma \wedge (-\alpha)$.

2.4. The fundamental groupoid

More generally, we consider the fundamental groupoid $\pi_1(U, \{\eta_0, \eta_1\})$ of U with respect to the points η_0 and η_1. Let β_W be the path in U, which begins at the base point η_0 and ends at η_1, given by

$$\beta_W = \left(t, \sqrt[n]{t(1-t)^k}\right) \text{ for } t \in [0, 1]. \tag{2.4}$$

Here the symbol $\sqrt[n]{t(1-t)^k}$ denotes the real-valued and positive nth root.

Recall that $\epsilon((u, v)) = (u, \zeta v)$. For $0 \leq i \leq n-1$, we define a path in U, which begins at η_0 and ends at η_1 by

$$e_i = \epsilon^i \beta_W. \tag{2.5}$$

Define $\tau = \beta_W^{-1}$, where the inverse of a path is the path traversed in the opposite direction. Note that $e_i^{-1} = \epsilon^i \beta_W^{-1}$.

We define some loops in U with base point η_1: for $0 \le i \le n-1$, let

$$E_i := e_i^{-1} \cdot e_0 = \epsilon^i \tau \cdot \tau^{-1}. \tag{2.6}$$

The loop E_i implicitly depends on k. Note that

$$E_i \cdot E_j^{-1} = e_i^{-1} \cdot e_0 \cdot e_0^{-1} \cdot e_j = e_i^{-1} \cdot e_j. \tag{2.7}$$

If $i = 0$, then E_i is trivial in $\pi_1(U, \{\eta_0, \eta_1\})$. Corollary 4.5 shows that the converse is true.

2.5. Comparison with the Fermat curve

It is well-known that $W = W_{n,k}$ is a quotient of the Fermat curve X_n: $x^n + y^n = z^n$ of degree n (see, e.g. [9, Chapter 8]). Let Z_F be the set of n points where $z = 0$ on X_n. The open affine subset $U_F = X_n - Z_F$ is given by the set of points (x, y) such that $x^n + y^n = 1$.

In [3, (2.g)], the authors defined a path β in U_F. We remark that β_W is the image of β under the map $U_F \to U$ that takes (x, y) to (x^n, xy^k).

The automorphism group of X_n contains two automorphisms ϵ_0 and ϵ_1 of order n that commute; these act by $\epsilon_0((x, y)) = (\zeta x, y)$ and $\epsilon_1((x, y)) = (x, \zeta y)$. Let $H = H_{n,k}$ be the subgroup of $\mathrm{Aut}(X_n)$ generated by $h = \epsilon_0 \epsilon_1^{-k^{-1} \bmod n}$.

Lemma 2.3. *The cyclic Belyi curve $W_{n,k}$ is the quotient of the Fermat curve X_n of degree n by $H_{n,k}$. The fiber of X_n over η_∞ is the set of n points in Z_F; the fiber of X_n over η_0 (resp. η_1) is the set of n points on U_F where $x = 0$ (resp. $y = 0$).*

Proof. There is a well-defined inclusion from the function field of $W_{n,k}$ to the function field of X_n determined by $u \mapsto x^n$ and $v \mapsto xy^k$. This inclusion has degree n. The first claim follows since u and v are fixed by h. The claims about the fibers follow by calculation. □

Remark 2.4. Here are the reasons that proving Theorem 3.5 with a top-down approach would be more complicated.

First, the combinatorial description of the loop in Section 3 is substantially easier than the description of n loops in [3]. This is because the cover $\phi: W \to \mathbb{P}^1$ has degree n, rather than $n^2 = \deg(X_n \to \mathbb{P}^1)$, and also because there is one point η_∞ of W above ∞ rather than the n points of Z_F. The theoretical description of the boundary of a simple closed disk containing η_∞ is easier than that for the boundary of a simple closed disk in X_n containing the n points of Z_F.

Second, in Section 4, the homology group $\mathrm{H}_1(W)$ is a subspace of a free module of rank one over $\mathbb{Z}[\mu_n]$, while $\mathrm{H}_1(X_n)$ is a subquotient of a free module of rank one over the more complicated group ring $\mathbb{Z}[\mu_n \times \mu_n]$. The formula for Δ_W in (2.3) is easier than for the Fermat curve where there is a non-trivial homomorphism $\wedge^2 \mathrm{H}_1(U_F) \to \wedge^2 \mathrm{H}_1(X_n)$.

Third, the next lemma shows that the chosen basis elements of $\mathrm{H}_1(X_n)$ have slightly complicated images in terms of the chosen basis elements of $\mathrm{H}_1(W)$. For these reasons, the formula in Theorem 3.5 is easier to write down and prove using a direct approach.

Recall from [3, Section 2.3], the definitions of the paths $\{e_{i,j}\}_{0 \le i,j \le n-1}$ in U_F and the loops

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

By [3, Lemma 4.1], the images of $\{[E_{i,j}]\}_{1 \le i,j \le n-1}$ form a basis for $\mathrm{H}_1(U_F)$.

Lemma 2.5. *Under the map $\pi_1(U_F) \to \pi_1(U)$ induced by the map $U_F \to U$:*

(1) The image of $e_{i,j}$ in $\pi_1(U, \{\eta_0, \eta_1\})$ is e_{i+jk}.
(2) The image of $E_{i,j}$ in $\pi_1(U)$ is $e_0 \cdot e_{jk}^{-1} \cdot e_{i+jk} \cdot e_i^{-1}$, which starts and ends at η_0.
(3) The adapted loop $e_{jk}^{-1} \cdot e_{i+jk} \cdot e_i^{-1} \cdot e_0$, which starts and ends at η_1, equals $E_{jk} \cdot E_{i+jk}^{-1} \cdot E_i$.

Proof. This follows from the equalities $u = x^n$ and $v = xy^k$ in the proof of Lemma 2.3. □

3. The classifying element of the Belyi curve

We continue to study the curve $W = W_{n,k}$ with affine equation $v^n = u(1-u)^k$. Recall that $T = \prod_{i=1}^{g}[a_i, b_i] = c_\infty^{-1}$ is in the homotopy class of the boundary of a disk in W that contains the point η_∞. In Proposition 3.3, we find a loop homotopic to T written in terms of the elements E_i in $\pi_1(U)$. We then analyze the ordering of the loops E_i in T combinatorially. This enables us to find an explicit formula for $\Delta \in \mathrm{H}_1(U) \wedge \mathrm{H}_1(U)$, using a basis on which we have some information about the action of the absolute Galois group, see Theorem 3.5.

3.1. Gluing sheets of an unramified cover

Recall that $\phi\colon W \to \mathbb{P}^1$ is the μ_n-Galois cover given by $(u, v) \mapsto u$. The cover ϕ is branched at $\{u = 0, 1, \infty\}$ and is ramified at $\{\eta_0 = (0,0), \eta_1 = (1,0), \eta_\infty\}$. In this section, we remove some paths in W and $\mathbb{P}^1$ in order to work with an unramified cover.

Given the equation $v^n = u(1-u)^k$, the inertia type of ϕ is the 3-tuple $(1, k, -(1+k))$. This means that the canonical generators of inertia at η_0, η_1, and η_∞ are ζ^1, ζ^k, and ζ^{-1-k}, respectively. In other words, the chosen generator ϵ of the Galois group of ϕ acts on a uniformizer at each ramification point by this root of unity, respectively.

We make a slit cut along the positive real line in $\mathbb{P}^1(\mathbb{C})$ from $u = 1$ to $u = 0$ and another from $u = 1$ to $u = \infty$. We choose a base point $\underline{u}_1$ close to $u = 1$ and in the lower half plane; a technical term for this is a tangential base point at $u = 1$. We also make a short slit cut $\underline{t}$ from $u = \underline{u}_1$ to $u = 1$.

Let P° be the complement of these three slit cuts in $\mathbb{P}^1(\mathbb{C})$. Let W° be the complement of the $3n$ paths in W that lie above these three slit cuts.

Lemma 3.1. *The restriction $\phi\colon W^\circ \to P^\circ$ is unramified.*

Proof. The monodromy around $u = 0, 1, \infty$ is multiplication by ζ^1, ζ^k, and $\zeta^{-(k+1)}$, respectively. So a loop going around all 3 of these points is multiplication by 1. Therefore, the monodromy action of $\pi_1(P^\circ)$ on W° is trivial, which proves the claim. □

Thus W° is a disjoint union of n connected components, which are called sheets. We need to label the regions of $\mathbb{P}^1$ near the slit cuts and the edges along the boundary of W°. It might be helpful to look at Figure 1 for reference.

For the regions of $\mathbb{P}^1$: let N denote the region of the upper half plane which is close to the positive real axis; let E denote the region of the lower half plane which is close to the values $u \geq 1$ on the real axis; and let S denote the region of the lower half plane which is close to the values $0 \leq u \leq 1$ on the real axis.

For the edges along the boundary of W°, we start by labeling the unique edge τ of W° having the following property: it is on the path β_W; and it is on the right hand-side as one travels from η_1 to η_0, meaning that it lies above N rather than S.

Let $0 \leq i < n$. The action of ϵ^i on W° allow us to label n of the edges as $\epsilon^i\tau$; these are the edges that lie above the interval $[0, 1]$ in N. Furthermore, we label by R_i the sheet of W° that contains $\epsilon^i\tau$. In each sheet R_i: we label by $\epsilon^i\alpha$ the unique edge that lies above the ray $[1, \infty)$ in N; and we label by $\epsilon^i\xi$

the unique edge that lies above $\underline{t}$ in S. This completes the labeling of one side of each of the $3n$ slit cuts in W°.

The inertia type gives the information needed to glue the sheets together along the slit cuts to obtain the ramified cover ϕ of Riemann surfaces.

Lemma 3.2. *For $0 \leq i < n$:*

(1) The edge $\epsilon^i\tau$ on R_i glues with the unique edge in $R_{i-1 \bmod n}$ that lies above the interval $[0,1]$ in S.
(2) The edge $\epsilon^i\alpha$ on R_i glues with the unique edge in $R_{i-(k+1) \bmod n}$ that lies above the interval $[1,\infty)$ in E.
(3) The edge $\epsilon^i\xi$ on R_i glues with the unique edge in R_i that lies above $\underline{t}$ in E.

Proof. (1) Imagine a simple closed loop around η_0 that crosses the edge $\epsilon^i\tau$; as one travels around this loop in a counterclockwise direction, the fact that the generator of inertia at η_0 is ζ^1 implies that one passes from the sheet $R_{i-1 \bmod n}$ to the sheet R_i. Thus the edge $\epsilon^i\tau$ on R_i must be glued with the unique edge in $R_{i-1 \bmod n}$ that lies above the interval $[0,1]$ in S.
(2) Imagine a simple closed loop around η_∞ that crosses the edge $\epsilon^i\alpha$; as one travels around this loop in a counterclockwise direction, the fact that the generator of inertia at η_∞ is $\zeta^{-(k+1)}$ implies that one passes from the sheet R_i to the sheet $R_{i-(k+1) \bmod n}$. Thus the edge $\epsilon^i\alpha$ on R_i must be glued with the unique edge in $R_{i-(k+1) \bmod n}$ that lies above the interval $[1,\infty)$ in E.
(3) Imagine a simple closed loop around a lift of $\underline{t}$ that crosses the edge $\epsilon^i\xi$; as one travels around this loop in a counterclockwise direction, one should stay on the same sheet since $\underline{t}$ is not a branch point. Thus the edge $\epsilon^i\xi$ on R_i must be glued to the unique edge in R_i that lies above the interval $\underline{\mathrm{t}}$ in E. □

3.2. Lifting of a loop

Let $\mathbb{H}^+$ be the upper half plane and $\mathbb{H}^-$ be the lower half plane. Let $\tilde{u}_1$ be the lift of the base point $\underline{u}_1$ which is on ξ in R_0. In this section, all loops in $\mathbb{P}^1(\mathbb{C})$ (resp. $W(\mathbb{C})$) have base point $\underline{u}_1$ (resp. $\tilde{u}_1$).

In $\mathbb{P}^1(\mathbb{C})$, consider a counterclockwise simple closed loop $Z_\circ$ around ∞. It is homotopic to a clockwise simple closed loop Z that first crosses from $\mathbb{H}^-$ to $\mathbb{H}^+$ at some point in $\mathbb{R}^{u<0}$ and then crosses from $\mathbb{H}^+$ to $\mathbb{H}^-$ at some point in $\mathbb{R}^{u>1}$. Without loss of generality, we can suppose that this last crossing occurs at an arbitrarily large value of u.

Let $\tilde{Z}_\circ$ be a lift of $Z_\circ$ to W. Let $\tilde{Z}$ be a lift of Z to W.

Our goal now is to describe the loop $\tilde{Z}$ in terms of the edges $\epsilon^i\tau$, and then in terms of the loops E_i, for $0 \leq i < n$. Recall that $e_i = \epsilon^i\tau$ and $E_i = \epsilon^i\tau \cdot \tau^{-1}$. For $0 \leq j \leq n-1$, let

$$L_j := \epsilon^{j(n-k-1)+1}\tau \cdot (\epsilon^{j(n-k-1)}\tau)^{-1} = E_{j(n-k-1)+1} \cdot E^{-1}_{j(n-k-1)}, \tag{3.1}$$

where the second equality follows from (2.7). Let

$$L := L_0 \cdot L_1 \cdot \cdots \cdot L_{n-1}.$$

We view L as a word in $\{E_i, E_i^{-1}\}_{0 \leq i < n}$, including the elements E_0, E_0^{-1} as placeholders even though they are trivial in homology.

Proposition 3.3. *The loop c_∞ is homotopic to L.*

Proof. The loop c_∞ is homotopic to $\tilde{Z}$, because $\tilde{Z}$ is homotopic to $\tilde{Z}_\circ$, which is a counterclockwise simple closed loop around η_∞. So it suffices to prove the formula for $\tilde{Z}$.

The loop $\tilde{Z}$ in W covers the loop Z in $\mathbb{P}^1$ exactly n times. This is because it is homotopic to the simple closed loop $\tilde{Z}_\circ$ around the point η_∞, which is a ramification point for ϕ with ramification degree n. Each revolution begins above S, then goes above N, then switches sheets and goes above E.

The loop $\tilde{Z}$ starts on the sheet R_0. Then it crosses the edge α onto the sheet $R_{n-(k+1)}$, where it swings by the point $\epsilon_{n-(k+1)}\tilde{u}_1$. That completes one of the n revolutions. The next revolution is similar but starts on the sheet $R_{n-(k+1)}$. So the subindex on each path increases by $n-(k+1)$ after each revolution.

The first revolution is homotopic to a path that traces in a clockwise direction along the outside of the slits, going near the following points, in this order:

$$\tilde{u}_1 \mapsto \eta_1 \mapsto \eta_0 \mapsto \eta_1 \mapsto \eta_\infty \mapsto \eta_1 \mapsto \epsilon^{n-(k+1)}\tilde{u}_1.$$

This path is the composition of the following paths, written from left to right, with the first four on the sheet R_0 and the last two on the sheet $R_{n-(k+1)}$:

$$\xi^{-1} \cdot \epsilon\tau \cdot \tau^{-1} \cdot \alpha \cdot \alpha^{-1} \cdot \epsilon^{n-(k+1)}\xi.$$

The paths α and α^{-1} cancel. Also the last path $\epsilon^{n-(k+1)}\xi$ on the first revolution cancels with the first path on the next revolution, and the first path ξ^{-1} on the first revolution cancels with the last path on the last revolution; so these paths can be ignored, leaving only L_0.

Thus $\tilde{Z}$ is homotopic to $L_0 \cdot \epsilon^{n-(k+1)}L_0 \cdot \cdots \cdot \epsilon^{(n-1)(n-(k+1))}L_0$. By (3.1), the equation for L_{j+1} is $\epsilon^{n-(k+1)}L_j$. Thus $\tilde{Z}$ is homotopic to $L_0 \cdot L_1 \cdot \cdots \cdot L_{n-1}$. □

3.3. Combinatorial analysis of loop

We need a combinatorial analysis of the ordering of the edges in the loop L. We say that a loop E_j (or E_j^{-1}) is between E_i^{-1} and E_i if it is written between them after cyclically permuting the loops so that E_i^{-1} is the leftmost loop in L.

Recall that $\gcd(n, k+1) = 1$. Let $c \in \{1, \dots, n-1\}$ be such that $c \equiv (k+1)^{-1} \bmod n$. Note that $c(n-k-1) \equiv n-1 \bmod n$.

Proposition 3.4. *Let $0 \le i < n$. The loops between E_i^{-1} and E_i in L are*

$$\left\{E_{i+j(n-k-1)+1}, E^{-1}_{i+j(n-k-1)}\right\}_{1\le j\le c-1}.$$

Proof. It suffices to prove the result when $i = 0$ by symmetry. When $i = 0$, the claim is that the loops in L between E_0^{-1} and E_0 in L are $E_{j(n-k-1)+1}$ and $E^{-1}_{j(n-k-1)}$ for $1 \le j \le c-1$.

To see this, consider the ordering of the loops in L:

sheet 0: $L_0 = \epsilon\tau \cdot \tau^{-1} = E_1 \cdot E_0^{-1}$;

sheet $n-k-1$: $L_1 = \epsilon^{(n-k-1)+1}\tau \cdot \left(\epsilon^{n-k-1}\tau\right)^{-1} = E_{(n-k-1)+1} \cdot E^{-1}_{n-k-1}$;

sheet $2(n-k-1)$: $L_2 = \epsilon^{2(n-k-1)+1}\tau \cdot \left(\epsilon^{2(n-k-1)}\tau\right)^{-1} = E_{2(n-k-1)+1} \cdot E^{-1}_{2(n-k-1)}$;

and continuing on to sheet $c(n-k-1)$: $L_c = \tau \cdot \left(\epsilon^{n-1}\tau\right)^{-1} = E_0 \cdot E^{-1}_{n-1}$.

The loop E_0 occurs first on the sheet $c(n-k-1)$. The result follows because the stated loops are the ones that occur in $L_1, \dots, L_{c-1}$. □

3.4. Main result

Theorem 3.5. *Let n and k be integers with $1 \le k \le n-2$ and $\gcd(n, k(k+1)) = 1$. Let W be the smooth projective curve with affine equation $v^n = u(1-u)^k$.*

Let c be the integer such that $1 \le c \le n-1$ and c is the multiplicative inverse of $k+1$ modulo n. Then the classifying element Δ for W is given by

$$\Delta = \sum_{1\le I<J\le n-1} c_{I,J}[E_I] \wedge [E_J],$$

where

$$c_{I,J} = \begin{cases} -1 & \text{if } J - I \equiv j(k+1) - 1 \bmod n, \text{ or} \\ +1 & \text{if } J - I \equiv j(k+1) \bmod n, \end{cases}$$

for some j such that $1 \leq j \leq c - 1$*; and* $c_{I,J} = 0$ *otherwise.*

Proof. By Proposition 3.3, the loop c_∞ is homotopic to L. By Lemma 2.1, we can determine the image of L in $[\pi_1(U)]_2/[\pi_1(U)]_3$ by writing it as a product of commutators. By applying Lemma 2.2 repeatedly, this image is determined by the ordering of the loops in L; specifically, if E' lies between E_i^{-1} and E_i, then $-[E_i] \wedge [E']$ appears in the image. By Proposition 3.4, the image contains the terms

$$-[E_i] \wedge [E_{i+j(n-k-1)+1}] = -[E_i] \wedge [E_{i-j(k+1)+1}] = [E_{i-j(k+1)+1}] \wedge [E_i],$$

and

$$+[E_i] \wedge [E_{i+j(n-k-1)}] = [E_i] \wedge [E_{i-j(k+1)}] = -[E_{i-j(k+1)}] \wedge [E_i],$$

for $1 \leq j \leq c - 1$.

Since $T = c_\infty^{-1}$, we negate the coefficients once more; (this is not crucial, since this only scales Δ). Thus $c_{I,J} = -1$ if $J - I = j(k+1) - 1$ and $c_{I,J} = 1$ if $J - I = j(k+1)$ for some $1 \leq j \leq c - 1$, and $c_{I,J} = 0$ otherwise. □

Remark 3.6. The coefficient $c_{I,J}$ is nonzero if exactly one of E_J and E_J^{-1} is between E_I and E_I^{-1} in this loop, indicating that there is a nontrivial commutator involving these elements. Specifically, $c_{I,J} = 1$ for the ordering $E_I, E_J, E_I^{-1}, E_J^{-1}$ and $c_{I,J} = -1$ for the ordering $E_I, E_J^{-1}, E_I^{-1}, E_J$.

Remark 3.7. If $\gcd(j, n) = 1$, then it is possible to compare the classifying elements for the inertia types $(j, jk, -j(k+1))$ and $(1, k, -(k+1))$. Specifically, when we replace E_i by $E_{ji \bmod n}$ in the classifying element for the former, we obtain the classifying element of the latter. For example, $\Delta_{5,(3,1,1)} = -[E_1] \wedge [E_2] - [E_2] \wedge [E_3] - [E_3] \wedge [E_4]$. Replacing E_i by $E_{3i \bmod 5}$, we obtain the same result as for $\Delta_{5,(1,2,2)}$.

It is also possible to compare the classifying elements after a permutation of the three elements of the inertia type, but this involves a more complicated linear transformation on the homology.

3.5. Examples when n = 5

First, suppose that $k = 1$. The left-hand side of Figure 1 shows this example in detail. The colors and letters a – e in the figure represent the gluing of the sheets.

In Section 3.3, we consider a simple closed loop $L_\circ$ going counterclockwise around the point ∞ in $\mathbb{P}^1$. The loop illustrated in the base of the diagram is homotopic to $L_\circ$. We lift $L_\circ$ to a loop L in W. The loop L is homotopic to the following composition of paths:

$$\epsilon\tau \cdot \tau^{-1} \cdot \epsilon^4\tau \cdot (\epsilon^3\tau)^{-1} \cdot \epsilon^2\tau \cdot (\epsilon\tau)^{-1} \cdot \tau \cdot (\epsilon^4\tau)^{-1} \cdot \epsilon^3\tau \cdot (\epsilon^2\tau)^{-1}.$$

The order of the path is labeled in the figure with steps 1–6. Recall that $E_i = \epsilon^i\tau \cdot \tau^{-1}$ for $0 \leq i \leq 4$. Note that E_0 is trivial. Then L is homotopic to:

$$E_1 \cdot E_4 \cdot E_3^{-1} \cdot E_2 \cdot E_1^{-1} \cdot E_4^{-1} \cdot E_3 \cdot E_2^{-1}.$$

The ordering of the loops in L implies the following formula when $n = 5$ and $k = 1$:

$$\Delta = [E_1] \wedge (-[E_2] + [E_3] - [E_4]) + [E_2] \wedge (-[E_3] + [E_4]) + [E_3] \wedge (-[E_4]).$$

This formula agrees with Theorem 3.5.

For comparison, suppose $k = 2$. The right-hand side of Figure 1 shows the gluing of the sheets. In this case, L is homotopic to the following composition of paths:

$$\epsilon\tau \cdot \tau^{-1} \cdot \epsilon^3\tau \cdot (\epsilon^2\tau)^{-1} \cdot \tau \cdot (\epsilon^4\tau)^{-1} \cdot \epsilon^2\tau \cdot (\epsilon\tau)^{-1} \cdot \epsilon^4\tau \cdot (\epsilon^3\tau)^{-1}.$$

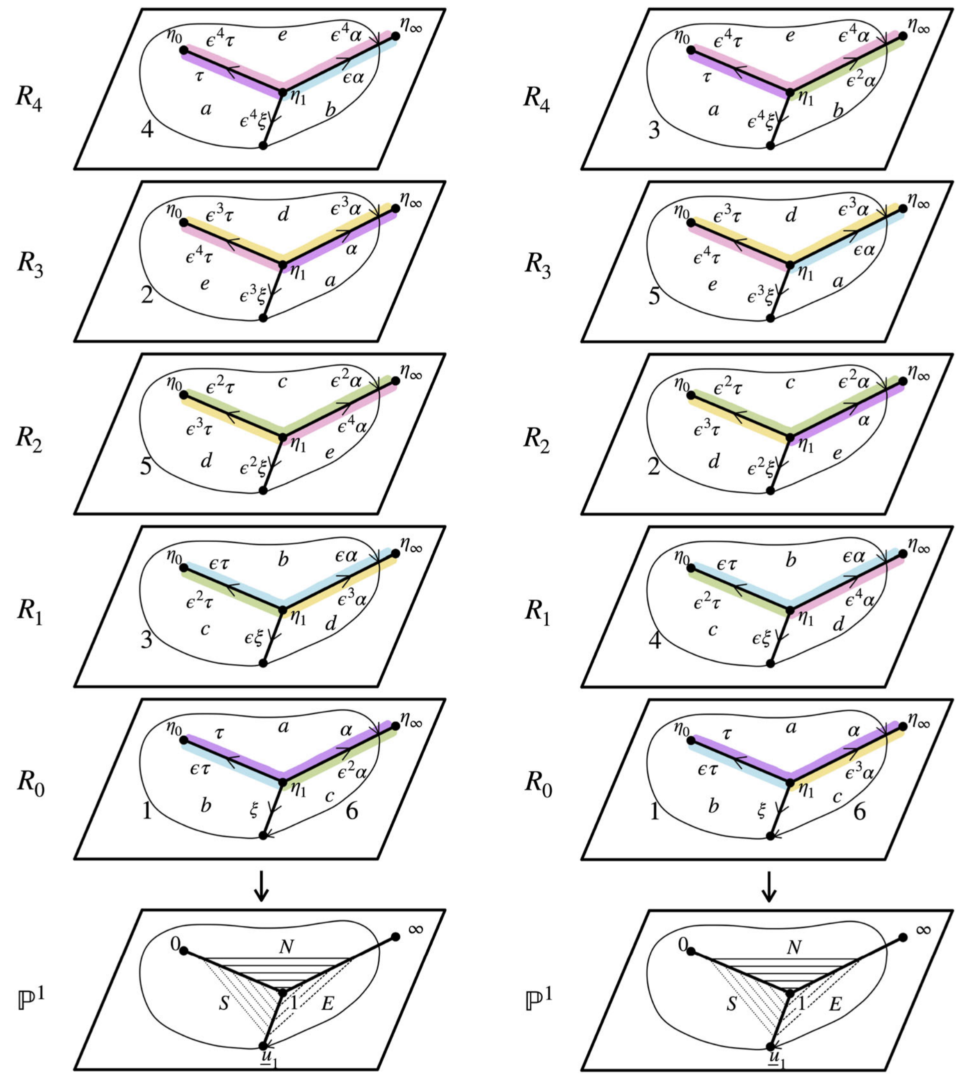

Figure 1. Examples: $n = 5$ and $k = 1$ on the left and $k = 2$ on the right.

So L is homotopic to:

$$E_1 \cdot E_3 \cdot E_2^{-1} \cdot E_4^{-1} \cdot E_2 \cdot E_1^{-1} \cdot E_4 \cdot E_3^{-1}.$$

From this, we can deduce for $n = 5$ and $k = 2$ that:

$$\Delta = E_1 \wedge (-[E_3] + [E_4]) + E_2 \wedge (-[E_4]).$$

4. Modular symbols and basis for homology

Fix an integer n. Let $W_k := W_{n,k}$ denote the smooth projective curve with affine equation $v^n = u(1-u)^k$, where k is such that $1 \le k \le n-2$ with $\gcd(n, k(k+1)) = 1$. We describe the homology group $\mathrm{H}_1(W_k, \mathbb{Z})$ using Manin's theory of modular symbols from [8], following the approach of Ejder [4]. In Corollary 4.5, we prove that a basis for $\mathrm{H}_1(W_k, \mathbb{Z})$ as a $\mathbb{Z}$-module is given by $\{[E_i] \mid 1 \le i \le n-1\}$.

4.1. A modular description of W_k

In $\mathrm{PSL}_2(\mathbb{Z})$, consider the congruence subgroup $\Gamma(2)$ and its commutator $\Gamma(2)'$. Let

$$A := \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \text{ and } B := \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}. \tag{4.1}$$

Let $\Phi(n) := \langle A^n, B^n, \Gamma(2)' \rangle$. Note that $\Phi(n) \subset \Phi_k$, where Φ_k is the congruence subgroup

$$\Phi_k := \left\langle AB^{-(k^{-1}) \bmod n},\ A^n,\ B^n,\ \Gamma(2)' \right\rangle. \tag{4.2}$$

Let $\mathfrak{H}$ denote the upper half plane. There is an isomorphism between the modular curve $X_{\Phi(n)} := \bar{\mathfrak{H}}/\Phi(n)$ and the Fermat curve $X_n\colon x^n + y^n = z^n$ by [10, Section 3]. We now give a similar description of W_k.

Lemma 4.1. *The curve W_k is isomorphic to $X_{\Phi_k} := \bar{\mathfrak{H}}/\Phi_k$. The index of $\Phi(n)$ in Φ_k is n.*

Proof. Possibly after adjusting the isomorphism $X_{\Phi(n)} \cong X_n$, we can identify A with the automorphism $\epsilon_0(x, y, z) = (\zeta x, y, z)$ and B with the automorphism $\epsilon_1(x, y, z) = (x, \zeta y, z)$, as in [4, Section 3.3]. The first statement is true because W_k is the quotient of X_n by $\langle \epsilon_0 \epsilon_1^{-(k^{-1}) \bmod n} \rangle$. The second statement follows since $n = \deg(X_n \to W_k)$. □

Let $\pi : \bar{\mathfrak{H}} \to \bar{\mathfrak{H}}/\Phi_k$ be the projection map.

The modular description of W_k allows us to use modular symbols to describe $\mathrm{H}_1(W_k, \mathbb{Z})$ as follows. A modular symbol is the image of a geodesic from α to β in $W_k(\mathbb{C})$ for some α, β in $\mathbb{P}^1(\mathbb{Q})$ and it is denoted by $\{\alpha, \beta\}$. By [8, Sections 1.3 and 1.5], every $g \in \Phi_k$ determines a modular symbol $[g] = \{\alpha_g, \beta_g\}$ where $\alpha_g := g \cdot 0$ and $\beta_g := g \cdot i\infty$. Manin proved [8, Proposition 1.4 & Proposition 1.6] that the elements of $\mathrm{H}_1(W_k, \mathbb{Z})$ are finite sums of the form $\sum_m n_m [g_m]$ where $\sum_m n_m(\pi(\beta_{g_m}) - \pi(\alpha_{g_m})) = 0$ for $n_m \in \mathbb{Z}$.

We now compute generators for the group of modular symbols of W_k.

Lemma 4.2. *With A and B as in (4.1), the sets $\Phi_k A^r B^s$ and $\Phi_k A^{r+m} B^{s-m(k^{-1}) \bmod n}$ are the same right coset of Φ_k in $\Gamma(2)$ for any $1 \le m \le n-1$. In particular, the right coset $\Phi_k A^r B^s$ equals $\Phi_k A^{r+ks}$. A set of representatives for the cosets of Φ_k in $\Gamma(2)$ is given by $\Phi_k A^r$ for $0 \le r \le n-1$.*

Proof. We note that $A, B \in \Gamma(2)$. Let $\tilde{k}$ be the unique integer such that $k^{-1} \equiv \tilde{k} \bmod n$. For $m = 1$, we compute:

$$\begin{aligned} \Phi_k A^r B^s &= \Phi_k (AB^{-\tilde{k}})(B^s A^r B^{-s} A^{-r}) A^r B^s \\ &= \Phi_k \left(A^r \left(AB^{s-\tilde{k}} \right) A^{-r} \left(AB^{s-\tilde{k}} \right)^{-1} \right) AB^{s-\tilde{k}} A^r \\ &= \Phi_k A^{r+1} B^{s-\tilde{k}}. \end{aligned}$$

By recursion, we get the desired equality for any m.

The second statement follows by taking $m = ks$.

A set of representatives for the right cosets of $\Phi(n)$ in $\Gamma(2)$ is given by $\{A^i B^j\}_{0 \le i,j \le n-1}$. By Lemma 4.1, the index of $\Phi(n)$ in Φ_k is n. So there are n right cosets of Φ_k in $\Gamma(2)$ and each of these is the union of n cosets of $\Phi(n)$ in $\Gamma(2)$. By the first statement, $\{A^r\}_{0 \le r \le n-1}$ is a complete set of representatives. □

Let $\tau = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$. The modular symbol $[\tau] = \{1, 0\}$ represents a geodesic that starts at 1 and ends at 0. To see this, we compute

$$\tau \cdot 0 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \end{bmatrix} = 1, \text{ and } \tau \cdot i\infty = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0. \tag{4.3}$$

We use the notation τ since $[\tau]$ is homotopic to the class of $\tau = \beta_W^{-1}$ as in (2.4).

Proposition 4.3. *The group of modular symbols for Φ_k is a free $\mathbb{Z}$-module of rank n with basis*

$$\{[A^r\tau] \mid 0 \leq r \leq n-1\}. \tag{4.4}$$

Proof. By [4, Proposition 3.1], the group of modular symbols for the Fermat group $\Phi(n)$ is free of rank n^2+1 generated by

$$\{[A^iB^j\tau] \mid 1 \leq i \leq n-1,\ 0 \leq j \leq n-1\} \cup \{[A^{n-1}B^j] \mid 0 \leq j \leq n-1\} \cup \{[B^{n-1}\tau]\}.$$

Since $\Phi(n) \subseteq \Phi_k$, the set of modular symbols for Φ_k is also generated as a $\mathbb{Z}$-module by these elements. All it remains to do is to find the relations between the generators. By Lemma 4.2, $[A^iB^j] = [A^{i+kj}]$, and so $[A^iB^j\tau] = [A^{i+kj}\tau]$. Thus, the modular symbols

$$\{[A^r\tau] \mid 0 \leq r \leq n-1\} \cup \{[A^r] \mid 0 \leq r \leq n-1\}$$

are generators for the group of modular symbols of Φ_k.

By [4, (3.7)] and Lemma 4.2, for any $1 \leq r \leq n-1$, we also have the relation

$$[A^r] - [A^{r-1}] = [A^{r-1}\tau] - [A^{r-k}\tau].$$

Taking $r = 1$ shows $[A] = [\tau] - [A^{1-k}\tau]$. Working inductively on i, we deduce that $[A^i]$ is a $\mathbb{Z}$-linear combination of the elements in (4.4), completing the proof that this set generates the group of modular symbols. The properties of being free and rank n follow because this proof uses all of the relations in [4, Section 3]. □

Proposition 4.4. *A basis for the homology group $\mathrm{H}_1(X_{\Phi_k}, \mathbb{Z})$ as a $\mathbb{Z}$-module is*

$$\rho_r := [A^r\tau] - [\tau] \quad \textit{for} \quad 1 \leq r \leq n-1.$$

Proof. We first show that $\rho_r := [A^r\tau] - [\tau]$ is a well-defined element in $\mathrm{H}_1(X_{\Phi_k}, \mathbb{Z})$ for all $1 \leq r \leq n-1$. It suffices to show that

$$\pi(A^r\tau \cdot 0) = \pi(\tau \cdot 0) \text{ and } \pi(A^r\tau \cdot i\infty) = \pi(\tau \cdot i\infty).$$

By (4.3), the equalities are equivalent to

$$\pi(A^r \cdot 1) = \pi(1) \text{ and } \pi(A^r \cdot 0) = \pi(0).$$

Recall that B fixes 0. So $A^r \cdot 0 = A^rB^{-(k^{-1}) \bmod n} \cdot 0$ for $r \in \{1, \ldots, n-1\}$. By Lemma 4.2, $\pi(A^r \cdot 0) = \pi(A^{r+1} \cdot 0)$. Thus $\pi(A^r \cdot 0) = \pi(\mathrm{Id} \cdot 0) = \pi(0)$.

For the other equality, as in [4, p. 2308], consider the degree n cover $X_{\Phi_k} \to X_{\Gamma(2)} \cong \bar{\mathfrak{H}}/\Gamma(2) \cong \mathbb{P}^1$. By Lemma 4.1, this corresponds to the cover $W_k \to \mathbb{P}^1$, given by $(u, v) \mapsto u$ in affine coordinates. The fact that this cover is totally ramified at η_1 over $u = 1$ implies that the same is true for $X_{\Phi_k} \to \mathbb{P}^1$. The elements $\{\pi(A^r \cdot 1)\}_{0 \leq r \leq n-1}$ all lie above the point corresponding to $u = 1$, so it follows that $\pi(A^r \cdot 1) = \pi(1)$ for all $1 \leq r \leq n-1$.

To see that the elements in $\{\rho_r\}_{1 \leq r \leq n-1}$ are $\mathbb{Z}$-linearly independent, we assume that $\sum_{r=1}^{n-1} a_r\rho_r = 0$, with $a_r \in \mathbb{Z}$. This implies that $\sum_{r=1}^{n-1} a_r[A^r\tau] - \left(\sum_{r=1}^{n-1} a_r\right)[\tau] = 0$. By Proposition 4.3, the set $\{[A^r\tau]\}_{0 \leq r \leq n-1}$ is linearly independent, so $a_r = 0$ for $1 \leq r \leq n-1$. □

Corollary 4.5. *The set $\{[E_i] \mid 1 \leq i \leq n-1\}$ is a basis for $\mathrm{H}_1(W_k, \mathbb{Z})$ as a $\mathbb{Z}$-module.*

Proof. The action of A is identified with ϵ_0 and $\epsilon_0((x, y)) = (\zeta x, y)$. Also $\epsilon((u, v)) = (u, \zeta v)$. Since $v = xy^k$, this shows that A acts like ϵ on $W_k = X_{\Phi_k}$. Since $E_i = \epsilon^i\tau \cdot \tau^{-1}$ and $[E_0] = 0$, this shows that $\rho_i = [E_i]$. The result is then immediate from Proposition 4.4. □

5. Description using invariants

As in Section 2, let $W = W_{n,k}$. In this section, we illustrate Theorem 3.5.

5.1. Some invariant elements of $\wedge^2 \mathrm{H}_1(W)$

By Corollary 4.5, $\{[E_i] \mid 1 \le i \le n-1\}$ is a basis for $\mathrm{H}_1(W,\mathbb{Z})$. For $1 \le r \le (n-1)/2$, in $\wedge^2\mathrm{H}_1(W)$, we define

$$T_r := \sum_{i=0}^{n-1} [E_i] \wedge [E_{i+r}].$$

Note that both E_i and T_r implicitly depend on k. For simplicity of notation, we write E_i rather than $[E_i]$ in the homology in the proofs in this section.

Lemma 5.1. *The element T_r is invariant under the automorphism ϵ.*

Proof. By (2.6), $E_i = e_i^{-1} \cdot e_0$. Then $\epsilon(E_i) = E_{i+1} \cdot E_1^{-1}$ in $\pi_1(W_k)$. So $\epsilon(E_i) = E_{i+1} - E_1$ in $\mathrm{H}_1(W_k,\mathbb{Z})$. We compute that

$$\begin{aligned}\epsilon(T_r) &= \sum_{i=0}^{n-1} \epsilon(E_i) \wedge \epsilon(E_{i+r}) = \sum_{i=0}^{n-1} (E_{i+1} - E_1) \wedge (E_{i+r+1} - E_1) \\ &= \sum_{i=0}^{n-1} (E_{i+1} \wedge E_{i+r+1} - E_1 \wedge E_{i+r+1} + E_1 \wedge E_{i+1}).\end{aligned}$$

Then $\sum_{i=0}^{n-1}(-E_1 \wedge E_{i+r+1} + E_1 \wedge E_{i+1}) = 0$ and so $\epsilon(T_r) = \sum_{i=0}^{n-1} E_{i+1} \wedge E_{i+r+1} = T_r$. □

5.2. Applications

By Theorem 3.5, the classifying element has the form

$$\Delta = \sum_{1 \le i < j \le n-1} c_{i,j} [E_i] \wedge [E_j].$$

In this section, we describe Δ using the invariant elements from Section 5.1.

Corollary 5.2. *Let n, k be integers such that $1 \le k \le n-2$ and $\gcd(n, k(k+1)) = 1$. Let $c \in \{1,\ldots,n-1\}$ be such that $c \equiv (k+1)^{-1} \bmod n$. Then $\Delta = \sum_{r \in S_{n,k}} (-T_{r-1} + T_r)$, where*

$$S_{n,k} = \{r \in \mathbb{Z}/n\mathbb{Z} \mid r \equiv j(k+1) \bmod n \text{ for some } 1 \le j \le c-1\}.$$

Proof. This is immediate from Theorem 3.5. □

Corollary 5.3. *With the same hypotheses as Corollary 5.2:*

(1) *If $k = 1$, then $\Delta = \sum_{r=1}^{(n-1)/2} (-1)^r T_r$.*
(2) *If $k = 2$, then $\Delta = \sum_{r=1}^{(n-1)/2} w_r T_r$ where $w_r = 1$ if $r \equiv 0 \bmod 3$ and $w_r = -1$ if $r \equiv n \bmod 3$.*
(3) *If $k = n-2$, then $\Delta = -T_1$.*
(4) *If $k = n-3$, then $\Delta = \sum_{r=2}^{(n-1)/2} (-1)^{r-1} T_r$.*
(5) *If $k = (n-1)/2$, then $\Delta = -T_{(n-1)/2}$.*
(6) *If $k = (n-3)/2$, then $\Delta = T_{(n-1)/2} - T_1$.*
(7) *If $n \equiv 2 \bmod 3$ and $k = (n-2)/3$, then $\Delta = T_{k+1} - T_k$.*
If $n \equiv 1 \bmod 3$ and $k = (2n-2)/3$, then $\Delta = T_{(k+2)/2} - T_{k/2}$.

Proof. (1) If $k = 1$, then $c = (n+1)/2$. Then $r \in S_{n,k}$ if and only if r is even.
(2) Write $c = (n+1)/3$ if $n \equiv 2 \bmod 3$ and $c = (2n+1)/3$ if $n \equiv 1 \bmod 3$. Write $\ell = n - 3$. Then

$$c_{I,J} = \begin{cases} -1 & \text{if } I - J \equiv \ell + 1,\ 2\ell + 1,\ \ldots,\ (c-1)\ell + 1 \bmod n; \\ +1 & \text{if } I - J \equiv \ell,\ 2\ell,\ \ldots,\ (c-1)\ell \bmod n; \\ 0 & \textit{otherwise.} \end{cases}$$

(3) If $k = n-2$, then $c = n-1$. In this case, we cover every sheet $0, 1, 2, \ldots, n-2, n-1$ in order, starting with sheet 0 and ending with sheet $n-1$. It is more convenient to consider the edges between τ and τ^{-1}, which are $(\epsilon^{n-1}\tau)^{-1}$ and $\epsilon\tau$. So $E_0 \wedge E_1$ and $-E_{n-1} \wedge E_0$ appear in Δ. So $c_{I,J} = -1$ (resp. $+1$) if $J - I \equiv 1 \bmod n$ (resp. $J - I \equiv n - 1 \bmod n$) and $c_{I,J} = 0$ otherwise.
(4) If $k = n - 3$, then $c = (n-1)/2$. We omit the details.
(5) If $k = (n-1)/2$, then $c = 2$. It follows that $c_{I,J} = -1$ (resp. $+1$) only if $J - I \equiv (n-1)/2 \bmod n$ (resp. $(n+1)/2 \bmod n$).
(6) If $k = (n-3)/2$, then $c = n - 2$. In this case, we cover all but the $(n-1)$st sheet, starting with sheet 0, then $(n+1)/2$, then 1, then $(n+3)/2$, etc. It is more convenient to consider the edges between τ and τ^{-1}, which are $(\epsilon^{n-1}\tau)^{-1}$, $\epsilon\tau$, $\epsilon^{(n+1)/2}\tau$, and $(\epsilon^{(n-1)/2}\tau)^{-1}$. So $c_{I,J} = -1$ if $J - I \equiv (n+1)/2$ or $1 \bmod n$, $c_{I,J} = +1$ if $J - I \equiv (n-1)/2$ or $n - 1 \bmod n$, and $c_{I,J} = 0$ otherwise.
(7) If $k = (n-2)/3$ and $n \equiv 2 \bmod 3$, (resp. $k = (2n-2)/3$ and $n \equiv 1 \bmod 3$), then $c = 3$. Let $\ell = n - (k+1)$ which equals $(2n-1)/3$ if $n \equiv 2 \bmod 3$ and equals $(n-1)/3$ if $n \equiv 1 \bmod 3$. Then $c_{I,J} = -1$ if $J - I \equiv \ell, 2\ell \bmod n$ and $c_{I,J} = +1$ if $J - I \equiv \ell + 1, 2\ell + 1 \bmod n$.

□

Corollary 5.2 determines Δ for all values of k when $3 \leq n < 11$ and for all but two values of k when $n = 11$. We include these two as final examples.

Example 5.4. *If $n = 11$ and $k = 6$, then $c = 8$ and $\Delta = -T_1 + T_3 - T_4$.*

Example 5.5. *If $n = 11$ and $k = 7$, then $c = 7$ and $\Delta = -T_1 + T_2 - T_3 + T_5$.*

Acknowledgments

We would like to thank the anonymous referee for their thoughtful and constructive feedback.

Funding

Duque-Rosero was supported by a grant from the Simons Foundation (550029, to Voight). Pries was supported by NSF grant DMS-22-00418.

References

[1] Anderson, G. W. (1987). Torsion points on Fermat Jacobians, roots of circular units and relative singular homology. *Duke Math. J.* 54(2):501–561.
[2] Davis, R., Pries, R., Stojanoska, V., Wickelgren, K. (2018). The Galois action and cohomology of a relative homology group of Fermat curves. *J. Algebra* 505:33–69.
[3] Davis, R., Pries, R., Wickelgren, K. (2023). The Galois action on the lower central series of the fundamental group of the Fermat curve. *Isr. J. Math.*
[4] Ejder, Ö. (2019). Modular symbols for Fermat curves. *Proc. Amer. Math. Soc.* 147(6):2305–2319.
[5] Hain, R. (1997). Infinitesimal presentations of the Torelli groups. *J. Amer. Math. Soc.* 10(3):597–651.
[6] Labute, J. P. (1970). On the descending central series of groups with a single defining relation. *J. Algebra* 14:16–23.
[7] Lazard, M. (1954). Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. Ecole Norm. Sup. (3)* 71:101–190.

[8] Manin, J. I. (1972). Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.* 6(1): 19–66.
[9] Kumar Murty, V. (1993). *Introduction to Abelian Varieties*, CRM Monograph Series, Vol. 3. Providence, RI: American Mathematical Society.
[10] Rohrlich, D. E. (1977). Points at infinity on the Fermat curves. *Invent. Math.* 39(2):95–127.
[11] Serre, J.-P. (1965). *Lie Algebras and Lie Groups*. Lectures given at Harvard University, Vol. 1964. New York-Amsterdam: W. A. Benjamin, Inc.