GALOIS ACTION ON THE HOMOLOGY OF FERMAT CURVES

RACHEL DAVIS, RACHEL PRIES, VESNA STOJANOSKA, AND KIRSTEN WICKELGREN

Abstract. In [And87], Anderson determines the homology of the degree n Fermat curve as a Galois module for the action of the absolute Galois group $G_{\mathbb{Q}(\zeta_n)}$. In particular, when n is an odd prime p, he shows that the action of $G_{\mathbb{Q}(\zeta_p)}$ on a more powerful relative homology group factors through the Galois group of the splitting field of the polynomial $1-(1-x^p)^p$. If p satisfies Vandiver's conjecture, we give a proof that the Galois group G of this splitting field over $\mathbb{Q}(\zeta_p)$ is an elementary abelian p-group of rank $(p+1)/2$. Using an explicit basis for G, we completely compute the relative homology, the homology, and the homology of an open subset of the degree 3 Fermat curve as Galois modules. We then compute several Galois cohomology groups which arise in connection with obstructions to rational points.
MSC2010: 11D41, 11R18, 11R34, 14F35, 14G25, 55S35
Keywords: Fermat curve, cyclotomic field, homology, cohomology, Galois module, étale fundamental group

1. Introduction

The Galois actions on the étale homology, cohomology, and homotopy groups of varieties carry information about rational points. We revisit results of Anderson [And87] on a relative homology group of the Fermat curve of prime exponent to make his results amenable to computations of groups such as $H^1(G_S, \pi_1^{\mathrm{ab}})$ and $H^2(G_S, \pi_1^{\mathrm{ab}} \wedge \pi_1^{\mathrm{ab}})$ where G_S denotes a Galois group of a maximal extension of a number field with restricted ramification and π_1^{ab} denotes the abelianized geometric fundamental group of the Fermat curve, or of an open subset. These groups arise in obstructions of Ellenberg to rational points [Ell00] as well as in McCallum's application of the method of Coleman and Chabauty to Fermat curves [McC94].

Let k be a number field. The Fermat curve of exponent n is the smooth projective curve $X \subset \mathbb{P}^2_k$ of genus $g=(n-1)(n-2)/2$ given by the equation

$$x^n + y^n = z^n.$$

The affine open $U \subset X$ given by $z \neq 0$ has affine equation $x^n+y^n=1$. The closed subscheme $Y \subset X$ defined by $xy=0$ consists of $2n$ points. Let $H_1(U, Y; \mathbb{Z}/n)$

We would like to thank BIRS for hosting the WIN3 conference where we began this project. Some of this work was done while the third and fourth authors were in residence at MSRI during the spring 2014 Algebraic topology semester, supported by NSF grant 0932078 000. The second author was supported by NSF grant DMS-1101712. The third author was supported by NSF grant DMS-1307390. The fourth author was supported by an American Institute of Mathematics five year fellowship and NSF grant DMS-1406380. We would also like to thank Sharifi and the referee for helpful remarks.

denote the étale homology group of the pair $(U \otimes \overline{k}, Y \otimes \overline{k})$, which is a continuous module over the absolute Galois group G_k of k. The $\mu_n \times \mu_n$ action on X given by

$$(\zeta^i, \zeta^j) \cdot [x, y, z] = [\zeta^i x, \zeta^j y, z],\ (\zeta^i, \zeta^j) \in \mu_n \times \mu_n$$

determines an action on U and Y. These actions give $H_1(U, Y; \mathbb{Z}/n)$ the structure of a $(\mathbb{Z}/n)[\mu_n \times \mu_n]$ module. As a $(\mathbb{Z}/n)[\mu_n \times \mu_n]$ module, $H_1(U, Y; \mathbb{Z}/n)$ is free of rank one [And87, Theorem 6], with generator denoted β. It follows that the Galois action of $\sigma \in G_k$ is determined by $\sigma\beta = B_\sigma \beta$ for some $B_\sigma \in (\mathbb{Z}/n)[\mu_n \times \mu_n]$.

Anderson shows that B_σ is determined by an analogue of the classical gamma function $\Gamma_\sigma \in \mathbb{Z}/n^{\mathrm{sh}}[\mu_n]$, where $\mathbb{Z}/n^{\mathrm{sh}}$ denotes the strict Henselization of $\mathbb{Z}/n$. In particular, there is a formula [And87, Theorem 9, Theorem 7] recalled in (2.b) as the equation $d'^{sh}(\Gamma_\sigma) = B_\sigma$ with d'^{sh} defined in (2.a) and immediately below. The canonical derivation $d : \mathbb{Z}/n^{\mathrm{sh}}[\mu_n] \to \Omega\mathbb{Z}/n^{\mathrm{sh}}[\mu_n]$ from the ring $\mathbb{Z}/n^{\mathrm{sh}}[\mu_n]$ to its module of Kähler differentials allows one to take the logarithmic derivative $\operatorname{dlog} \Gamma_\sigma$ of Γ_σ, which it is convenient to view as an element of a particular quotient of $\Omega\mathbb{Z}/n^{\mathrm{sh}}[\mu_n]$. See Section 2. For n prime, $\operatorname{dlog} \Gamma_\sigma$ determines B_σ uniquely [And87, 10.5.2,10.5.3]. The function $\sigma \mapsto \operatorname{dlog} \Gamma_\sigma$ is in turn determined by a relative homology group of the punctured affine line $H_1(\mathbb{A}^1 - V(\sum_{i=0}^{n-1} x^i), \{0, 1\}; \mathbb{Z}/n)$ [And87, Theorem 10]. Putting this together, Anderson shows that, for $n = p$ a prime, the $G_{\mathbb{Q}(\zeta_p)}$ action on $H_1(U, Y; \mathbb{Z}/p)$ factors through $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$ where L is the splitting field of $1 - (1 - x^p)^p$. Ihara [Iha86] and Coleman [Col89] obtain similar results from different viewpoints.

Let K denote the cyclotomic field $K = \mathbb{Q}(\zeta_n)$, where ζ_n denotes a primitive nth root of unity, and let G_K be its absolute Galois group. When the exponent is clear, let ζ denote ζ_n or ζ_p for a prime p. Let κ denote the classical Kummer map; for $\theta \in K^*$, let $\kappa(\theta) : G_K \to \mu_n$ be defined by

$$\kappa(\theta)(\sigma) = \frac{\sigma \sqrt[n]{\theta}}{\sqrt[n]{\theta}}.$$

In Proposition 4.1, we determine $\operatorname{dlog} \Gamma_\sigma$ in terms of the classical Kummer map for all $n \geq 3$, modulo indeterminacy which does not affect B_σ, with the answer being $\operatorname{dlog} \Gamma_\sigma = \sum_{i=1}^{n-1} \kappa(1 - \zeta^{-i})(\sigma)\zeta^i \operatorname{dlog} \zeta$.

Recall that Vandiver's Conjecture for a prime p is that p does not divide h^+, where h^+ is the order of the class group of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. It has been verified for all p less than 163 million. For $n = p$ a prime satisfying Vandiver's conjecture, we give a proof that $\mathrm{Gal}(L/K)$ is isomorphic to $(\mathbb{Z}/p)^r$ with $r = (p + 1)/2$ in Proposition 3.6. This is false for p not satisfying Vandiver's conjecture as seen in Remark 3.8. There are a couple of natural choices for such an isomorphism. In Corollary 3.7, we show that the following map gives an isomorphism:

$$\Phi = \kappa(\zeta) \times \prod_{i=1}^{\frac{p-1}{2}} \kappa(1 - \zeta^{-i}) : \mathrm{Gal}(L/K) \to (\mu_p)^{\frac{p+1}{2}}.$$

For $p = 3$, we use the formula for $\operatorname{dlog} \Gamma_\sigma$ to compute B_σ explicitly in Lemma 5.5. It is possible to extend this calculation to compute B_σ for all primes p and we will make this computation available in a forthcoming paper. (As seen in Remark 5.3, the element $\operatorname{dlog} \Gamma_\sigma$ and [And87, 10.5.2] do not determine B_σ when n is not prime so the calculation of B_σ when n is not prime will require further input.) Combining the above, we obtain:

Theorem 1.1. *Let $p = 3$ and $K = \mathbb{Q}(\zeta_p)$. The G_K-action on $H_1(U, Y; \mathbb{Z}/p)$ factors through $G_K \to \mathrm{Gal}(L/K)$, where L denotes the splitting field of $1 - (1 - x^p)^p$ (or equivalently of $x^6 - 3x^3 + 3$). Write $H_1(U, Y; \mathbb{Z}/p) \cong \mathbb{Z}_p[\zeta_0, \zeta_1]/\langle \zeta_0^p - 1, \zeta_1^p - 1\rangle$ and $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p \times \mathbb{Z}/p$. Then $(c_0, c_1) \in \mathbb{Z}/p \times \mathbb{Z}/p$ acts on $\mathbb{Z}_p[\zeta_0, \zeta_1]/\langle \zeta_0^p - 1, \zeta_1^p - 1\rangle$ by multiplication by $B_\sigma = \sum_{i,j=0}^{p-1} b_{i,j}\zeta_0^i\zeta_1^j$ where*

$$b_{0,0} = 1 + c_0 - c_0^2$$
$$b_{0,1} = c_1 - c_0^2$$
$$b_{1,1} = -c_1 - c_0^2.$$

and where the rest of the coefficients $b_{i,j}$ are determined by $b_{i,j} = b_{j,i}$, and the fact that $b_{0,0} + b_{0,1} + b_{0,2} = 1$, $b_{1,0} + b_{1,1} + b_{1,2} = 0$, and $b_{2,0} + b_{2,1} + b_{2,2} = 0$.

We have an analogous calculation of $H_1(U, Y; \mathbb{Z}/p)$ for all primes p satisfying Vandiver's conjecture, which we will make available shortly.

Given the Galois action on $H_1(U, Y; \mathbb{Z}/n)$, we compute the Galois actions on $H_1(U; \mathbb{Z}/n)$ and $H_1(X; \mathbb{Z}/n)$ for all $n \geq 3$ in Section 6.

These computations can be used to study rational points on varieties in the following way. Let Z be a scheme over k, and for simplicity assume that Z has a rational point b. (This assumption is unnecessary, but it is satisfied in the situations encountered in this paper and it simplifies the exposition.) Choose a geometric point of Z with image b and let $\pi = \pi_1(Z_{\overline{k}}, b)$ denote the geometric étale fundamental group of Z based at the chosen geometric point. The generalized *Kummer map* associated to Z and b is the map $\kappa : Z(k) \to H^1(G_k, \pi)$ defined by

$$\kappa(x) = [\sigma \mapsto \gamma^{-1}\sigma\gamma]$$

where γ is an étale path from b to a geometric point above x. Before returning to the potential application to rational points, we remark that the map κ is functorial and the computation of $\operatorname{dlog}\Gamma_\sigma$ in Proposition 4.1 is obtained by applying κ to the K-map $\mathbb{A}^1 - V(\sum_{i=0}^{n-1} x^i) \to \mathbb{G}_m^{n-1}$.

From κ, we also obtain a map $\kappa^{\mathrm{ab,p}} : Z(k) \to H^1(G_k, \pi^{\mathrm{ab}} \otimes \mathbb{Z}_p)$ defined to be the composition of κ with the map $H^1(G_k, \pi) \to H^1(G_k, \pi^{\mathrm{ab}} \otimes \mathbb{Z}_p)$ induced by the quotient map $\pi \to \pi^{\mathrm{ab}} \otimes \mathbb{Z}_p$, where $\mathbb{Z}_p$ denotes the p-adic integers. For Z a curve or abelian variety over a number field, $\kappa^{\mathrm{ab,p}}$ is well-known to be injective. Let S denote a set of places of k including the infinite places, all the primes of bad reduction of Z and a place above p. Let $G_S = \pi_1(\mathcal{O}_k[1/S])$ denote the Galois group of the maximal extension of k ramified only over S. Assume that Z is proper to simplify exposition. Then $\kappa^{\mathrm{ab,p}}$ factors through a map $\kappa^{\mathrm{ab,p}} : Z(k) \to H^1(G_S, \pi^{\mathrm{ab}} \otimes \mathbb{Z}_p)$. Let $\pi = [\pi]_1 \supseteq [\pi]_2 \supseteq \ldots$ denote the lower central series of the profinite group π, where $[\pi]_m$ is the closure of the subgroup $[[\pi]_{m-1}, \pi]$ generated by commutators of elements of π with elements of $[\pi]_{m-1}$. Using work of Schmidt and Wingberg [SW92], Ellenberg [Ell00] defines a series of obstructions to a point of the Jacobian of a curve Z lying in the image of the Abel-Jacobi map associated to b. The first of these obstructions is defined using a map

$$\delta_2 : H^1(G_S, \pi^{\mathrm{ab}} \otimes \mathbb{Z}_p) \to H^2(G_S, ([\pi]_2/[\pi]_3) \otimes \mathbb{Z}_p)$$

such that $\operatorname{Ker}\delta_2 \supset Z(k)$. Zarkhin defines a similar map [Zar74]. The group $([\pi]_2/[\pi]_3) \otimes \mathbb{Z}_p$ fits into a short exact sequence

$$0 \to \mathbb{Z}_p(1) \to (\pi^{\mathrm{ab}} \wedge \pi^{\mathrm{ab}}) \otimes \mathbb{Z}_p \to ([\pi]_2/[\pi]_3) \otimes \mathbb{Z}_p \to 0.$$

There are mod p versions of δ_2 and the generalized Kummer maps. A more detailed account of Ellenberg's obstructions is in [Wic12].

Thus computations of $H^1(G_S, \pi^{\mathrm{ab}} \otimes \mathbb{Z}/p)$ and $H^2(G_S, (\pi^{\mathrm{ab}} \wedge \pi^{\mathrm{ab}}) \otimes \mathbb{Z}/p)$ give information about rational points. Groups closely related to $H^1(G_S, \pi^{\mathrm{ab}} \otimes \mathbb{Z}/p)$ also appear in [CNGJ13] and [McC94].

The final section of this paper includes calculations of $H^1(\mathrm{Gal}(L/K), M)$ and $H^2(\mathrm{Gal}(L/K), M)$ for M each of $H_1(U, Y; \mathbb{Z}/n)$, $H_1(U; \mathbb{Z}/n)$, $H_1(X; \mathbb{Z}/n)$, and $H_1(U, \mathbb{Z}/n) \wedge H_1(U, \mathbb{Z}/n)$. These can be inserted into the Hochschild-Serre spectral sequence

$$H^i(\mathrm{Gal}(L/K), H^j(G_{S,L}, M)) \Rightarrow H^{i+j}(G_{S,K}, M),$$

where $G_{S,L}$ denotes the Galois group of the maximal extension of L only ramified at places above S, and $G_{S,K} = G_S$. Since $H_1(U, Y; \mathbb{Z}/n)$, $H_1(U; \mathbb{Z}/n)$, $H_1(X; \mathbb{Z}/n)$ are $\pi^{\mathrm{ab}} \otimes \mathbb{Z}/n$ for $Z = U/Y$, $Z = U$ and $Z = X$ respectively, these are groups mentioned above, and appear in Ellenberg's obstructions. This is the subject of on-going work.

1.1. **Notation.** Let $n \geq 3$ be an integer; often n will be a prime p. Let ζ be a fixed primitive n-th root of unity and $K = \mathbb{Q}(\zeta)$. For brevity, let $A = \mathbb{Z}/n$, and let A^{sh} denote the strict Henselization of A. If $n = p$ is prime, then the field A is a Henselian local ring and its strict Henselization is the separable closure $A^{sh} \simeq \bar{\mathbb{F}}_p$.

If k is any number field, G_k denotes the absolute Galois group of k.

Definition 1.2. Given a primitive nth root $\sqrt[n]{\theta}$ of $\theta \in k$ and $\sigma \in G_k$, then $\kappa(\theta)\sigma$ is the element of A such that

$$\sigma \sqrt[n]{\theta} = \zeta^{\kappa(\theta)\sigma} \sqrt[n]{\theta}.$$

Remark 1.3. The map $\kappa : k^* \to H^1(G_k, \mathbb{Z}/n(1))$ defined by letting $\kappa(\theta)$ be represented by the twisted homomorphism $\sigma \mapsto \kappa(\theta)\sigma$ is the generalized Kummer map of $\mathbb{G}_{m,k}$ with base point $1 \in \mathbb{G}_{m,k}(k)$. Here $\mathbb{Z}/n(1)$ is the Galois module with underlying group $\mathbb{Z}/n$ and Galois action given by the cyclotomic character. See, for example, [Wic12, 12.2.1 Example 1].

For $\theta \in K^*$ and $n = p$, the map $\kappa(\theta) : G_K \to \mathbb{Z}/p$ is a homomorphism and is independent of the choice of pth root of θ because $\mu_p \subset K$.

2. Anderson's results, revisited

In this section, we recall results from [And87] that are relevant for this paper. Recall that $K = \mathbb{Q}(\zeta)$, that $U \subset \mathbb{A}^2_K$ denotes the affine Fermat curve over K with equation $x^n + y^n = 1$, and that $Y \subset U$ is the divisor defined by $xy = 0$. The path $\beta : [0, 1] \to U(\mathbb{C})$ given by $t \mapsto (\sqrt[n]{t}, \sqrt[n]{1-t})$, where $\sqrt[n]{-}$ denotes the real nth root, determines a singular 1-simplex in the homology of U relative to Y whose class we denote by the same name.

For $m \in \mathbb{N}$, let Λ_m denote the group ring over A of the finite group $\mu_n(\mathbb{C})^{\times(m+1)}$. Then Λ_m has a natural G_K-action. For $0 \leq i \leq m$, let ζ_i denote a primitive nth root of unity in the ith copy of $\mu_n(\mathbb{C})$. Then

$$\Lambda_m = A[\zeta_0, \ldots, \zeta_m]/(\zeta_0^n - 1, \ldots, \zeta_m^n - 1).$$

There is an action of Λ_1 on U given by $\zeta_0^i \times \zeta_1^j : (x, y) \mapsto (\zeta_0^i x, \zeta_1^j y)$. This action stabilizes Y. Thus the relative homology group $H_1(U, Y; A)$ is a Λ_1-module. Note that $H_1(U, Y; A)$ has rank n^2 over A.

Anderson describes the G_K-action on $H_1(U, Y; A)$. First, [And87, Theorem 6] states that $H_1(U, Y; A)$ is a free rank one module over Λ_1 generated by the class β.

Specifically, $\sigma \in G_K$ acts A-linearly, and

$$\sigma \cdot (\zeta_0^i \zeta_1^j \beta) = (\sigma \cdot \zeta_0^i)(\sigma \cdot \zeta_1^j) B_\sigma \beta,$$

where B_σ is a unit in Λ_1 defined by

$$\sigma \cdot \beta = B_\sigma \beta.$$

Thus to describe the G_K-action on $H_1(U, Y; A)$, it is necessary and sufficient to describe the action on the element β.

Anderson also proves that the action of the absolute Galois group $G_{\mathbb{Q}}$ on $H_1(U, Y; A)$ factors through a finite quotient. This result is a consequence of the analysis in the rest of the section. In particular, if n is a prime p, then $\sigma \in G_K$ acts trivially on $H_1(U, Y; A)$ if and only if σ fixes the splitting field L of the polynomial $f_p = 1 - (1 - x^p)^p$, [And87, Section 10.5]. In Section 3, we prove that $\mathrm{Gal}(L/K)$ is an elementary abelian p-group of rank at most $(p + 1)/2$.

Anderson highlights the following application of this result. By [And87, Lemma, page 558], there is a connection between the action of $\sigma \in G_{\mathbb{Q}}$ on $H_1(U, Y; A)$ and the action of σ on the fields of definition of points of a generalized Jacobian of X.

Theorem 2.1 ([And87], Theorem 0)**.** *Let S be the generalized Jacobian of X with conductor ∞. Let b denote the $\mathbb{Q}$-rational point of S corresponding to the difference of the points $(0, 1)$ and $(1, 0)$. The number field generated by the coordinates of the nth roots of b in $S(\overline{\mathbb{Q}})$ contains the splitting field L of the polynomial $1 - (1 - x^n)^n$, with equality if n is prime.*

Information on fields generated by points of the Jacobian of quotients of Fermat curves is also contained in [CNGJ13], [CTT98], [Gre81], and[Tze07].

In the remainder of this section, we describe Anderson's method for determining B_σ. Let $b_{i,j}$ denote the coefficients of B_σ, so that

$$B_\sigma = \sum_{0 \leq i,j < n} b_{i,j} \zeta_0^i \zeta_1^j.$$

It will often be convenient to arrange the coefficients of B_σ in an $n \times n$ matrix.

Let $w : \Lambda_1 \to \Lambda_1$ be the map induced by swapping the two copies of $\mu_n(\mathbb{C})$, i.e. by swapping ζ_0 and ζ_1. Then w preserves the units in Λ_1. Let $(\Lambda_1^\times)^w$ denote the symmetric units, i.e., the units fixed by w. If $a_{i,j} \in A$, then an element

$$\sum_{0 \leq i,j < n} a_{i,j}\zeta_0^i\zeta_1^j \in \Lambda_1^\times$$

is in $(\Lambda_1^\times)^w$ precisely when $a_{i,j} = a_{j,i}$ for all i, j.

Fact 2.2. [And87, Theorem 7] If $\sigma \in G_{\mathbb{Q}}$, then $B_\sigma \in (\Lambda_1^\times)^w$. In other words, the coefficients of B_σ are symmetric; $b_{i,j} = b_{j,i}$ for any $0 \leq i, j < n$.

Next, consider the map $d'' : (\Lambda_1^\times)^w \to \Lambda_2^\times$ given by

$$\sum a_{i,j}\zeta_0^i\zeta_1^j \mapsto \frac{\left(\sum a_{i,j}\zeta_0^j\zeta_1^i\zeta_2^j\right)\left(\sum a_{i,j}\zeta_0^i\zeta_2^j\right)}{\left(\sum a_{i,j}\zeta_0^i\zeta_1^j\zeta_2^j\right)\left(\sum a_{i,j}\zeta_1^i\zeta_2^j\right)}.$$

By [And87, Theorem 7], B_σ is in the kernel of d''. In particular, there is an equality in $\Lambda_2^\times$, given by

$$\left(\sum b_{i,j}\zeta_0^j\zeta_1^i\zeta_2^j\right)\left(\sum b_{i,j}\zeta_0^i\zeta_2^j\right) = \left(\sum b_{i,j}\zeta_0^i\zeta_1^j\zeta_2^j\right)\left(\sum b_{i,j}\zeta_1^i\zeta_2^j\right).$$

This gives, via the map $\Lambda_2^\times \to \Lambda_1^\times$ sending $\zeta_2 \mapsto 1$, the equality

$$\left(\sum b_{i,j}\zeta_0^j\zeta_1^i\right)\left(\sum b_{i,j}\zeta_0^i\right) = \left(\sum b_{i,j}\zeta_0^i\zeta_1^j\right)\left(\sum b_{i,j}\zeta_1^i\right).$$

By Fact 2.2, the first terms on each side cancel giving

$$\sum b_{i,j}\zeta_0^i = \sum b_{i,j}\zeta_1^j.$$

This is only possible if the following is true.

Fact 2.3. [And87, 10.5.4] If $1 \leq i \leq n$, then $\sum_{0 \leq j < n} b_{i,j} = 0$.

In other words, the entries of each column of the matrix B_σ sum up to zero, for all but the zeroth column. By Fact 2.2, the entries of each row of the matrix B_σ also sum up to zero, for all but the zeroth row.

Furthermore, consider the map $d' : \Lambda_0^\times \to (\Lambda_1^\times)^w$ given by

$$\sum a_i\zeta_0^i \mapsto \frac{\left(\sum a_i\zeta_0^i\right)\left(\sum a_i\zeta_1^i\right)}{\left(\sum a_i\zeta_0^i\zeta_1^i\right)}, \tag{2.a}$$

as well as its extension $d'^{sh} : \bar{\Lambda}_0^\times \to (\bar{\Lambda}_1^\times)^w$, where $\bar{\Lambda}_i = \Lambda_i \otimes_A A^{sh}$. The kernel $\mathrm{Ker}(d'^{sh})$ is determined in [And87, Proposition 8.3.1]; when $n = p$ is prime, it is the cyclic subgroup of order p multiplicatively generated by ζ_0.

Fact 2.4. [And87, Theorem 9] Let $n \geq 3$ and let $\mathrm{Ker}(d'^{sh})$ denote the kernel of d'^{sh}. In $\bar{\Lambda}_0^\times/\mathrm{Ker}(d'^{sh})$, there exists a unique element Γ_σ which maps to B_σ under d'^{sh}.

In the sequel, the notation Γ_σ will also be used to denote an element of $\bar{\Lambda}_0^\times$ representing this coset in $\bar{\Lambda}_0^\times/\mathrm{Ker}(d'^{sh})$.

Fact 2.5. [And87, 9.6 and 10.5.2] The difference $B_\sigma - 1$ lies in the augmentation ideal $(1 - \epsilon_0)(1 - \epsilon_1)\Lambda_1$.

Consider the element Γ_σ such that

$$d'^{sh}(\Gamma_\sigma) = B_\sigma. \tag{2.b}$$

By Fact 2.4, in order to determine B_σ, it suffices to find the preimage Γ_σ. To accomplish this, Anderson looks at the logarithmic derivative homomorphisms from the groups of units $\Lambda_k^\times$ to the Kähler differentials $\Omega(\Lambda_k)$. This has the geometric meaning of comparing with "the circular motive," where the Galois action is more transparent.

There is a commutative square

$$\begin{array}{ccc} \bar{\Lambda}_0^\times & \xrightarrow{d'} & (\bar{\Lambda}_1^\times)^w \\ {\scriptstyle \mathrm{dlog}}\downarrow & & \downarrow{\scriptstyle \mathrm{dlog}} \\ \Omega(\bar{\Lambda}_0) & \longrightarrow & \Omega(\bar{\Lambda}_1)^w, \end{array}$$

where the bottom horizontal map is defined analogously to d'. Note that for each m, the $\bar{\Lambda}_m$-module $\Omega(\bar{\Lambda}_m)$ is free on generators $\{\mathrm{dlog}\,\zeta_i\}_{0\le i\le m}$.

Here is some notation needed to describe $\mathrm{dlog}\,\Gamma_\sigma$. Let $\tilde{V} = \mathbb{A}^1 - \mu_n$ and let $V = \tilde{V} \cup \{1\}$. Let λ_0 be a small counterclockwise loop around 1. Choose the isomorphism

$$H_1(\tilde{V}; A) = A[\mu_n]\lambda_0 \simeq \Omega A[\Lambda_0],$$

where $\lambda_0 \mapsto \frac{d\epsilon_0}{\epsilon_0}$.

Consider the exact sequence from [And87, §9]

$$0 \to A\lambda_0 \to H_1(\tilde{V}; A) \to H_1(V; A) \to 0,$$

or

$$0 \to A\frac{d\epsilon_0}{\epsilon_0} \to \Omega A[\Lambda_0] \to H_1(V; A) \to 0, \tag{2.c}$$

which identifies $H_1(V; A)$ as a quotient of $\Omega(\Lambda_0)$.

Let Z denote the subscheme of V defined by the vanishing of $x_0(1 - x_0)$, i.e., the points 0 and 1 in V. Let $\psi \in H_1(V, Z; A)$ denote the homology class represented by the cycle given by the interval $[0, 1]$. Let $(\sigma - 1)\psi$ denote the cycle given by concatenating the path $\sigma\psi$ and the path ψ traveled in reverse. Since G_K fixes the endpoints of ψ, the cycle $(\sigma - 1)\psi$ represents a class in $H_1(V; A) = H_1(V, \emptyset; A)$.

Let Ψ_σ denote the coset in $\Omega(\Lambda_0)/A\,\mathrm{dlog}\,\zeta_0$ which corresponds to the homology class of $(\sigma - 1)\psi$ under (2.c). The following theorem computes $\mathrm{dlog}\,\Gamma_\sigma$ to be Ψ_σ.

Theorem 2.6. [And87, Theorem 10] $\mathrm{dlog}\,\Gamma_\sigma \in \Omega(\bar{\Lambda}_0)$ *represents the* $A^{sh}\,\mathrm{dlog}\,\zeta_0$-*coset* Ψ_σ.

For this paper, the importance of Theorem 2.6 lies in the geometric description of Ψ_σ. This description shows that $\sigma \mapsto \Psi_\sigma$ is the image of a rational point under a generalized Kummer map of the sort which arises in the section conjecture. We use this observation to compute Ψ_σ in Section 4. By Theorem 2.6, we have therefore also computed $\mathrm{dlog}\,\Gamma_\sigma$.

To give a complete description of $H_1(U,Y;A)$ as a Galois module, it thus suffices to achieve the following goal, which we complete in Section 5 for the case $n=3$ and in future work for n an odd prime.

Goal: reconstruct B_σ from Ψ_σ.

3. Galois group of the splitting field of $1-(1-x^p)^p$ over K

Let $n=p$ be an odd prime and let ζ be a primitive pth root of unity. The choice of ζ fixes an identification $\mathbb{Z}/p \to \mu_p$ by sending i to ζ^i. Let $K=\mathbb{Q}(\zeta)$.

Let L be the splitting field of the polynomial $f_p(x)=1-(1-x^p)^p$. In Proposition 3.6, we determine the structure of the Galois group $G=\mathrm{Gal}(L/K)$ for primes p satisfying Vandiver's conjecture. The techniques in this section are well-known to experts but we could not find an off-the-shelf reference for this result. Before starting the proof, we describe some motivation for it in the next remark.

Remark 3.1.
(1) As seen in Theorem 2.1, L is the field of definition of the pth roots of a point b in a certain generalized Jacobian. By [And87, Section 10.5], an automorphism $\sigma \in G_K$ acts trivially on $H_1(U,Y;A)$ if and only if $\sigma \in G_L$. In view of this result, to determine the action of G_K on $H_1(U,Y;A)$, it remains to determine the action of the finite Galois group $\mathrm{Gal}(L/K)$.

(2) We would like to thank the referee for pointing out related work in [Gre81]. Recall that the Jacobian of the Fermat curve X of exponent p is isogenous to $\mathbb{J}=\prod_{a=1}^{p-2} J_a$ where J_a is the Jacobian of the curve $y^p=x^a(1-x)$. Consider the field extension $L_{\mathbb{J}}$ of $\mathbb{Q}$ generated by the points of order p on $\mathbb{J}$. In [Gre81, Theorem 4], Greenberg proves that $L_{\mathbb{J}}$ is the field $K(\{\sqrt[p]{\eta} \mid \eta \in C^+)$ generated over K by the pth roots of the real cyclotomic units. (Note that Lemma 3.3 below implies that $L_{\mathbb{J}} \subset L$.) He remarks that $\mathrm{Gal}(L_{\mathbb{J}}/K) \simeq (\mathbb{Z}/p)^t$ with $t \le (p-3)/2$ and that $t=(p-3)/2$ when p satisfies Vandiver's conjecture.

(3) We would like to thank Sharifi for pointing out similar work in [AI88, Section 2.8], where the authors determine the Galois group of the Galois closure of $\sqrt[p]{1-\sqrt[p]{1-\zeta}}$ over K. That extension is non-abelian over $\mathbb{Q}(\mu_{p^2})$, in contrast with the extension in this paper which is abelian even over K.

3.1. The splitting field of $1-(1-x^p)^p$.

The prime p is totally ramified in K with $p=\langle 1-\zeta\rangle^{p-1}$ [Was97, Lemma 1.4]. Thus there is a unique place $\nu=\langle 1-\zeta\rangle$ above p in K. Also, $p=\prod_{i=1}^{p-1}(1-\zeta^i)$ and $(1-\zeta^i)/(1-\zeta)$ is a unit of $\mathcal{O}_K$ by [Was97, Lemma 1.3]. Thus $\nu=\langle 1-\zeta^i\rangle$ for all $i=1,2,\ldots,p-1$. Since $1=v_\nu(p)=(p-1)v_\nu(1-\zeta)$, it follows that $v_\nu(1-\zeta^i)=1/(p-1)$ for $1\le i\le p-1$.

Let L' be the maximal elementary abelian p-group extension of K unramified except over $\nu=\langle 1-\zeta\rangle$.

Lemma 3.2. *(1)* $L=K(\sqrt[p]{1-\zeta^i}, 1\le i\le p-1)$.

(2) $L\subset L'$ *and* $\mathrm{Gal}(L/K)$ *is an elementary abelian p-group.*

Proof. (1) Let $z = 1 - x^p$ where x is a root of $1-(1-x^p)^p$. The equality $z^p = 1$ implies that $K \subset L$. The $p^2 - p$ non-zero roots of $f_p(x)$ are the pth roots of $1 - \zeta^i$ for $1 \leq i \leq p-1$. Thus $L = K(\sqrt[p]{1-\zeta^i}, 1 \leq i \leq p-1)$.

(2) The field L is the compositum of the fields $K(\sqrt[p]{1-\zeta^i})$. For each i, the extension $K(\sqrt[p]{1-\zeta^i})/K$ is a Galois degree p extension ramified only above $1-\zeta^i$ and ∞. This proves both statements.

□

Lemma 3.3. *The field L is the same as the fields L_2 and L_3 where*

$$L_2 = K(\sqrt[p]{1-\zeta^i}, 1 \leq i \leq \frac{p-1}{2}, \sqrt[p]{p});$$

$$L_3 = K(\sqrt[p]{1-\zeta^i}, 1 \leq i \leq \frac{p-1}{2}, \sqrt[p]{\zeta}).$$

Proof. The idea of the proof is to show $L \subseteq L_3 \subseteq L_2 \subseteq L$.

$L \subseteq L_3$: For $\frac{p-1}{2} < i \leq p-1$, write $j = -i$. Then

$$\sqrt[p]{1-\zeta^j} = \sqrt[p]{1-\zeta^{-i}} = \sqrt[p]{\zeta^{-i}-1} \cdot \sqrt[p]{-1}.$$

Since p is odd, $\sqrt[p]{-1} \in K$. So

$$\sqrt[p]{1-\zeta^j} = \sqrt[p]{\zeta^{-i}(1-\zeta^i)} \cdot \sqrt[p]{-1} = \sqrt[p]{1-\zeta^i} \cdot (\sqrt[p]{\zeta})^{-i} \cdot \sqrt[p]{-1} \in L_3.$$

$L_3 \subseteq L_2$:

Let ζ_{p^2} denote a pth root of ζ. It suffices to show that $\zeta_{p^2} \in L_2$. Write $p = bc$ with

$$b = \prod_{i=1}^{\frac{p-1}{2}} (1-\zeta^i), \ c = \prod_{i=\frac{p+1}{2}}^{p-1} (1-\zeta^i).$$

Note that $(1-\zeta^i)/(1-\zeta^{-i}) = -\zeta^i$. Thus, $\frac{b}{c} = (-1)^{\frac{p-1}{2}} \zeta^{\frac{(p-1)(p+1)}{8}}$ and

$$b^2 = \frac{b}{c} \cdot bc = (-1)^{\frac{p-1}{2}} \zeta^{\frac{(p-1)(p+1)}{8}} \cdot p.$$

Then

$$\zeta^{\frac{(p-1)(p+1)}{8}} = (-1)^{\frac{p-1}{2}} p^{-1} \prod_{i=1}^{\frac{p-1}{2}} (1-\zeta^i)^2.$$

Let $J = (p-1)^2(p+1)/16$ and note that $p \nmid J$. Raising both sides of the previous equation to the power $\frac{p-1}{2}\frac{1}{p}$ shows that

$$\zeta_{p^2}^J = \zeta'(\sqrt[p]{-1})^{\frac{(p-1)^2}{4}} (\sqrt[p]{p})^{\frac{1-p}{2}} \prod_{i=1}^{\frac{p-1}{2}} \left(\sqrt[p]{(1-\zeta^i)^2}\right)^{\frac{p-1}{2}},$$

for some pth root of unity ζ'. Thus $\zeta_{p^2}^J \in L_2$ and $\zeta_{p^2} \in L_2$.

$L_2 \subseteq L$: This follows from the equality $\sqrt[p]{p} = \prod_{i=1}^{p-1} \sqrt[p]{1-\zeta^i}$. □

3.2. Background on units in cyclotomic fields.

Let $K = \mathbb{Q}(\zeta)$ and let $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. Let $E = \mathcal{O}_K^*$ (resp. $E^+ = \mathcal{O}_{K^+}^*$) denote the group of units in $\mathcal{O}_K$ (resp. $\mathcal{O}_{K^+}$). Let V denote the subgroup of K^* generated by $\{\pm\zeta, 1-\zeta^i : i = 1, 2, \ldots, p-1\}$. Let W be the group of roots of unity in K.

Consider the cyclotomic units $C = V \cap \mathcal{O}^*$ of K and the cyclotomic units $C^+ = C \cap (\mathcal{O}^+)^*$ of K^+ [Was97, page 143]. By [Was97, Lemma 8.1], C is generated by ζ and C^+; and C^+ is generated by -1 and the units

$$\epsilon_a = \zeta^{(1-a)/2}(1-\zeta^a)/(1-\zeta),$$

for $1 < a < p/2$. By [Was97, Theorem 4.12], the index of WE^+ in E is 1 or 2. Let h^+ denote the order of the class group of K^+.

Theorem 3.4. [Was97, Theorem 8.2] *The index of the cyclotomic units C^+ in E^+ is the class number h^+ of K^+. Thus if Vandiver's Conjecture is true for the prime p, then E/E^p is generated by C.*

Remark 3.5. Vandiver's Conjecture (first conjectured by Kummer in 1849) states that p does not divide the class number h^+. It has been verified for all p less than 163 million [BH11]. It is also true for all regular primes.

3.3. The Galois group of $1-(1-x^p)^p$.

Proposition 3.6. *If Vandiver's Conjecture is true for the prime p, then the Galois group of L/K is an elementary abelian p-group of rank $(p+1)/2$.*

Proof. By Lemma 3.2, $\mathrm{Gal}(L/K)$ is an elementary abelian p-group. Let r be the integer such that $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/p)^r$. The field L is obtained by adjoining pth roots of elements in some subgroup $B \subset K^*/(K^*)^p$, and by Kummer theory $B \simeq (\mathbb{Z}/p)^r$. By Lemma 3.3, B is generated by ζ and $1-\zeta^i$ for $1 \leq i \leq (p-1)/2$. Thus $r \leq (p+1)/2$. Thus it suffices to show that $r \geq (p+1)/2$.

Note that B is generated by ζ and $1-\zeta^i$ for $1 \leq i \leq (p-1)/2$. Thus B is also generated by ζ, $1-\zeta$, and ϵ_a for $1 < a < p/2$. Consider the subgroup B' of $K^*/(K^*)^p$ generated by ζ and ϵ_a for $1 < a < p/2$. Let r' be the rank of B' over $\mathbb{Z}/p$. Since ζ and ϵ_a are units, and $1-\zeta$ has positive valuation at the prime above p, it suffices to show that $r' \geq (p-1)/2$.

Since -1 is a pth power, B' is also the subgroup generated by the cyclotomic units C. By hypothesis, p satisfies Vandiver's conjecture and so Theorem 3.4 implies that $B' \simeq E/E^p$. By Dirichlet's unit theorem, $E \simeq \mathbb{Z}^{\frac{p-1}{2}-1} \times \mu_p$. Thus $r' = \frac{p-1}{2} - 1 + 1 = (p-1)/2$. □

We now describe an explicit set of generators for $\mathrm{Gal}(L/K)$. Given a primitive pth root $\sqrt[p]{\theta}$ of $\theta \in K$ and $\sigma \in G_K$, recall from Definition 1.2 that $\kappa(\theta)\sigma$ is the element of $\mathbb{Z}/p$ such that

$$\sigma \sqrt[p]{\theta} = \zeta^{\kappa(\theta)\sigma} \sqrt[p]{\theta}.$$

Corollary 3.7. *Let p be an odd prime such that $p \nmid h^+$. Then the following map is an isomorphism:*

$$\Phi = \kappa(\zeta) \times \prod_{i=1}^{\frac{p-1}{2}} \kappa(1-\zeta^{-i}) : \mathrm{Gal}(L/K) \to (\mathbb{Z}/p)^{\frac{p+1}{2}}.$$

Proof. By Lemma 3.3, $L = K(\sqrt[p]{\zeta}, \sqrt[p]{1-\zeta^{-i}} : i = 1, 2, \ldots, \frac{p-1}{2})$. Let $G \subseteq K^*/(K^*)^p$ denote the subgroup generated by $S = \{\zeta, 1-\zeta^{-i} : i = 1, 2, \ldots, \frac{p-1}{2}\}$. By Kummer theory, it suffices to show that S is a $\mathbb{Z}/p$-basis for the $\mathbb{Z}/p$-vector space $\mathrm{Gal}(L/K)$, which follows from Proposition 3.6. □

Remark 3.8. If $p \mid h^+$ then p divides $[E^+ : C^+]$ by [Was97, Theorem 8.2]. Since E^+ does not contain the pth roots of unity, E^+ has no p-torsion, and it follows that there is an element c of C^+ which is a pth power of an element in E^+, but not a pth power of any element of C^+. Since -1 is a pth power and C^+ is generated by -1 and $\{\epsilon_a : 1 < i < p/2\}$, c may be taken to be $c = \prod_{a=2}^{(p-1)/2} \epsilon_a^{e_a}$ with $0 \le e_a \le p-1$. Since B' in the previous proof is generated by C, it follows that B' is generated by $\{\zeta, \epsilon_a : 1 < i < p/2\}$. Since c maps to 0 in E/E^p, this implies that the rank r' of B' is less than the cardinality of $\{\zeta, \epsilon_a : 1 < i < p/2\}$. Thus $r = r' + 1 < (p+1)/2$. Thus if Vandiver's Conjecture is not true for the prime p, then the rank of the elementary abelian p-group $\mathrm{Gal}(L/K)$ is strictly less than $(p+1)/2$.

4. Comparison with an $(n-1)$-torus

Recall the notation from Section 2 that $\tilde{V} = \mathbb{A}^1 - \mu_n$, $V = \tilde{V} \cup \{1\}$, and Z consists of the points 0 and 1 in V. Recall that $\psi \in H_1(V, Z; A)$ denotes the homology class represented by the path from 0 to 1 along the real axis, and that Ψ_σ is defined to be the element of $\Omega(\Lambda_0)/A \,\mathrm{dlog}\, \zeta_0$ determined by $(\sigma - 1)\psi$ and the exact sequence

$$0 \to A \,\mathrm{dlog}\, \zeta_0 \to \Omega(\Lambda_0) \to H_1(V; A) \to 0,$$

where the quotient map $\Omega(\Lambda_0) \to H_1(V; A)$ is the map of Λ_0 modules mapping $\zeta_0 \,\mathrm{dlog}\, \zeta_0$ to a small counterclockwise loop around ζ.

Note that there is a map from V to a torus which induces a Galois equivariant isomorphism on $H_1(-; A)$. For example, this map could be the Abel-Jacobi map to the generalized Jacobian. Furthermore, over K, this torus splits, and it is easy to write down a map to a split torus inducing an isomorphism on $H_1(-; A)$. Namely, the map

$$f : V_K \to (\mathbb{G}_{m,K})^{\times n-1},$$

given by $z \mapsto (z - \zeta, z - \zeta^2, \ldots, z - \zeta^{n-1})$ induces a Galois equivariant isomorphism on $H_1(-; A)$.

In this section, we use the isomorphism $H_1(f; A)$ to compute Ψ_σ in terms of the classical Kummer map, relying on the facts that $H_1((\mathbb{G}_{m,K})^{\times(n-1)}; A) \cong A^{n-1}$ and that the map κ for $\mathbb{G}_m$ can be identified with the classical Kummer map. We will furthermore see in Section 4.2 that this computation is compatible with Section 3.

4.1. **Computation of Ψ_σ.** Fix the isomorphism $I : \Omega(\Lambda_0)/A \,\mathrm{dlog}\, \zeta_0 \to A^{n-1}$ given by

$$\sum_{i=1}^{n-1} a_i \zeta_0^i \,\mathrm{dlog}\, \zeta_0 \mapsto (a_1, a_2, \ldots, a_{n-1}).$$

This isomorphism I can also be obtained by composing the isomorphism described above $\Omega(\Lambda_0)/A \,\mathrm{dlog}\, \zeta_0 \cong H_1(V; A)$ with $H_1(f; A)$ and an obvious isomorphism $H_1((\mathbb{G}_{m,K})^{\times(n-1)}; A) \cong A^{n-1}$.

Proposition 4.1. *With notation as above,*

$$\Psi_\sigma = (\kappa(1 - \zeta^{-1})(\sigma), \ldots, \kappa(1 - \zeta^{-(n-1)})(\sigma)).$$

Proof. Consider the maps $\kappa^{ab}_{V,b} : V(K) \to H^1(G_K, H_1(V))$, defined so that $\kappa^{ab}_{V,b}(x)$ is represented by the cocycle

$$\sigma \mapsto \gamma^{-1}\sigma\gamma$$

where γ is a path from b to x, and composition of paths is written from right to left, so $\gamma^{-1}\sigma\gamma$ is a loop based at b. As in [Wic12, p. 8], the dependency on the choice of basepoint b in V is

$$\kappa_{b'}(x) = \kappa_b(x) - \kappa_b(b'). \tag{4.d}$$

By definition, Ψ_σ is the element of $H_1(V; A)$ determined by $(\sigma - 1)\psi$. Note that $(\sigma - 1)\psi = \kappa^{\mathrm{ab}}_{V,0}(1)(\sigma)$.

Since κ is functorial, one sees that $H_1(f)(\sigma - 1)\psi = \kappa^{\mathrm{ab}}_{T,f(0)}(f(1))(\sigma)$, where T is the torus $T = (\mathbb{G}_{m,K})^{\times(n-1)}$ and f is the map $V_K \to T$ defined above.

Since the geometric fundamental group respects products over algebraically closed fields of characteristic 0 [sga03, XIII Proposition 4.6], the map $\kappa_T = \kappa^{\mathrm{ab}}_T$ for T decomposes as the product of the maps κ for $\mathbb{G}_{m,K}$ which are each given by $\kappa_{\mathbb{G}_{m,K},1}(\theta)(\sigma) = \kappa(\theta)\sigma$ as in Definition 1.2 and Remark 1.3. Thus $\kappa^{\mathrm{ab}}_{T,f(0)}(f(1))(\sigma)$ is identified with $\prod_{i=1}^{n-1} \kappa_{\mathbb{G}_{m,K},-\zeta^i}(1 - \zeta^i)(\sigma)$ when, via the projection maps, $\pi_1(T_{\overline{k}}, 1)$ is identified with $\prod_{i=1}^{n-1} \pi_1(\mathbb{G}_{m,\overline{k}}, 1)$.

Applying (4.d) with $b = 1$, using the fact that κ from Definition 1.2 is a homomorphism, yields that $\prod_{i=1}^{n} \kappa_{\mathbb{G}_{m,K},-\zeta^i}(1 - \zeta^i)(\sigma) = \prod_{i=1}^{n} \kappa(\frac{1-\zeta^i}{-\zeta^i})(\sigma)$. The proposition follows from the above, since $(1 - \zeta^i)/(-\zeta^i) = 1 - \zeta^{-i}$. □

Combining with Theorem 2.6 (c.f. [And87, Theorem 10]), we obtain:

Corollary 4.2. *Modulo a term of the form $\alpha \,\mathrm{dlog}\, \zeta$, with $\alpha \in A^{sh}$,*

$$\mathrm{dlog}(\Gamma_\sigma) = \sum_{i=1}^{n-1} c_i \zeta^i \,\mathrm{dlog}\, \zeta, \text{ with } c_i = \kappa(1 - \zeta^{-i})(\sigma).$$

4.2. Compatibility with Section 3.

Remark 4.3. In computing $\kappa(1-\zeta^{-i})(\sigma)$ for $k = K$, one can restrict to the image $\overline{\sigma} \in \mathrm{Gal}(L/K)$.

Corollary 4.4. *Suppose $n = p$ is a prime satisfying Vandiver's conjecture. With respect to the isomorphism $\Phi : \mathrm{Gal}(L/K) \to A^{\frac{p+1}{2}}$ from Corollary 3.7 and the isomorphism $I : \Omega(\Lambda_0)/A \operatorname{dlog} \zeta_0 \to A^{p-1}$ from Section 4.1, the map*

$$\mathrm{Gal}(L/K) \to \Omega(\Lambda_0)/A \operatorname{dlog} \zeta_0, \ \sigma \mapsto \Psi_\sigma$$

is the explicit A-linear map

$$(c_0, c_1, \ldots, c_{\frac{p-1}{2}}) \mapsto (c_1, c_2, \ldots, c_{\frac{p-1}{2}}, c_{\frac{p-1}{2}} + \tfrac{p-1}{2} c_0, \ldots, c_2 + 2c_0, c_1 + c_0).$$

Proof. By Proposition 4.1, Ψ_σ is computed

$$\Psi_\sigma = (\kappa(1-\zeta^{-1})(\sigma), \ldots, \kappa(1-\zeta^{-(p-1)})(\sigma))$$

with respect to the isomorphism I. For $i = 1, 2, \ldots, \frac{p-1}{2}$, then $\kappa(1-\zeta^{-i})$ is identified with the projection onto c_i, the $(i+1)$st coordinate of $(\mathbb{Z}/p)^{\frac{p+1}{2}} \cong \mathrm{Gal}(L/K)$ via the isomorphism Φ. Recall that $(1-\zeta^i)/(1-\zeta^{-i}) = -\zeta^i$ and -1 is a pth power since p is odd. Thus

$$\kappa(1-\zeta^i) - \kappa(1-\zeta^{-i}) = i\kappa(\zeta) = ic_0.$$

Rearranging terms yields that $\kappa(1-\zeta^{-i}) = \kappa(1-\zeta^i) - ic_0$. Applying this equation when $i = \frac{p-1}{2}+1, \ldots, p-1$ shows that $\kappa(1-\zeta^{-i}) = \kappa(1-\zeta^{-(p-i)}) - ic_0 = c_{p-i} - ic_0$. This implies that $\kappa(1-\zeta^{-i})$ is the projection onto the $(p-i+1)$st coordinate c_{p-i} plus $p-i$ times the projection onto the first coordinate c_0. □

4.3. Coordinate sum of Ψ_σ.

We include the following result for its own interest; it is not needed in the computation of $H_1(U, Y; A)$, $H_1(U; A)$, or $H_1(X; A)$ as Galois modules, and it is not needed in the computations of Section 7. For $\sigma \in \mathrm{Gal}(L/K)$, write $\Psi_\sigma = (c_1, \ldots, c_{p-1})$ as in Corollary 4.4.

Lemma 4.5. *If $\sigma \in G_M$, with $M = \mathbb{Q}(\sqrt[p]{p})$, then $\sum_{i=1}^{p-1} c_i \equiv 0 \bmod p$. More generally, if $M_1 = \mathbb{Q}(\zeta_p, \sqrt[p]{p})$ and if $\tau \in \mathrm{Gal}(M_1, \mathbb{Q}(\zeta_p))$ is such that $\tau(\sqrt[p]{p}) = \zeta_p^j \sqrt[p]{p}$, then $\sum_{i=1}^{p-1} c_i \equiv j \bmod p$.*

Proof. Write $\theta_i = 1 - \zeta_p^{-i}$ and note that $\prod_{i=1}^{p-1} \theta_i = p$. Thus $\prod_{i=1}^{p-1} \sqrt[p]{\theta_i} = \sqrt[p]{p} \in M$ is fixed by $\sigma \in G_M$. So $\prod_{i=1}^{p-1} \sigma(\sqrt[p]{\theta_i}) = \sqrt[p]{p}$. By definition, $\sigma(\sqrt[p]{\theta_i}) = \zeta_p^{\kappa_p(\theta_i)\sigma} \sqrt[p]{\theta_i}$. By Proposition 4.1, $c_i = \kappa_p(\theta_i)\sigma$. Thus,

$$\sqrt[p]{p} = \prod_{i=1}^{p-1} \zeta_p^{c_i} \sqrt[p]{\theta_i} = \zeta_p^{\sum_{i=1}^{p-1} c_i} \sqrt[p]{p}.$$

It follows that $\sum_{i=1}^{p-1} c_i \equiv 0 \bmod p$.

Similarly,

$$\zeta_p^j \sqrt[p]{p} = \tau(\sqrt[p]{p}) = \prod_{i=1}^{p-1} \zeta_p^{c_{i,\tau}} \sqrt[p]{\theta_i} = \zeta_p^{\sum_{i=1}^{p-1} c_{i,\tau}} \sqrt[p]{p},$$

so $\sum_{i=1}^{p-1} c_{i,\tau} \equiv j \bmod p$. □

5. Explicit computation of B_σ

5.1. **Determining B_σ from Ψ_σ.** Recall from Fact 2.4 that Γ_σ is an element of $\bar{\Lambda}_0^\times$, unique modulo the kernel of $d'^{sh}: \bar{\Lambda}_0^\times \to \Lambda_1^\times$, such that

$$d'^{sh}(\Gamma_\sigma) = B_\sigma.$$

Corollary 4.2 determines the coefficients of the logarithmic derivative $\operatorname{dlog} \Gamma_\sigma$; they are the ones appearing in Ψ_σ, and explicitly described in Proposition 4.1.

When n is prime, the kernel of dlog is easy to manage and thus Ψ_σ determines the action of G_K on $H_1(U, Y; A)$ as seen in the next result. This result is implicit in [And87, 10.5].

Proposition 5.1. *Let $n = p$ be a prime. Then Ψ_σ uniquely determines B_σ.*

The following lemmas will be useful for the proof of Proposition 5.1.

Lemma 5.2. *The kernel of* $\operatorname{dlog}: \bar{\Lambda}_0^\times \to \Omega(\bar{\Lambda}_0)$ *consists of elements $x = \sum_{0 \le i < n} a_i \zeta_0^i$ such that $ia_i = 0 \in A$ for all $0 \le i < n$. In particular, when n is prime, the kernel of* dlog *consists of the constant (in ζ_0) invertible polynomials $(A^{sh})^\times \subset \bar{\Lambda}_0^\times$.*

Remark 5.3. On the contrary, when n is not prime, this kernel can be significantly larger. For example, when $n = 6$, it contains elements such as $3\zeta_0^2 + 2\zeta_0^3$.

The following characterization of Γ_σ will be used to pinpoint the exact element in a coset that Γ_σ represents.

Lemma 5.4. *Write $\Gamma_\sigma = \sum_{0 \le i < n} d_i \zeta_0^i$, with $d_i \in A^{sh}$, for an element in $\bar{\Lambda}_0^\times$ which is a d'^{sh}-preimage of B_σ. Then $d_\Sigma := \sum_{0 \le i < n} d_i = 1$.*

Proof. By Fact 2.5, $B_\sigma - 1$ is in the augmentation ideal $(1 - \epsilon_0)(1 - \epsilon_1)\Lambda_1$. Since

$$B_\sigma - 1 = \frac{\left(\sum d_i \zeta_0^i\right)\left(\sum d_i \zeta_1^i\right)}{\left(\sum d_i \zeta_0^i \zeta_1^i\right)} - 1,$$

it lies in the augmentation ideal if and only if the difference

$$\left(\sum d_i \zeta_0^i\right)\left(\sum d_i \zeta_1^i\right) - \left(\sum d_i \zeta_0^i \zeta_1^i\right)$$

does. But the augmentation of the latter is precisely $(d_\Sigma^2 - d_\Sigma) = d_\Sigma(d_\Sigma - 1)$. As Γ_σ is invertible, d_Σ must also be invertible, hence $d_\Sigma = 1$. □

We are now ready to prove Proposition 5.1.

Proof. Consider $\Psi_\sigma = \sum_{0 \le i < n} c_i \zeta_0^i \operatorname{dlog} \zeta_0$, with $c_i \in A^{sh}$. By Fact 2.4, [And87, Theorem 9], B_σ is uniquely determined by Γ_σ in an explicit way, as $B_\sigma = d'^{sh}(\Gamma_\sigma)$. Hence it suffices to show that Γ_σ is determined by Ψ_σ in a way unique modulo the kernel of d'^{sh}.

Corollary 4.2 gives that

$$\operatorname{dlog} \Gamma_\sigma = \alpha \operatorname{dlog} \zeta_0 + \sum_{0 \le i < n} c_i \zeta_0^i \operatorname{dlog} \zeta_0,$$

for some $\alpha \in A^{sh}$. Note that the kernel $\mathrm{Ker}(d'^{sh})$ (cf. Fact 2.4) of $d'^{sh} : \bar{\Lambda}_0^\times \to \bar{\Lambda}_1^\times$ maps under dlog to the kernel $\mathrm{Ker}(d'^{sh}_\Omega)$ of the map

$$d'^{sh}_\Omega : \Omega(\bar{\Lambda}_0) \to \Omega(\bar{\Lambda}_1),$$

which is given by $\mathrm{dlog}(d'^{sh})$, i.e.

$$d'^{sh}_\Omega(\sum a_i\zeta_0^i \,\mathrm{dlog}\,\zeta_0) = \sum a_i\zeta_0^i(1-\zeta_1^i)\,\mathrm{dlog}\,\zeta_0 + \sum a_i\zeta_1^i(1-\zeta_0^i)\,\mathrm{dlog}\,\zeta_1.$$

By [And87, 8.5.1], $\mathrm{Ker}(d'^{sh}_\Omega)$ is precisely $A^{sh}\,\mathrm{dlog}\,\zeta_0$. When n is prime, $\mathrm{dlog} : \mathrm{Ker}(d'^{sh}) \to \mathrm{Ker}(d'^{sh}_\Omega)$ is an isomorphism by [And87, 8.3.1], which determines $\mathrm{Ker}(d'^{sh})$. Hence the ambiguity that α introduces is irrelevant for the computation of B_σ.

The remaining obstruction to reconstructing Γ_σ, and therefore B_σ, is the kernel of $\mathrm{dlog} : \bar{\Lambda}_0^\times \to \Omega(\bar{\Lambda}_0)$.

By Lemma 5.2, when n is prime, the kernel of dlog is $A^{sh} \simeq \bar{\mathbb{F}}_p^\times \subset \Lambda_0^\times$. Suppose a lies in this kernel; this means that $\mathrm{dlog}(a\Gamma_\sigma) = \mathrm{dlog}(\Gamma_\sigma)$. On the other hand, $d'^{sh}(a\Gamma_\sigma) = ad'^{sh}(\Gamma_\sigma) = aB_\sigma$, thus a could introduce an ambiguity.

Nonetheless, this ambiguity can be eliminated using Lemma 5.4, which asserts that the sum of the coefficients of Γ_σ is fixed and equals one. Hence the sum of the coefficients of $a\Gamma_\sigma$, for $a \in \bar{\mathbb{F}}_p^\times$, must be a. By Lemma 5.4, this implies that $a\Gamma_\sigma$ is not a preimage of B_σ unless $a = 1$.

In conclusion, when n is prime, $\mathrm{dlog}\,\Gamma_\sigma$ uniquely determines Γ_σ and therefore B_σ. □

In theory, by Proposition 5.1, the coefficients c_i of Ψ_σ studied in Section 4 uniquely and explicitly determine the coefficients of B_σ, and thus the action of G_K on $H_1(U, Y; A)$. We carry out this computation explicitly when $n = 3$ in the following subsection.

5.2. The case $n = 3$.

Consider the smallest example, i.e., that of $n = 3$. Write

$$\Psi_\sigma = (c_1\zeta_0 + c_2\zeta_0^2)\,\mathrm{dlog}\,\zeta_0,$$

for $c_1, c_2 \in \bar{\mathbb{F}}_p \simeq A^{sh}$. Write

$$\Gamma_\sigma = d_0 + d_1\zeta_0 + d_2\zeta_0^2,$$

with $d_i \in \bar{\mathbb{F}}_p$ such that $d_0 + d_1 + d_2 = 1$. To determine the d_i's in terms of the c_i's, it is easier to work with the nilpotent variable $y = \zeta_0 - 1$ instead of ζ_0 and use the basis $dy = \zeta_0\,\mathrm{dlog}\,\zeta_0$ of $\Omega(\Lambda_0)$.

Indeed, $\Gamma_\sigma = 1 + (d_1 - d_2)y + d_2y^2$, and

$$\Psi_\sigma = (c_1 + c_2 + c_2y)dy.$$

By Fact 2.6, $\mathrm{dlog}\,\Gamma_\sigma$ agrees with Ψ_σ modulo terms in $\bar{\mathbb{F}}_3\,\mathrm{dlog}\,\zeta_0 = \bar{\mathbb{F}}_3(y+1)^2dy$. Therefore, for some $\alpha \in \bar{\mathbb{F}}_3$, one sees that

$$\mathrm{dlog}\,\Gamma_\sigma = \Psi_\sigma + \alpha(y+1)^2dy,$$

which yields the equalities

$$\begin{aligned} d_2 - d_1 &= c + \alpha \\ -d_2 &= (c+\alpha)^2 + c_2 - \alpha \\ 0 &= d_2(c+\alpha) + (c+\alpha)(c_2 - \alpha) + \alpha, \end{aligned}$$

where $c = c_1 + c_2$. In particular, α must be a solution of the polynomial equation

$$\alpha^3 - \alpha + c^3 = 0.$$

For an arbitrary choice of solution α, the coefficients of Γ_σ are

$$\begin{aligned} d_1 &= c_1 - \alpha - (c+\alpha)^2, \\ d_2 &= -c_2 + \alpha - (c+\alpha)^2. \end{aligned}$$

Note that the inverse of Γ_σ expressed in the original ζ_0-basis is

$$\Gamma_\sigma^{-1} = (1 + d_1 + d_2 + (d_2 - d_1)^2) + ((d_2 - d_1)^2 - d_1)\zeta_0 + ((d_2 - d_1)^2 - d_2)\zeta_0^2.$$

In terms of the c's and α, this becomes

$$\Gamma_\sigma^{-1} = (1 + c_1 - c_2 - (c+\alpha)^2) + (c_2 + c - (c+\alpha)^2)\zeta_0 + (c_2 - \alpha - (c+\alpha)^2)\zeta_0^2.$$

Now $B_\sigma = d'^{sh}(\Gamma_\sigma)$ can be computed.

Lemma 5.5. *Suppose* $\Psi_\sigma = (c_1\zeta_0 + c_2\zeta_0^2)\,\mathrm{dlog}\,\zeta_0$*, and let* $b_{i,j}$ *be the coefficient of* $\zeta_0^i\zeta_1^j$ *in* B_σ*. Then*

$$\begin{aligned} b_{0,0} &= 1 + c_2 - c_1 - (c_2 - c_1)^2 \\ b_{0,1} &= c_1 - (c_2 - c_1)^2 \\ b_{1,1} &= -c_1 - (c_2 - c_1)^2. \end{aligned} \tag{5.e}$$

The rest of the coefficients are determined by symmetry $b_{i,j} = b_{j,i}$ *and the fact that* $b_{0,0} + b_{0,1} + b_{0,2} = 1$*,* $b_{1,0} + b_{1,1} + b_{1,2} = 0$*, and* $b_{2,0} + b_{2,1} + b_{2,2} = 0$*.*

Remark 5.6. From the proof of Corollary 4.4, if $i = 1, \ldots, \frac{p-1}{2}$, then $\kappa(1-\zeta^{-i}) = c_{p-i} - ic_0$. By Proposition 4.1, $c_2 = \kappa(1-\zeta^{-2})$. Rearranging terms gives $c_0 = c_2 - c_1$, and it follows that Lemma 5.5 completes the proof of Theorem 1.1.

6. Homology of the affine and projective Fermat curve

In this section, we determine the Galois module structure of the homology of the projective Fermat curve X and its affine open $U = X - Y$ with coefficients in $A = \mathbb{Z}/n$ for all $n \geq 3$.

6.1. **Homology of the affine curve.** We first determine the Galois module structure of $H_1(U)$, where $H_i(U)$ abbreviates $H_i(U; A)$, and more generally, all homology groups will be taken with coefficients in A.

The closed subset $Y \subset U$ given by $xy = 0$ consists of the $2n$ points

$$R_i = [\zeta^i : 0 : 1], \ Q_i = [0 : \zeta^i : 1].$$

Thus, $H_0(Y) \simeq \Lambda_0 \oplus \Lambda_0$ is generated by $\zeta_0 \oplus 0$ and $0 \oplus \zeta_1$. The first copy indexes the points R_i and the second copy indexes the points Q_i. The homomorphism $H_0(Y) \to H_0(U) \simeq A$ sends both $\zeta_0 \oplus 0$ and $0 \oplus \zeta_1$ to 1.

Note that $H_0(Y)$ is an Λ_1-module via $\zeta_0 \mapsto \zeta_0 \oplus 1$ and $\zeta_1 \mapsto 1 \oplus \zeta_1$. The boundary map $\delta : H_1(U,Y) \to H_0(Y)$ is a Λ_1-module map given by

$$\beta \mapsto 1 \oplus 0 - 0 \oplus 1. \tag{6.f}$$

Lemma 6.1. *There is an exact sequence of Galois modules*

$$0 \to H_1(U) \to H_1(U,Y) \xrightarrow{\delta} H_0(Y) \to H_0(U) \to 0. \tag{6.g}$$

The first Betti number of U is $(n-1)^2$.

Proof. This follows from the long exact sequence for relative homology, using the facts that $H_1(Y) = 0$ and $H_0(U,Y) = 0$. The Betti number is the A-rank of $H_1(U)$; note that $H_1(U,Y)$, $H_0(Y)$, and $H_0(U)$ are all free A-modules, hence

$$\mathrm{rank}(H_1(U)) = \mathrm{rank}(H_1(U,Y)) - \mathrm{rank}(H_0(Y)) + \mathrm{rank}(H_0(U)).$$

So, the rank of $H_1(U)$ is $n^2 - 2n + 1 = (n-1)^2$. □

An element $W \in \Lambda_1$ will be written as $W = \sum_{0 \le i,j \le n-1} a_{ij}\zeta_0^i\zeta_1^j$.

Proposition 6.2. *Let $W = \sum_{0 \le i,j \le n-1} a_{ij}\zeta_0^i\zeta_1^j$ be an element of Λ_1, and consider the corresponding element $W\beta$ of $H_1(U,Y)$. Then $W\beta$ restricts to $H_1(U)$ if and only if for each $0 \le j \le n-1$, $\sum_{i=0}^{n-1} a_{ij} = 0$, and for each $0 \le i \le n-1$, $\sum_{j=0}^{n-1} a_{ij} = 0$.*

Proof. By Lemma 6.1, $W\beta \in H_1(U)$ if and only if $W\beta \in \ker(\delta)$. Note that, by (6.f),

$$\delta(\zeta_0\beta) = (\zeta_0 \oplus 1)(1 \oplus 0 - 0 \oplus 1) = \zeta_0 \oplus 0 - 0 \oplus 1,$$

and similarly,

$$\delta(\zeta_1\beta) = (1 \oplus \zeta_1)(1 \oplus 0 - 0 \oplus 1) = 1 \oplus 0 - 0 \oplus \zeta_1.$$

Thus

$$\begin{aligned} \delta(W\beta) &= \sum_{0 \le i,j \le n-1} a_{ij}\delta(\zeta_0^i\zeta_1^j\beta) \\ &= \sum a_{ij}(\zeta_0^i \oplus 1)(1 \oplus \zeta_1^j)(1 \oplus 0 - 0 \oplus 1) \\ &= \sum a_{ij}(\zeta_0^i \oplus 0 - 0 \oplus \zeta_1^j). \end{aligned}$$

So $W\beta \in \ker(\delta)$ if and only if the rows and columns of W sum to zero. □

6.2. **Homology of the projective curve.** We next determine the Galois module structure of $H_1(X)$, which has rank $2g = n^2 - 3n + 2$.

Proposition 6.3. *(1) There is an exact sequence of Galois modules and A-modules:*

$$0 \to H_2(X) \to H_2(X,U) \xrightarrow{D} H_1(U) \to H_1(X) \to 0.$$

(2) The image of D is $\mathrm{Stab}(\zeta_0\zeta_1)$ *where* $\mathrm{Stab}(\zeta_0\zeta_1)$ *consists of $W\beta \in H_1(U)$ which are invariant under $\zeta_0\zeta_1$, i.e., for which $a_{i+1,j+1} = a_{ij}$, where indices are taken modulo n when necessary.*

(3) As a Galois module and A-module, $H_1(X) = H_1(U)/\mathrm{Stab}(\zeta_0\zeta_1)$.

Proof. (1): The long exact sequence in homology of the pair (X, U) implies that the sequence

$$\cdots \to H_2(U) \to H_2(X) \to H_2(X,U) \xrightarrow{D} H_1(U) \to H_1(X) \to H_1(X,U) \to \cdots$$

is exact. Since U is affine, $H_2(U) = 0$. It thus suffices to show $H_1(X, U) = 0$. This follows from the fact that $H_1(X, U)$ is isomorphic as an abelian group to the singular homology of $(X(\mathbb{C}), U(\mathbb{C}))$, where $X(\mathbb{C})$ and $U(\mathbb{C})$ are given the analytic topology.

Here is an alternative proof that $H_1(X, U) = 0$ which does not use the analytic topology and which will be useful for part (2). It follows from [And87, §4 Theorem 1] that Anderson's étale homology with coefficients in A [And87, §2] is naturally isomorphic to the homology of the étale homotopy type in the sense of Friedlander [Fri82]. It follows from Voevodsky's purity theorem [MV99, Theorem 2.23] and the factorization of the étale homotopy type through $\mathbb{A}^1$ algebraic topology [Isa04] that there is a natural isomorphism $H_i(X,U) \cong \tilde{H}_i(\vee_{(X-U)(\overline{K})}\mathbb{P}^1_{\overline{K}})$, where $\tilde{H}_i$ denotes reduced homology. (For this, it is necessary to observe that the proof of [MV99, Theorem 2.23] goes through with the étale topology replacing the Nisnevich topology.) Thus

$$\tilde{H}_i(\mathbb{P}^1_{\overline{K}}; A) = \begin{cases} A(1) & \text{if } i = 2 \\ 0 & \text{otherwise,} \end{cases}$$

where $A(1)$ denotes the module $A = \mathbb{Z}/n$ with action given by the cyclotomic character. Over K, $A(1) = A$. It follows that

$$H_1(X,U) = \tilde{H}_1(\vee_{(X-U)(\overline{K})}\mathbb{P}^1_{\overline{K}}; A) = \oplus_{(X-U)(\overline{K})}\tilde{H}_i(\mathbb{P}^1_{\overline{K}}; A) = 0.$$

As a third alternative, one can see that $H_1(X, U) = 0$ using [Mil80, VI Theorem 5.1] and a universal coefficients argument to change information about cohomology to information about homology.

(2) As above,

$$H_2(X,U) \cong \tilde{H}_1(\vee_{(X-U)(\overline{K})}\mathbb{P}^1_{\overline{K}}) = \oplus_{(X-U)(\overline{K})}\tilde{H}_i(\mathbb{P}^1_{\overline{K}}) = \oplus_{(X-U)(\overline{K})}A(1).$$

For $\eta \in (X - U)(\overline{K})$, let η also represent the corresponding basis element of $\oplus_{(X-U)(\overline{K})}A(1)$. Then $D(\eta)$ is represented by a small loop around η.

Note that the coordinates of η are $[\epsilon : -\epsilon : 0]$ for some nth root of unity ϵ. In particular, η is fixed by $\zeta_0\zeta_1$. The loop $D(\eta)$ is therefore also fixed by $\zeta_0\zeta_1$ because $\zeta_0\zeta_1$ preserves orientation.

Consider the subset $\mathrm{Stab}(\zeta_0\zeta_1)$ of elements of $H_1(U)$ fixed by $\zeta_0\zeta_1$. Then $\mathrm{Stab}(\zeta_0\zeta_1)$ contains the image of D. In fact, $\mathrm{Stab}(\zeta_0\zeta_1) = \mathrm{Image}(D)$. To see this, it suffices to show that both $\mathrm{Stab}(\zeta_0\zeta_1)$ and $\mathrm{Image}(D)$ are isomorphic to A^{n-1}.

By (1), one sees that $\mathrm{Image}(D)$ is isomorphic to the quotient of $H_2(X, U)$ by the image of $H_2(X) \to H_2(X, U)$. Since X is a smooth proper curve, $H_2(X) \cong A(1)$ and $H_2(X, U) \cong \oplus_{(X-U)(\overline{K})}A(1)$. The map $H_2(X) \to H_2(X, U)$ can be described as the map that sends the basis element of $A(1)$ to the diagonal element $\oplus_{(X-U)(\overline{K})}1$. It follows that $\mathrm{Image}(D) \simeq A^{n-1}$ as claimed.

Now ζ_0 and ζ_1 act on $H_1(U,Y)$ via multiplication. Note that these actions have the effect of shifting the columns or rows of W and thus stabilize $H_1(U)$. The stabilizer of $\zeta_0\zeta_1$ is isomorphic to A^{n-1} because an element of the stabilizer is uniquely determined by an arbitrary choice of $a_{01}, a_{02}, \ldots, a_{0n}$.

(3) is immediate from (1) and (2). □

7. Computing Galois cohomology when $p = 3$

In this section, we explicitly compute several cohomology groups when $p = 3$. Let $e = \zeta_0$ and $f = \zeta_1$.

7.1. Computation of B_σ.

Let σ and τ denote the generators of $G = \mathrm{Gal}(L/K) \simeq (\mathbb{Z}/3)^2$ such that

$$\sigma : \sqrt[3]{\zeta} \mapsto \zeta\sqrt[3]{\zeta}, \qquad \tau : \sqrt[3]{\zeta} \mapsto \sqrt[3]{\zeta}$$
$$\sqrt[3]{1-\zeta^{-1}} \mapsto \sqrt[3]{1-\zeta^{-1}} \qquad \sqrt[3]{1-\zeta^{-1}} \mapsto \zeta\sqrt[3]{1-\zeta^{-1}}.$$

The equality $-\zeta(1-\zeta^{-1}) = 1-\zeta$ shows that $(c_1)_\sigma = 0$, $(c_2)_\sigma = 1$ and $(c_1)_\tau = 1$, $(c_2)_\tau = 1$. By Lemma 5.5, this implies that

$$\begin{aligned} B_\sigma &= 1 - (e+f) + (e^2 - ef + f^2) - (e^2 f + ef^2) \\ &= 1 - (e+f)(1-e)(1-f), \\ B_\tau &= 1 + (e+f) - (e^2 + ef + f^2) + e^2 f^2. \end{aligned} \tag{7.h}$$

7.1.1. *The kernel and image of B.* Let $G = \langle \sigma, \tau \rangle$. Consider the map

$$B : \mathbb{F}_3[G] \to \Lambda_1, \ B(\sigma) = B_\sigma.$$

When $p = 3$, the domain and range of B both have dimension 9. Of course, B is not surjective since its image is contained in the 6 dimensional subspace of symmetric elements.

Lemma 7.1. *When $p = 3$, the image of B has dimension 4 and the kernel of B has dimension 5. In particular, $\mathrm{Im}(B)$ consists of symmetric elements whose 2nd and 3rd rows sum to 0, i.e., elements of the form*

$$a_{00}+a_{01}(e+f)+a_{02}(e^2+f^2)+a_{11}ef-(a_{01}+a_{11})(e^2f+ef^2)+(a_{01}+a_{11}-a_{02})e^2f^2;$$

and $\mathrm{Ker}(B)$ is determined by the relations:

$$B_{\tau^2} + B_\tau + B_1 = 0,$$
$$B_{\sigma^2\tau} - B_{\sigma^2} - B_\tau + B_1 = 0,$$
$$B_{\sigma\tau} - B_\sigma - B_\tau + B_1 = 0,$$
$$B_{\sigma^2\tau^2} - B_{\sigma^2} - B_{\tau^2} + B_1 = 0,$$
$$B_{\sigma\tau^2} - B_\sigma - B_{\tau^2} + B_1 = 0.$$

Proof. Magma computation using (7.h). □

7.2. **Cohomology of** $\mathrm{Gal}(L/K)$**.** Since σ has order 3, by [Bro82, Example 1.1.4, Exercise 1.2.2], the projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[\langle\sigma\rangle]$-module is

$$\mathbb{Z}[G] \overset{1-\sigma}{\leftarrow} \mathbb{Z}[G] \overset{1+\sigma+\sigma^2}{\leftarrow} \mathbb{Z}[G] \overset{1-\sigma}{\leftarrow} \cdots$$

where $G = \mathrm{Gal}(L/K) = \langle \sigma, \tau \mid \sigma^3 = \tau^3 = [\sigma,\tau] = 1\rangle \simeq (\mathbb{Z}/3)^2$. By [Bro82, Proposition V.1.1], the total complex associated to the following double complex is a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module:

$$\begin{array}{ccccccc}
\mathbb{Z}[G] & \xleftarrow{1-\sigma} & \mathbb{Z}[G] & \xleftarrow{1+\sigma+\sigma^2} & \mathbb{Z}[G] & \xleftarrow{1-\sigma} & \\
\downarrow{\scriptstyle 1+\tau+\tau^2} & & \downarrow{\scriptstyle 1+\tau+\tau^2} & & \downarrow{\scriptstyle 1+\tau+\tau^2} & & \\
\mathbb{Z}[G] & \xleftarrow{-(1-\sigma)} & \mathbb{Z}[G] & \xleftarrow{-(1+\sigma+\sigma^2)} & \mathbb{Z}[G] & \xleftarrow{1-\sigma} & \\
\downarrow{\scriptstyle 1-\tau} & & \downarrow{\scriptstyle 1-\tau} & & \downarrow{\scriptstyle 1-\tau} & & \\
\mathbb{Z}[G] & \xleftarrow{1-\sigma} & \mathbb{Z}[G] & \xleftarrow{1+\sigma+\sigma^2} & \mathbb{Z}[G] & \xleftarrow{1-\sigma} &
\end{array}$$

Therefore, to compute $H^1(G, M)$, one can compute the cohomology of the complex

$$\begin{array}{ccccc}
 & & & \xrightarrow{1+\sigma+\sigma^2} & M \\
 & \xrightarrow{1-\sigma} & M & \xrightarrow{1-\tau} & \oplus \\
M & & \oplus & \xrightarrow{-(1-\sigma)} & M \\
 & \xrightarrow{1-\tau} & M & & \oplus \\
 & & & \xrightarrow{1+\tau+\tau^2} & M.
\end{array}$$

Given $h \in \mathbb{F}_3[G]$, let $\mathrm{Ann}_M(h) = \{m \in M \mid hm = 0\}$. Let $M = \Lambda_1$.

Lemma 7.2. *Let* $M = \Lambda_1$ *with* $e = \epsilon_0$ *and* $f = \epsilon_1$*.*

(1) $\mathrm{Ann}_M(1+\tau+\tau^2) = M$*.*

(2) $\mathrm{Ann}_M(1+\sigma+\sigma^2) = (1-e, 1-f)$ *consists of all* $m = \sum m_{ij}e^i f^j$ *such that* $\sum m_{ij} = 0$.

(3) $\mathrm{Ann}_M(1-\sigma) = (1+e+e^2, 1+f+f^2)$.

(4) $\mathrm{Ann}_M(1-\tau) = (e-f, 1+f+f^2)$.

Proof. (1) Every $m \in M$ is in the annihilator of $1+\tau+\tau^2$ because $1+B_\tau+B_{\tau^2}$ equals

$$(e+f) - (e^2+ef+f^2) + e^2f^2 + (e+f)^2 + (e^2+ef+f^2)^2 + ef$$
$$+(e+f)(e^2+ef+f^2) - (e+f)e^2f^2 + (e^2+ef+f^2)e^2f^2,$$

which is zero.

(2) Note that $B_\sigma = 1-(e+f)(1-e)(1-f)$, which gives that

$$\begin{aligned} 1+B_\sigma+B_{\sigma^2} &= (e^2-ef+f^2)(1+e+e^2)(1+f+f^2) \\ &= (1+e+e^2)(1+f+f^2). \end{aligned}$$

Note that $(1+B_\sigma+B_{\sigma^2})e^if^j = (1+B_\sigma+B_{\sigma^2})$, so for $m = \sum_{i,j} m_{i,j}e^if^j$,

$$(1+B_\sigma+B_{\sigma^2})m = (1+B_\sigma+B_{\sigma^2})(\sum_{i,j} m_{i,j}).$$

Thus $\mathrm{Ann}_M(1+B_\sigma+B_{\sigma^2})$ consists of $m \in M$ whose entries sum to 0.

(3) Note that $(1-\sigma)m = 0$ if and only if $\sigma m = m$ which in turn simplifies to $(e+f)(1-e)(1-f)m = 0$. Thus $\mathrm{Ann}_M(1-\sigma)$ is generated by the annihilators of $1-e$ and $1-f$ and $e+f$, which are $1+e+e^2$ and $1+f+f^2$ and 0.

(4) A Magma calculation using that $1-B_\tau = -(e+f)+(e^2+f^2)+ef-e^2f^2$.

□

7.3. **Preliminary calculations.** Consider the maps $X : M \to M^2$, $Y : M^2 \to M^3$, and $Z : M^3 \to M^4$. The goal is to compute $\ker(Y)/\operatorname{im}(X)$ and $\ker(Z)/\operatorname{im}(Y)$.

After choosing a basis for M, the maps X, Y, and Z can be written in matrix form. The basis of M chosen here is

$$1, f, f^2, e, ef, ef^2, e^2, e^2f, e^2f^2.$$

By Lemma 7.2, all of the entries of the matrix V for the map $\mathrm{Nm}(\tau) : M \to M$ are 0. All of the entries of the matrix U for the map $\mathrm{Nm}(\sigma) : M \to M$ are 1 since $\mathrm{Nm}(\sigma)$ acts on each element of M by summing its coefficients.

Let S be the matrix for the map $1 - B_\sigma : M \to M$. Let T be the matrix for the map $1 - B_\tau : M \to M$. Here are the matrices S and T:

$$S = \begin{bmatrix} 0 & 1 & 2 & 1 & 1 & 1 & 2 & 1 & 0 \\ 2 & 0 & 1 & 1 & 1 & 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 & 1 & 1 & 1 & 0 & 2 \\ 2 & 1 & 0 & 0 & 1 & 2 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 & 2 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 0 & 2 & 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 2 & 1 & 2 & 0 \end{bmatrix};$$

and

$$T = \begin{bmatrix} 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 & 2 & 1 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 & 0 & 2 & 0 & 2 & 1 \\ 1 & 0 & 2 & 0 & 2 & 1 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 & 0 & 2 & 0 & 2 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 2 & 1 & 0 & 1 & 0 & 2 & 0 & 2 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 & 2 & 1 & 2 & 1 & 0 \end{bmatrix}.$$

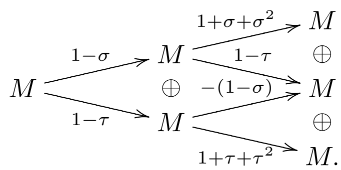
The block matrices for X, Y, and Z are given as follows:

$$X = \begin{bmatrix} S & T \end{bmatrix};$$

$$Y = \begin{bmatrix} U & T & 0 \\ 0 & -S & V = 0 \end{bmatrix};$$

$$Z = \begin{bmatrix} S & T & 0 & 0 \\ 0 & -U & V = 0 & 0 \\ 0 & 0 & S & T \end{bmatrix}.$$

7.4. **Calculation of $H^1(\mathrm{Gal}(L/K), M)$.** The plan is to compute the cohomology of the complex:



Lemma 7.3. *The kernel of $Y : M^2 \to M^3$ has dimension 13 and a basis is:*

$$\begin{aligned}
(f - e^2f^2) &\oplus 0,\\
(e - e^2f^2) &\oplus 0,\\
(1 - e^2f^2) &\oplus (ef - ef^2 - e^2f + e^2f^2),\\
(f^2 - e^2f^2) &\oplus (-ef + ef^2 + e^2f - e^2f^2),\\
(ef - e^2f^2) &\oplus (-ef + ef^2 + e^2f - e^2f^2),\\
(ef^2 - e^2f^2) &\oplus (ef - ef^2 - e^2f + e^2f^2),\\
(e^2 - e^2f^2) &\oplus (-ef + ef^2 + e^2f - e^2f^2),\\
(e^2f - e^2f^2) &\oplus (ef - ef^2 - e^2f + e^2f^2),\\
0 &\oplus (1 - ef - ef^2 - e^2f - e^2f^2),\\
0 &\oplus (f + ef + e^2f),\\
0 &\oplus (f^2 + ef^2 + e^2f^2),\\
0 &\oplus (e + ef + ef^2),\\
0 &\oplus (e^2 + e^2f + e^2f^2).
\end{aligned}$$

Proof. Magma calculation. □

Lemma 7.4. *The image of $X : M \to M^2$ has dimension 4 and a basis is:*

$$\begin{aligned}
(1 - f^2 - e^2 + e^2f^2) &\oplus (1 - f^2 - ef + ef^2 - e^2 + e^2f),\\
(f - f^2 - e^2 + e^2f) &\oplus (1 - f + f^2 - e - ef^2 - e^2 + e^2f^2),\\
(e - ef^2 - e^2 + e^2f^2) &\oplus (f - f^2 + e - ef - e^2 + e^2f^2),\\
(ef - ef^2 - e^2f + e^2f^2) &\oplus (-1 + f + e - ef^2 - e^2f + e^2f^2).
\end{aligned}$$

Proof. Magma calculation. □

Note that the image of X is contained in the kernel of Y.

Proposition 7.5. *The dimension of* $H^1(\mathrm{Gal}(L/K), M)$ *is 9 and a basis is:*

$$\begin{aligned}
(f^2 - e^2) &\oplus 0,\\
(ef^2 - fe^2) &\oplus 0,\\
(e^2 + e^2 f + e^2 f^2) &\oplus 0,\\
(e^2 f - e^2 f^2) &\oplus (ef - ef^2 - e^2 f + e^2 f^2),\\
0 &\oplus (1 - ef - ef^2 - e^2 f - e^2 f^2),\\
0 &\oplus (f + ef + e^2 f),\\
0 &\oplus (f^2 + ef^2 + e^2 f^2),\\
0 &\oplus (e + ef + ef^2),\\
0 &\oplus (e^2 + e^2 f + e^2 f^2).
\end{aligned}$$

Proof. The quotient $H^1(\mathrm{Gal}(L/K), M) = \ker(Y)/\mathrm{im}(X)$ can be computed using the complement function in Magma. □

7.5. **Calculation of** $H^2(\mathrm{Gal}(L/K), M)$**.** In this section, we compute the kernel of $Z : M^3 \to M^4$ modulo the image of $Y : M^2 \to M^3$.

Proposition 7.6. *The dimension of* $H^2(\mathrm{Gal}(L/K), M)$ *is 13 and a basis is:*

$$\begin{array}{rcccl}
(f + ef + e^2 f) & \oplus & 0 & \oplus & 0,\\
(f^2 + ef^2 + e^2 f^2) & \oplus & 0 & \oplus & 0,\\
(e + ef + ef^2) & \oplus & 0 & \oplus & 0,\\
(e^2 + e^2 f + e^2 f^2) & \oplus & 0 & \oplus & 0,\\
0 & \oplus & (f^2 - e^2 f^2) & \oplus & 0,\\
0 & \oplus & (ef^2 - e^2 f^2) & \oplus & 0,\\
0 & \oplus & (e^2 - e^2 f^2) & \oplus & 0,\\
0 & \oplus & (e^2 f - e^2 f^2) & \oplus & 0,\\
0 & \oplus & 0 & \oplus & (1 - ef - ef^2 - e^2 f - e^2 f^2),\\
0 & \oplus & 0 & \oplus & (f + ef + e^2 f),\\
0 & \oplus & 0 & \oplus & (f^2 + ef^2 + e^2 f^2),\\
0 & \oplus & 0 & \oplus & (e + ef + ef^2),\\
0 & \oplus & 0 & \oplus & (e^2 + e^2 f + e^2 f^2).
\end{array}$$

7.6. **First and second cohomology with coefficients in** $H_1(U)$**.** Recall that $V = H_1(U)$ has dimension $(p-1)^2$. If $p = 3$, then V is a 4-dimensional subspace of M and a basis for V is:

$$v_1 = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix};$$

$$v_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{bmatrix};$$

$$v_3 = \begin{bmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{bmatrix};$$

$$v_4 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}.$$

Let X_1, Y_1, and Z_1 be the restriction of X, Y, and Z respectively. Similarly, let $S_1 = 1 - B_\sigma$, $T_1 = 1 - B_\tau$, $U_1 = \mathrm{Nm}(\sigma)$, and $V_1 = \mathrm{Nm}(\tau)$ be the restrictions of S, T, U, and V respectively. Then T_1, U_1, and V_1 are each the 4×4 zero matrix and

$$S_1 = \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \end{bmatrix}.$$

Then

$$X_1 = \begin{bmatrix} S_1 & T_1 = 0 \end{bmatrix};$$

$$Y_1 = \begin{bmatrix} U_1 = 0 & T_1 = 0 & 0 \\ 0 & -S_1 & V_1 = 0 \end{bmatrix};$$

$$Z_1 = \begin{bmatrix} S_1 & T_1 = 0 & 0 & 0 \\ 0 & -U_1 = 0 & V_1 = 0 & 0 \\ 0 & 0 & S_1 & T_1 = 0 \end{bmatrix}.$$

Proposition 7.7. *The dimension of $H^1(G, H_1(U))$ is 6 and a basis is*

$$v_2 \oplus 0, v_3 \oplus 0, v_4 \oplus 0, 0 \oplus (v_1 - v_4), 0 \oplus (v_2 - v_4), 0 \oplus (v_3 - v_4).$$

The dimension of $H^2(G, H_1(U))$ is 9 and a basis is:

$$\begin{array}{rcccl} (v_1 - v_4) & \oplus & 0 & \oplus & 0, \\ (v_2 + v_4) & \oplus & 0 & \oplus & 0, \\ (v_3 + v_4) & \oplus & 0 & \oplus & 0, \\ 0 & \oplus & v_2 & \oplus & 0, \\ 0 & \oplus & v_3 & \oplus & 0, \\ 0 & \oplus & v_4 & \oplus & 0, \\ 0 & \oplus & 0 & \oplus & (v_1 - v_4), \\ 0 & \oplus & 0 & \oplus & (v_2 + v_4), \\ 0 & \oplus & 0 & \oplus & (v_3 + v_4). \end{array}$$

7.7. **First and second cohomology with coefficients in $H_1(U) \wedge H_1(U)$.** The vector space $W = H_1(U) \wedge H_1(U)$ has dimension $\binom{(p-1)^2}{2} = 6$.

Proposition 7.8. *Let $W = H_1(U) \wedge H_1(U)$. Then $H^1(G, W) = W^2$ (with dimension 12) and $H^2(G, W) = W^3$ (with dimension 18).*

Proof. The map $S^\wedge : V \wedge V \to V \wedge V$ induced by $S = (1 - B_\sigma)$ is the exterior square of S_1. One computes that $S^\wedge$ is the 6×6 zero matrix. Similarly the matrices for $T^\wedge$, $U^\wedge$ and $V^\wedge$ are zero. Then $H^1(G, W) = W^2$ since $\mathrm{Im}(X^\wedge) = 0$ and $\mathrm{Ker}(Y) = W^2$. Also $H^2(G, W) = W^3$ since $\mathrm{Im}(Y^\wedge) = 0$ and $\mathrm{Ker}(Z) = W^3$. □

References

[AI88] Greg Anderson and Yasutaka 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 (89f:14023)

[And87] Greg 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)

[BH11] J. P. Buhler and D. Harvey, *Irregular primes to 163 million*, Math. Comp. **80** (2011), no. 276, 2435–2444. MR 2813369 (2012j:11243)

[Bro82] Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York-Berlin, 1982. MR 672956 (83k:20002)

[CNGJ13] Phillippe Cassou-Nogués, Jean Gillibert, and Arnaud Jehanne, *Galois module structure and Jacobians of Fermat curves*, January 2013.

[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)

[CTT98] Robert F. Coleman, Akio Tamagawa, and Pavlos Tzermias, *The cuspidal torsion packet on the Fermat curve*, J. Reine Angew. Math. **496** (1998), 73–81. MR 1605810 (99b:11066)

[Ell00] Jordan Ellenberg, *2-nilpotent quotients of fundamental groups of curves*, Preprint, 2000.

[Fri82] Eric M. Friedlander, *Étale homotopy of simplicial schemes*, Annals of Mathematics Studies, vol. 104, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1982. MR 676809 (84h:55012)

[Gre81] Ralph Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1980/81), no. 3, 345–359. MR 607375 (82j:14036)

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

[Isa04] Daniel C. Isaksen, *Etale realization on the* $\mathbb{A}^1$*-homotopy theory of schemes*, Adv. Math. **184** (2004), no. 1, 37–63. MR 2047848 (2005d:14029)

[McC94] William G. McCallum, *On the method of Coleman and Chabauty*, Math. Ann. **299** (1994), no. 3, 565–596. MR 1282232 (95c:11079)

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR 559531 (81j:14002)

[MV99] Fabien Morel and Vladimir Voevodsky, $\mathbf{A}^1$*-homotopy theory of schemes*, Inst. Hautes Études Sci. Publ. Math. (1999), no. 90, 45–143 (2001). MR 1813224 (2002f:14029)

[sga03] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)]. MR MR2017446 (2004g:14017)

[SW92] Alexander Schmidt and Kay Wingberg, *On the fundamental group of a smooth arithmetic surface*, Math. Nachr. **159** (1992), 19–36. MR 1237099 (94k:14026)

[Tze07] Pavlos Tzermias, *Almost rational torsion points and the cuspidal torsion packet on Fermat quotient curves*, Math. Res. Lett. **14** (2007), no. 1, 99–105. MR 2289623 (2008a:11068)

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)

[Wic12] Kirsten Wickelgren, *3-nilpotent obstructions to* π_1 *sections for* $\mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$, The Arithmetic of Fundamental Groups (PIA 2010) (Berlin Heidelberg) (Jakob Stix, ed.), Contributions in Mathematical and Computational Sciences, vol. 2, Springer-Verlag, 2012, pp. 281–329.

[Zar74] Ju. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Mat. Zametki **15** (1974), 415–419. MR 0354612 (50 #7090)

Purdue University

E-mail address: `davis705@math.purdue.edu`

Colorado State University

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

Max Planck Institute for Mathematics

E-mail address: `vstojanoska@mpim-bonn.mpg.de`

Georgia Institute of Technology

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