Journal of Algebra 554 (2020) 78–105

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Cohomology groups of Fermat curves via ray class fields of cyclotomic fields

Rachel Davis [a], Rachel Pries [b,*]

[a] *University of Wisconsin-Madison, United States of America*
[b] *Colorado State University, United States of America*

ARTICLE INFO

Article history:
Received 31 July 2018
Available online 1 April 2020
Communicated by Kirsten Eisentraeger

MSC:
primary 11D41, 11R18, 11R34, 11R37, 11Y40
secondary 13A50, 14F20, 20D15, 20J06, 55S35

Keywords:
Cyclotomic field
Class field theory
Ray class field
Absolute Galois group
Heisenberg group
Fermat curve
Homology
Galois cohomology
Obstruction
Transgression

ABSTRACT

The absolute Galois group of the cyclotomic field $K = \mathbb{Q}(\zeta_p)$ acts on the étale homology of the Fermat curve X of exponent p. We study a Galois cohomology group which is valuable for measuring an obstruction for K-rational points on X. We analyze a 2-nilpotent extension of K which contains the information needed for measuring this obstruction. We determine a large subquotient of this Galois cohomology group which arises from Heisenberg extensions of K. For $p = 3$, we perform a Magma computation with ray class fields, group cohomology, and Galois cohomology which determines it completely.

* Corresponding author.
E-mail addresses: rachel.davis@wisc.edu (R. Davis), pries@math.colostate.edu (R. Pries).

https://doi.org/10.1016/j.jalgebra.2020.02.030
0021-8693/

Acknowledgments: We would like to thank Vesna Stojanoska and Kirsten Wickelgren, for their help with Lemmas 3.4 and 3.5 and, more generally, for their ideas in developing this project and a wonderful experience collaborating together. We would like to thank Gras and Maire for suggesting Proposition 3.1 and Nguyen-Quang-Do for helpful comments. We would like to thank AIM for support for this project through a Square collaboration grant. Pries was partially supported by NSF grants DMS-15-02227 and DMS-19-01819.

1. Introduction

Let p be an odd prime and let $r = (p-1)/2$. Consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$. Let $Q = \mathrm{Gal}(L/K)$ where L is the splitting field of the polynomial $1 - (1 - x^p)^p$. Then Q is an elementary abelian p-group. For p satisfying Vandiver's conjecture, the rank of Q is $r + 1$ [6, Proposition 3.6].

Let E be the maximal elementary abelian p-group extension of L ramified only over p. The field E is contained in a ray class field of L. Let $G = \mathrm{Gal}(E/K)$. Then, letting $N = \mathrm{Gal}(E/L)$, there is a short exact sequence

$$1 \to N \to G \to Q \to 1. \tag{1}$$

If p is a regular prime, we prove that $\dim_{\mathbb{F}_p}(N) = 1 + p^{r+1}(p-1)/2$ in Proposition 3.1.

There is an element $\omega \in \mathrm{H}^2(\mathrm{Q}, \mathrm{N})$ which classifies the extension (1) and determines the isomorphism class of the group G. After choosing generators for Q and a splitting $s : Q \to G$, then ω is determined by certain elements $a_i, c_{j,k} \in N$ for $0 \le i \le r$ and $0 \le j < k \le r$, see Section 3.4.

Suppose M is a G-module on which N acts trivially. The inflation-restriction exact sequence yields a short exact sequence:

$$0 \to \mathrm{H}^1(\mathrm{Q}, \mathrm{M}) \to \mathrm{H}^1(\mathrm{G}, \mathrm{M}) \to \mathrm{Ker}(\mathrm{d}_2) \to 0, \tag{2}$$

where $d_2 : \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{M})$ is the transgression map, which depends on ω as in [14, 3.7] and [21, 1.6.6, 2.4.3]. In [7, Theorem 6.11], given $\phi \in \mathrm{Hom}(N, M)^Q$, we prove that the class of ϕ is in $\mathrm{Ker}(d_2)$ if and only if the values of ϕ on a_i and $c_{j,k}$ satisfy certain algebraic properties, see Theorem 3.7.

This paper is about the Galois cohomology of the homology of Fermat curves. The Fermat curve X of exponent p is the smooth curve in $\mathbb{P}^2$ with equation $x^p + y^p = z^p$. Let $\mathrm{H}_1(\mathrm{X})$ denote the étale homology of X. Anderson proves that N acts trivially on $\mathrm{H}_1(\mathrm{X}; \mathbb{Z}/\mathrm{p}\mathbb{Z})$, [1, Section 10.5]. In this paper, we study the Galois cohomology group $\mathrm{H}^1(\mathrm{G}, \mathrm{H}_1(\mathrm{X}; \mathbb{Z}/\mathrm{p}\mathbb{Z}))$. More generally, we study $\mathrm{H}^1(\mathrm{G}, \mathrm{M})$ for subquotients M of the relative homology $\mathrm{H}_1(\mathrm{U}, \mathrm{Y}; \mathbb{Z}/\mathrm{p}\mathbb{Z})$ where U is the affine curve $x^p + y^p = 1$ and Y is the set of $2p$ cusps where $xy = 0$. The motivation for studying this Galois cohomology group and $\mathrm{Ker}(d_2)$ is in Section 1.1.

The main theme of the paper is that Galois extensions of the cyclotomic field K determine information about the kernel of the transgression map $\mathrm{Ker}(d_2)$. In Section 3,

under the condition that $\mathrm{Cl}(L)[p]$ is trivial, we analyze how N, G, ω, and $\mathrm{Ker}(d_2)$ are determined from certain ray class field extensions.

Suppose p is an odd prime satisfying Vandiver's Conjecture. The main result of the paper is Theorem 4.18, in which we determine the subspace of $\mathrm{Ker}(d_2)$ arising from Heisenberg extensions of K. In Section 4.7, we calculate the dimension of this subspace for some small p. More generally, in Section 4, we consider natural subextensions $\bar{E}/L$ of E/L, which lead to quotients $\bar{N}$ of N for which we can analyze $\mathrm{H}^1(\bar{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}}$, and thus determine a subspace of $\mathrm{Ker}(d_2)$. In Section 4.2, we determine the subspaces of $\mathrm{Ker}(d_2)$ arising from ray class, cyclotomic, and Kummer extensions of K; the latter two are trivial unless $p = 3$.

In Section 5, when $p = 3$, we perform an extensive MAGMA calculation to determine N, G, ω, and $\mathrm{Ker}(d_2)$; in particular, we determine the dimension of $\mathrm{Ker}(d_2)$ in Corollary 5.7. The results in Sections 3.6, 4.7 and 5 are possible because we have explicit knowledge about the action of $Q = \mathrm{Gal}(L/K)$ on M from [7].

1.1. Motivation

The motivation to study the Galois cohomology group $\mathrm{H}^1(\mathrm{G}, \mathrm{H}_1(\mathrm{X}; \mathbb{Z}/\mathrm{p}\mathbb{Z}))$ arises from the Kummer map. Let $b = [0 : 1 : 0]$ be a base point of X. Let $\pi = \pi_1(X_{\bar{K}}, b)$ denote the geometric étale fundamental group of X based at b. Consider the lower central series:

$$\pi = [\pi]_1 \supseteq [\pi]_2 \supseteq \ldots \supseteq [\pi]_n \supseteq \ldots.$$

Let G_K be the absolute Galois group of K. For a K-rational point η of X, let γ be a path in $X(\mathbb{C})$ from b to η. The Kummer map

$$\kappa : X(K) \to \mathrm{H}^1(\mathrm{G_K}, \pi_1(\mathrm{X})) \tag{3}$$

is defined by $\kappa(\eta) = [\sigma \mapsto \gamma^{-1}\sigma(\gamma)]$ for $\sigma \in G_K$.

The étale homology $\mathrm{H}_1(\mathrm{X}) = \pi/[\pi]_2$ is the maximal abelian quotient of π. From (3), we obtain a map $\kappa : X(K) \to \mathrm{H}^1(\mathrm{G_K}, \mathrm{H}_1(\mathrm{X}) \otimes \mathbb{Z}_\mathrm{p})$, which is injective. Let $G_{K,S}$ be the Galois group of the maximal pro-p extension of K ramified only over $S = \{\nu\}$ where $\nu = \langle 1 - \zeta_p \rangle$. Since the Fermat curve X has good reduction away from p and K has no infinite primes, κ factors through $\kappa : X(K) \to \mathrm{H}^1(\mathrm{G_{K,S}}, \mathrm{H}_1(\mathrm{X}) \otimes \mathbb{Z}_\mathrm{p})$.

Using work of Schmidt and Wingberg [23], Ellenberg [8] defines a series of obstructions to a K-rational point of the Jacobian of X lying in the image of the Abel-Jacobi map. Namely, via the Kummer map, $X(K)$ and $\mathrm{Jac}(X)(K)$ can be viewed as subsets of $\mathrm{H}^1(\mathrm{G_{K,S}}, \mathrm{H}_1(\mathrm{X}) \otimes \mathbb{Z}_\mathrm{p})$. Let δ_2 denote the first of these obstructions; it was also studied by Zarkhin [28]. By [23, Proposition 3.2], the map δ_2 also factors through $G_{K,S}$ and has the form

$$\delta_2 : \mathrm{H}^1(\mathrm{G_{K,S}}, \mathrm{H}_1(\mathrm{X}) \otimes \mathbb{Z}_\mathrm{p}) \to \mathrm{H}^2(\mathrm{G_{K,S}}, ([\pi]_2/[\pi]_3) \otimes \mathbb{Z}_\mathrm{p}); \tag{4}$$

it is the coboundary map associated to the p-part of the exact sequence

$$1 \to [\pi]_2/[\pi]_3 \to \pi/[\pi]_3 \to \pi/[\pi]_2 \to 1.$$

Thus, a complete understanding of $\mathrm{H}^1(\mathrm{G_{K,S}}, \mathrm{H_1(X)} \otimes \mathbb{Z}_\mathrm{p})$, together with the map δ_2, provides important information about K-rational points on X. In this paper, by taking the homology with coefficients in $\mathbb{Z}/p\mathbb{Z}$, we consider the "first level" of the cohomology. In Section 2.7, we show that we can replace $G_{K,S}$ by G for this first level and we use a spectral sequence to produce the exact sequence (2).

The goal of this paper is to analyze the quotient $\mathrm{Ker}(d_2)$ of $\mathrm{H}^1(\mathrm{G}, \mathrm{H_1(X; \mathbb{Z}/p\mathbb{Z})})$. This material will be needed in future work, where we analyze the kernel $\mathrm{H}^1(\mathrm{Q}, \mathrm{M})$ of (2) and compute the obstruction map δ_2.

2. Background

2.1. Field theory

Let p be an odd prime and let $r = (p-1)/2$. Let ζ_p be a primitive pth root of unity. Let $K = \mathbb{Q}(\zeta_p)$. By [27, Lemmas 1.3, 1.4], K is ramified only above p and $\langle p \rangle = \nu^{p-1}$ where $\nu = \langle 1 - \zeta_p \rangle$ is the unique prime above p; also $\nu = \langle 1 - \zeta_p^i \rangle$ for $1 \le i \le p-1$.

Let L be the splitting field of $1 - (1-x^p)^p$. Note that $\zeta_p \in L$. Also L contains the pth roots of $t_0 = \zeta_p$ and $t_i = 1 - \zeta_p^{-i}$ for $1 \le i \le r$. Let $K_0 = K(\zeta_{p^2})$ and $K_i = K(\sqrt[p]{t_i})$. By [6, Lemma 3.3], L is the compositum of K_0 and K_i for $1 \le i \le r$. By [6, Lemma 3.3], L/K is only ramified at ν. So L is contained in the maximal elementary abelian p-extension of K ramified only over the prime above p.

2.2. Galois groups

Let $Q = \mathrm{Gal}(L/K)$. We assume throughout that p satisfies Vandiver's Conjecture, namely that p does not divide the order h^+ of the class group of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$; this is true for all p less than 163 million and all regular primes. By [6, Proposition 3.6], this implies that $K_0, \ldots, K_r$ are linearly disjoint over K and so $Q \simeq (\mathbb{Z}/p\mathbb{Z})^{r+1}$, where $r = (p-1)/2$. In particular, the degree $d = \deg(L/\mathbb{Q})$ satisfies $d = (p-1)p^{r+1}$.

Note that $Q \simeq \times_{i=0}^{r} \mathrm{Gal}(K_i/K)$. We choose an explicit basis $\{\tau_0, \ldots, \tau_r\}$ for Q as follows. For $0 \le i \le r$, let $\tau_i \in Q$ be such that $\tau_i(\sqrt[p]{t_i}) = \zeta_p \sqrt[p]{t_i}$ and $\tau_i(\sqrt[p]{t_j}) = \sqrt[p]{t_j}$ for $i \ne j$. Let τ_i also denote the image of τ_i in $\mathrm{Gal}(K_i/K)$.

Let G_K (resp. G_L) denote the absolute Galois group of K (resp. L).

2.3. A 2-nilpotent extension of K

Let E be the maximal elementary abelian p-group extension of L which is ramified only above p. Then E/K is Galois. Let $N = \mathrm{Gal}(E/L)$ and $G = \mathrm{Gal}(E/K)$. By definition, N

is an elementary abelian p-group. As in (1), there is a short exact sequence $1 \to N \to G \to Q \to 1$.

2.4. Class groups

Let $\mathrm{Cl}(L)$ denote the class group of L. Let $\mathrm{Cl}^S(L)$ be the quotient of $\mathrm{Cl}(L)$ by the subgroup of classes of ideals generated by the primes of a set S. Let $\mathrm{Cl}(L)[p]$ and $\mathrm{Cl}^S(L)[p]$ denote the p-Sylow subgroups of these.

For a number field F, let $r_2(F)$ denote the number of complex places of F. Let $G_{F,p}$ be the Galois group of the maximal pro-p extension of F ramified only above the primes above p, see [14, Section 11.1]. Since L is totally complex, $r_2(L) = d/2$. This implies that no infinite places are ramified in finite extensions of L and that restricted and ordinary class groups are equal.

There is a short exact sequence

$$1 \to G_{L,p} \to G_{K,p} \to Q \to 1. \tag{5}$$

For a finitely generated p-group Γ, let $\Phi(\Gamma)$ denote its Frattini subgroup, namely the closed characteristic subgroup of Γ topologically generated by pth powers and commutators. We write $\Phi(\Gamma) = \Gamma^p[\Gamma, \Gamma]$. The Frattini quotient $\Gamma' = \Gamma/\Phi(\Gamma)$ is an elementary abelian p-group. By Burnside's basis theorem, $\dim_{\mathbb{F}_p}(\Gamma') = \dim_{\mathbb{F}_p}(\Gamma)$.

By definition, N is the Frattini quotient $G'_{L,p}$ of $G_{L,p}$. The group G is the pushout of $G_{K,p}$ and N with respect to the inclusion $G_{L,p} \to G_{K,p}$ and the quotient map $G_{L,p} \to N$.

2.5. The Fermat curve

The Fermat curve of exponent p is the smooth projective curve $X \subset \mathbb{P}^2$ given by the equation $x^p + y^p = z^p$. The open affine $U \subset X$ given by $z \neq 0$ has affine equation $x^p + y^p = 1$. Let $Y \subset U$ denote the closed subscheme of $2p$ points with $xy = 0$.

The curve X has good reduction away from p. Thus U/K has good reduction except at ν.

The group $\mu_p \times \mu_p$ acts on X, and this action stabilizes U and Y. Let ϵ_0, ϵ_1 be the generators of $\mu_p \times \mu_p$ which act by $\epsilon_0(x, y) = (\zeta_p x, y)$ and $\epsilon_1(x, y) = (x, \zeta_p y)$. Consider the group ring $\Lambda_1 = (\mathbb{Z}/p\mathbb{Z})[\mu_p \times \mu_p]$.

Let $y_i = \epsilon_i - 1$. Then $y_i^p = 0$ and $\Lambda_1 \simeq (\mathbb{Z}/p\mathbb{Z})[y_0, y_1]/\langle y_0^p, y_1^p \rangle$. Consider the augmentation ideal $\langle (1 - \epsilon_0)(1 - \epsilon_1) \rangle = \langle y_0 y_1 \rangle$ of Λ_1.

2.6. Homology

We consider étale homology groups with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Let $M = \mathrm{H}_1(\mathrm{U}, \mathrm{Y}) = \mathrm{H}_1(\mathrm{U}, \mathrm{Y}; \mathbb{Z}/p\mathbb{Z})$ denote the homology of U relative to Y.

By [1, Theorem 6], M is a free rank one Λ_1-module, with generator denoted β. Under the identification of M with Λ_1, the homology $\mathrm{H}_1(\mathrm{U}) = \mathrm{H}_1(\mathrm{U}; \mathbb{Z}/p\mathbb{Z})$ identifies with the augmentation ideal $\langle y_0 y_1 \rangle \subset \Lambda_1$ [6, Proposition 6.2]. Furthermore, $\mathrm{H}_1(\mathrm{X}) = \mathrm{H}_1(\mathrm{X}; \mathbb{Z}/\mathrm{p}\mathbb{Z})$ is the quotient of $\mathrm{H}_1(\mathrm{U})$ by $\mathrm{Stab}(\epsilon_0 \epsilon_1)$ [6, Proposition 6.3].

In addition, M is a p-torsion G_K-module. By [1, Section 10.5], the action of G_K on M factors through L. This implies that G_L and N act trivially on M. This means that the action of G_K on M is determined by the action of $Q = \mathrm{Gal}(L/K)$ on M. Write β for the chosen generator of M and let $B_i = B_{\tau_i} \in \Lambda_1$ denote the element such that $\tau_i \cdot \beta = B_i \beta$. By [1, 9.6, 10.5.2], $B_i - 1 \in \langle y_0 y_1 \rangle$.

2.7. The transgression map

Let M be a p-torsion $G_{K,p}$-module. From (5) and the Lyndon-Hochschild-Serre spectral sequence

$$\mathrm{H}^{\mathrm{i}}(\mathrm{Q}, \mathrm{H}^{\mathrm{j}}(\mathrm{G}_{\mathrm{L,p}}, \mathrm{M})) \Rightarrow \mathrm{H}^{\mathrm{i+j}}(\mathrm{G}_{\mathrm{K,p}}, \mathrm{M}),$$

we obtain the exact sequence

$$0 \to \mathrm{H}^1(\mathrm{Q}, \mathrm{M}^{\mathrm{G_{L,p}}}) \to \mathrm{H}^1(\mathrm{G}_{\mathrm{K,p}}, \mathrm{M}) \to \mathrm{H}^1(\mathrm{G}_{\mathrm{L,p}}, \mathrm{M})^{\mathrm{Q}} \xrightarrow{\mathrm{d_2}} \mathrm{H}^2(\mathrm{Q}, \mathrm{M}^{\mathrm{G_{L,p}}}). \tag{6}$$

Here d_2 is called the transgression map. Suppose $G_{L,p}$ acts trivially on M, then $\mathrm{H}^{\mathrm{i}}(\mathrm{Q}, \mathrm{M}^{\mathrm{G_{L,p}}}) = \mathrm{H}^{\mathrm{i}}(\mathrm{Q}, \mathrm{M})$ for $i = 1, 2$.

Since N is the Frattini quotient of $G_{L,p}$ and since M is a finite dimensional vector space over $\mathbb{F}_p$, there is an isomorphism $\mathrm{H}^1(\mathrm{G}_{\mathrm{L,p}}, \mathrm{M})^{\mathrm{Q}} \simeq \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}}$. Since G is a quotient of $G_{K,p}$, there is an injection $\mathrm{H}^1(\mathrm{G}, \mathrm{M}) \to \mathrm{H}^1(\mathrm{G}_{\mathrm{K,p}}, \mathrm{M})$. By the short five lemma, $\mathrm{H}^1(\mathrm{G}_{\mathrm{K,p}}, \mathrm{M}) \simeq \mathrm{H}^1(\mathrm{G}, \mathrm{M})$. With some abuse of notation, we write $d_2 : \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{M})$. Then there is an exact sequence, as in (2),

$$0 \to \mathrm{H}^1(\mathrm{Q}, \mathrm{M}) \to \mathrm{H}^1(\mathrm{G}, \mathrm{M}) \to \mathrm{Ker}(\mathrm{d_2}) \to 0.$$

Since N acts trivially on M, an element $\phi \in \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}}$ is uniquely determined by a Q-invariant homomorphism $\phi : N \to M$. To compute d_2, we consider a 2-cocycle $\tilde{\omega} : Q \times Q \to N$ for the element $\omega \in \mathrm{H}^2(\mathrm{Q}, \mathrm{N})$ classifying the extension (1). By [21, 1.6.6, 2.4.3] and [14, 3.7 (3.9) and (3.10)] (see [7, Proposition 6.1]), $d_2(\phi) = -\phi \circ \tilde{\omega}$.

3. Ray class fields and the classifying element

Suppose that p is an odd prime satisfying Vandiver's Conjecture. From Sections 2.1 and 2.2, recall that $K = \mathbb{Q}(\zeta_p)$, L is the splitting field of the polynomial $1 - (1 - x^p)^p$, and $Q = \mathrm{Gal}(L/K)$ is an elementary abelian p-group of rank $r + 1$, where $r = (p-1)/2$.

From Section 2.3, E is the maximal elementary abelian p-group extension of L, ramified only above p. Let $G = \mathrm{Gal}(E/K)$ and $N = \mathrm{Gal}(E/L)$. There is an exact sequence:

$$1 \to N \to G \to Q \to 1. \tag{7}$$

In Sections 3.1, 3.2, and 3.3, under the condition that p is regular, we use class field theory to give results on N and its connection with ray class fields. Section 3.4 contains the material needed to classify the extension (7). If M is a G-module on which N acts trivially, in Section 3.5, we give an algebraic description of the kernel of the transgression map $d_2 : \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{M})$. We specialize this to the case that M is the relative homology of the Fermat curve in Section 3.6.

3.1. The rank of N when p is regular

Using the topic of p-rationality, we determine more information about L and N when p is a regular prime. A good reference for p-rationality is [18] or [10, IV, Section 3]. A number field M is p-rational when $G_{M,p}$ is a free pro-p group of rank $1 + r_2(M)$. See other equivalent definitions in [10, IV, Remark 3.4.5, Theorem 3.5].

Proposition 3.1. *If p is a regular prime, then L is p-rational and $\dim_{\mathbb{F}_p}(N) = 1 + d/2$. Also, there is a unique prime $\mathfrak{p}$ of L above p and $\mathrm{Cl}^{\{p\}}(L)[p]$ is trivial.*

(Recall that $\mathrm{Cl}^{\{p\}}(L)[p]$ is the p-Sylow subgroup of the quotient $\mathrm{Cl}^{\{p\}}(L)$ of $\mathrm{Cl}(L)$ by the subgroup of classes of ideals generated by $\mathfrak{p}$.)

Proof. If p is a regular prime, then K is p-rational by [17, Proposition 3, Example page 166]. Since L/K is a Galois p-extension unramified outside p, L/K is p-primitively ramified, e.g., [9, page 330]. Then L is p-rational by [17, Theorem 3]. Since L is p-rational, then $G_{L,p}$ is a free pro-p group of rank $1 + r_2(L)$ where $r_2(L) = d/2$. Thus $N \simeq (\mathbb{Z}/p\mathbb{Z})^{1+d/2}$. The other claims follow from [17, Proposition 3] or [13, Theorem 4.1(iva)]. □

We remark that it might be possible to extend the results to the case that p satisfies Vandiver's conjecture, using the techniques of [11,12].

3.2. Local and global units

Let $\mathcal{O}_L$ denote the maximal order of L. Let $\mathcal{O}_L^\times/p = \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p$ denote the global units modulo p. By Proposition 3.1, if p is a regular prime, then there is a unique prime $\mathfrak{p}$ of L above p.

Corollary 3.2. *If p is a regular prime, then the p-rank of $(\mathcal{O}_L/\mathfrak{p}^{n+1})^\times$ is $d+1$ if $n \geq p^{r+2}$.*

Proof. Let e (resp. f) denote the ramification index (resp. residue degree) of $\mathfrak{p}$ over $\mathbb{Q}$. Set $e_1 = \lfloor e/(p-1) \rfloor$. By [19, Theorem 1, page 45] or [24, Theorem 1, page 31], since

$\zeta_p \in L$, the p-rank of $(\mathcal{O}_L/\mathfrak{p}^{n+1})^\times$ is $ef+1$ if $n \geq e+e_1$. The result follows since $e = d = (p-1)p^{r+1}$, $f = 1$, and $e_1 = p^{r+1}$. □

Let $\mathcal{O}_\mathfrak{p}^\times/p = \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^p$ denote the local units modulo p. Both $\mathcal{O}_L^\times/p$ and $\mathcal{O}_\mathfrak{p}^\times/p$ are $\mathbb{F}_p$-vector spaces with an action of $Q = \mathrm{Gal}(L/K)$. Let $*$ denote the dual.

Proposition 3.3. *If* $\mathrm{Cl}(L)[p]$ *is trivial, then there is a* Q*-invariant short exact sequence:*

$$0 \to \mathrm{H}^1(\mathrm{N}, \mathbb{F}_\mathrm{p}) \to (\mathcal{O}_\mathfrak{p}^\times/\mathrm{p})^* \xrightarrow{\varphi_2^*} (\mathcal{O}_\mathrm{L}^\times/\mathrm{p})^* \to 1. \tag{8}$$

Proof. The hypothesis that $\mathrm{Cl}(L)[p]$ is trivial implies that p is a regular prime. Let φ_2^* be the dual to the homomorphism $\varphi_2 : \mathcal{O}_L^\times/p \to \mathcal{O}_\mathfrak{p}^\times/p$ induced from the inclusion $\mathcal{O}_L \to \mathcal{O}_\mathfrak{p}$. By [14, pages 114-115, Theorem 11.7], there is a Q-invariant exact sequence

$$0 \to \mathrm{H}^2(\mathrm{Cl(L)[p]}, \mathbb{F}_\mathrm{p}) \xrightarrow{\inf} \mathrm{H}^1(\mathrm{G_{L,p}}, \mathbb{F}_\mathrm{p}) \to (\mathcal{O}_\mathfrak{p}^\times/\mathrm{p})^* \xrightarrow{\varphi_2^*} \mathcal{O}_\mathrm{L}^\times/\mathrm{p} \to \mathrm{B}_\mathfrak{p} \to 0.$$

Since $\mathrm{Cl}(L)[p]$ is trivial, $\mathrm{H}^2(\mathrm{Cl(L)[p]}, \mathbb{F}_\mathrm{p}) = 0$. Also, $\mathrm{H}^1(\mathrm{G_{L,p}}, \mathbb{F}_\mathrm{p}) \simeq \mathrm{H}^1(\mathrm{N}, \mathbb{F}_\mathrm{p})$. By [14, page 120], $\dim_{\mathbb{F}_p}(\mathcal{O}_L^\times/p) = d/2$ and $\dim_{\mathbb{F}_p}(\mathcal{O}_\mathfrak{p}^\times/p) = d+1$. By Proposition 3.1, $\dim_{\mathbb{F}_p}(N) = 1 + d/2$. The result follows since $B_\mathfrak{p}$ is trivial by a dimension count. □

3.3. Ray class fields

Let $L_\mathbf{m}$ (resp. $\mathrm{Cl}_\mathbf{m}(L)$) denote the ray class field (resp. group) of L of modulus $\mathbf{m}$. Every extension of L has a conductor, a minimal admissible modulus, which is only divisible by the ramified primes. Thus the field E is contained in the ray class field $L_{\mathfrak{p}^i}$, for i sufficiently large. Since L is totally complex, the narrow ray class group is the same as the ray class group, e.g., [20, page 368]. Let $(\mathcal{O}_L/\mathbf{m})^\times$ denote the units mod $\mathbf{m}$ of L.

Lemma 3.4. *If* $\mathrm{Cl}(L)[p]$ *is trivial, then the* p*-ranks of* $\mathrm{Cl}_{\mathfrak{p}^i}(L)$ *and* $(\mathcal{O}_L/\mathfrak{p}^i)^\times$ *stabilize at the same index* i*.*

Proof. Consider the exact sequence [5, 3.2.3]:

$$U(L)[p] \xrightarrow{\mathrm{Ho_m}} (\mathcal{O}_L/\mathbf{m})^\times[p] \xrightarrow{\psi} \mathrm{Cl}_\mathbf{m}(L)[p] \xrightarrow{\phi} \mathrm{Cl}(L)[p] \to 0. \tag{9}$$

If $\mathrm{Cl}(L)[p]$ is trivial, then $\mathrm{Cl}_\mathbf{m}(L)[p] = (\mathcal{O}_L/\mathbf{m})^\times[p]/(\mathrm{Ho_m(U(L)[p])}$ by (9). Consider (9) for the moduli $\mathbf{m} = \mathfrak{p}^i$ and $\mathfrak{p}^{i+1}$. There is a commutative diagram

$$\begin{array}{ccc} U(L)[p] & \xrightarrow{\mathrm{Ho}_{\mathfrak{p}^{i+1}}} & (\mathcal{O}_L/\mathfrak{p}^{i+1})^\times[p] \\ \| & & \downarrow \\ U(L)[p] & \xrightarrow{\mathrm{Ho}_{\mathfrak{p}^i}} & (\mathcal{O}_L/\mathfrak{p}^i)^\times[p]. \end{array}$$

Consider the surjection of the Frattini quotients $(\mathcal{O}_L/\mathfrak{p}^{i+1})^\times[p]' \to (\mathcal{O}_L/\mathfrak{p}^i)^\times[p]'$. The p-rank of $(\mathcal{O}_L/\mathfrak{p}^i)^\times$ stabilizes at index i if and only if i is the first value such that this surjection is an isomorphism. This is equivalent to the equality $\dim_{\mathbb{F}_p}(\mathrm{Im}(\rho_{\mathfrak{p}^{i+1}})) = \dim_{\mathbb{F}_p}(\mathrm{Im}(\rho_{\mathfrak{p}^i}))$ or the fact that the p-rank of $\mathrm{Cl}_{\mathfrak{p}^i}(L)[p]$ stabilizes at index i. □

3.4. Classifying the extension

Let $N = \mathrm{Gal}(E/L)$, $G = \mathrm{Gal}(E/K)$, and $Q = \mathrm{Gal}(L/K)$. Let ω be the element of $\mathrm{H}^2(\mathrm{Q},\mathrm{N})$ classifying (7) $1 \to N \to G \to Q \to 1$. Since Q and N are both elementary abelian p-groups, the structure of $\mathrm{H}^2(\mathrm{Q},\mathrm{N})$ can be computed abstractly. However, the precise identification of $\omega \in \mathrm{H}^2(\mathrm{Q},\mathrm{N})$ depends intrinsically on the structure of G.

For example, by Lemma 4.14, G surjects onto a Heisenberg group. Then (7) is not split because the short exact sequence for the Heisenberg group has no splitting. This implies that ω is non-trivial (i.e., G is not a semi-direct product).

Consider a section $s : Q \to G$ of the extension (7). Without loss of generality, we assume that $s(1) = 1$ and

$$s(\tau_0^{e_0} \cdots \tau_r^{e_r}) = s(\tau_0)^{e_0} \cdots s(\tau_r)^{e_r}, \text{ for } 0 \le e_i \le p-1. \tag{10}$$

Then there is a 2-cocycle $\tilde{\omega} : Q \times Q \to N$ defined with the formula

$$\tilde{\omega}(q_1, q_2) = s(q_1)s(q_2)s(q_1q_2)^{-1}.$$

The class of $\tilde{\omega}$ in $\mathrm{H}^2(\mathrm{Q},\mathrm{N})$ is ω; in particular, it does not depend on the choice of s.

Consider the generators τ_i with $0 \le i \le r$ for $Q \simeq (\mathbb{Z}/p\mathbb{Z})^{r+1}$ from Section 2.2. For $0 \le i \le r$, define elements a_i by

$$a_i = s(\tau_i)^p, \tag{11}$$

and for $0 \le j < k \le r$, define $c_{j,k}$ by

$$c_{j,k} = [s(\tau_k), s(\tau_j)] = s(\tau_k)s(\tau_j)s(\tau_k)^{-1}s(\tau_j)^{-1}. \tag{12}$$

Note that $a_i, c_{j,k} \in N$ since their images in Q are trivial. These values provide a useful way to classify the extension (7) and play a key role in our analysis of $\mathrm{Ker}(d_2)$, see Theorem 3.7.

The difficulty is that not every section s satisfies (10). Thus, following [3, IV, §3], suppose $\omega' : Q \times Q \to N$ is another 2-cocycle representing the class $\omega \in \mathrm{H}^2(\mathrm{Q},\mathrm{N})$. We may choose ω' such that $\omega'(q,1) = \omega'(1,q) = 1$ for all $q \in Q$. By [3, page 92], ω' determines a unique extension as in (7), together with a section $t : Q \to G$ such that $t(1) = 1$. By [3, IV §3 (3.3)], the correspondence between t and ω' is described by

$$\omega'(q_1, q_2) = t(q_1)t(q_2)t(q_1q_2)^{-1}. \tag{13}$$

This yields the following description of $G = \mathrm{Gal}(E/K)$ as an abstract group: the elements of G are in bijection with $N \times Q$; this bijection takes (n, q) to $nt(q)$. The group law is:

$$(n_1, q_1)(n_2, q_2) = (n_1(q_1 n_2)\omega(q_1, q_2), q_1 q_2).$$

The section t for ω might not satisfy the conditions in (10). To fix this, we set $s(\tau_i) = t(\sigma) = 0 \times \tau_i$ and extend s to a set-theoretic section $s : Q \to G$ using (10). Next, we show that the values of $a_i = s(\tau_i)^p$ and $c_{j,k} = [s(\tau_k), s(\tau_j)]$ can be computed from ω'.

Lemma 3.5. *With notation as above:*

$$a_i = \sum_{\ell=1}^{p-1} \omega'(\tau_i^\ell, \tau_i) \text{ and } c_{j,k} = \omega'(\tau_k, \tau_j) - \omega'(\tau_j, \tau_k).$$

Proof. First, by (13), $\omega'(\tau_i^\ell, \tau_i) = t(\tau_i^\ell)t(\tau_i)t(\tau_i^{\ell+1})^{-1}$. Taking the telescoping product yields

$$\omega'(\tau_i, \tau_i)\omega'(\tau_i^2, \tau_i) \cdots \omega'(\tau_i^{p-1}, \tau_i) = t(\tau_i)^p. \tag{14}$$

Second, by (13),

$$\omega'(\tau_k, \tau_j) = t(\tau_k)t(\tau_j)t(\tau_k\tau_j)^{-1}. \tag{15}$$

By (13), $\omega'(\tau_j, \tau_k) = t(\tau_j)t(\tau_k)t(\tau_j\tau_k)^{-1}$. Since $\tau_j\tau_k = \tau_k\tau_j$ in Q, then $t(\tau_j\tau_k) = t(\tau_k\tau_j)$. So

$$\omega'(\tau_j, \tau_k)^{-1} = t(\tau_k\tau_j)t(\tau_k)^{-1}t(\tau_j)^{-1}. \tag{16}$$

Multiplying (15) and (16) yields

$$\omega'(\tau_k, \tau_j)\omega'(\tau_j, \tau_k)^{-1} = t(\tau_k)t(\tau_j)t(\tau_k)^{-1}t(\tau_j)^{-1} = [t(\tau_k), t(\tau_j)]. \tag{17}$$

To finish, we replace $t(\tau_i)$ with $s(\tau_i)$ in (14) and (17) and rewrite the equations additively. □

Remark 3.6. Lemma 3.5 is a generalization of [7, Lemma 6.10]. To see this, note that if the section t does satisfy (10) then $\omega'(\tau_i^\ell, \tau_i) = 0$ for $0 \le \ell \le p-2$.

3.5. The transgression map

Let M be a G-module such that N acts trivially on M. Since the action of N on M is trivial, an element $\phi \in \mathrm{H}^1(\mathrm{N}, \mathrm{M})$ is uniquely determined by a homomorphism $\phi : N \to M$.

Furthermore, Q acts by conjugation on N. Then $\phi \in \mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$ if and only if the homomorphism ϕ is Q-invariant, i.e., $\phi(q \cdot n) = q \cdot \phi(n)$ for all $n \in N$.

As in Section 2.7, associated with the exact sequence (7), there is the transgression map

$$d_2 : \mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q},\mathrm{M}). \tag{18}$$

We now give an algebraic description of $\mathrm{Ker}(d_2)$. Recall the definitions of $a_i, c_{j,k} \in N$ from (11) and (12). Write $N_{\tau_i} = 1 + \tau_i + \cdots + \tau_i{}^{p-1}$ for the norm of τ_i.

Theorem 3.7. *[7, Theorem 1.2]. Let M be a G-module such that N acts trivially on M. Suppose $\phi \in \mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$ is a class represented by a Q-invariant homomorphism $\phi : N \to M$. Then ϕ is in the kernel of d_2 if and only if there exist $m_0, \ldots, m_r \in M$ such that*

1. *$\phi(a_i) = -N_{\tau_i} m_i$ for $0 \le i \le r$ and*
2. *$\phi(c_{j,k}) = (1-\tau_k)m_j - (1-\tau_j)m_k$ for $0 \le j < k \le r$.*

3.6. The transgression map for Fermat curves

We now specialize to the Fermat curve setting. If M is any subquotient of the relative homology $\mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/\mathrm{p}\mathbb{Z})$ of the Fermat curve of degree p, then M is a G-module on which N acts trivially.

Recall that $Q = \mathrm{Gal}(L/K)$ is generated by $\{\tau_i \mid 0 \le i \le r\}$. From Section 2.6, $B_i \in \Lambda_1$ is such that $\tau_i \cdot \beta = B_i \beta$. The norm of B_{τ_i} is almost always zero, which is useful for determining subspaces of the kernel of d_2 arising from certain extensions of K in the next section.

Theorem 3.8. *[7, Theorem 4.6] Suppose $M = \mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/\mathrm{p}\mathbb{Z})$ is the relative homology of the Fermat curve of exponent p. Let N_{τ_i} denote the norm of B_i in Λ_1. If $p \ge 5$, then $N_{\tau_i} = 0$ for $0 \le i \le r$; if $p = 3$, then $N_{\tau_1} = 0$ but $N_{\tau_0} = y_0^2 y_1^2$.*

4. Subspaces of the kernel of the transgression map

The results in this section apply for any odd prime p satisfying Vandiver's Conjecture. The main theme is that Galois extensions of the cyclotomic field $K = \mathbb{Q}(\zeta_p)$ determine subspaces of the kernel $\mathrm{Ker}(d_2)$ of the transgression map.

We study this when M is a subquotient of the relative homology of the Fermat curve of degree p. In Section 4.2, we determine the subspaces of $\mathrm{Ker}(d_2)$ arising from ray class, cyclotomic and Kummer field extensions of K; Propositions 4.4, 4.9, 4.11 show that these are frequently trivial. The main result is Theorem 4.18 in Section 4.5 in which we determine the subspace of $\mathrm{Ker}(d_2)$ arising from Heisenberg extensions of K. We compute

this subspace with Magma for $p = 3, 5, 7$ using our explicit knowledge of the action of G_K on M.

4.1. Subextensions and subspaces

Suppose $\bar{E}$ is a subfield of E containing L such that E/K is Galois. Let $\bar{G} = \mathrm{Gal}(\bar{E}/K)$ and let $\bar{N} = \mathrm{Gal}(\bar{E}/L)$. Then $\bar{G}$ is a quotient of G and $\bar{N}$ is a quotient of N. In this situation, there is an exact sequence

$$1 \to \bar{N} \to \bar{G} \to Q \to 1. \tag{19}$$

An element $\bar{\phi} \in \mathrm{H}^1(\bar{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}}$ is uniquely determined by a Q-invariant homomorphism $\bar{\phi} : \bar{N} \to M$.

Lemma 4.1. *If the conjugation action of Q on $\bar{N}$ is trivial, then $\mathrm{H}^1(\bar{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}} \simeq (\mathrm{M}^{\mathrm{Q}})^{\rho}$ where $\rho = \dim_{\mathbb{F}_p}(\bar{N})$.*

Proof. This is clear since $\bar{\phi} \in \mathrm{H}^1(\bar{\mathrm{N}}, \mathrm{M})$ is Q-invariant if and only if $\bar{\phi}(\bar{N}) \subset M^Q$. □

Lemma 4.2. *There is a natural inclusion $\iota : \mathrm{H}^1(\bar{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}} \hookrightarrow \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}}$.*

Proof. This is true because the action of N on M is trivial and $\bar{N}$ is Q-invariant. More explicitly, $\iota(\bar{\phi})$ is the composition of the surjective reduction map $N \to \bar{N}$ with $\bar{\phi}$; if $\bar{\phi}$ is non-trivial, then so is $\iota(\bar{\phi})$. □

Associated with the exact sequence (19), there is a differential map

$$\bar{d}_2 : \mathrm{H}^1(\bar{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{M}). \tag{20}$$

Lemma 4.3. *Then $\bar{d}_2 = d_2 \circ \iota$ and $\mathrm{Ker}(\bar{d}_2) \subset \mathrm{Ker}(d_2)$.*

Proof. This follows from the description of $\iota(\bar{\phi})$ in the proof of Lemma 4.2. □

For the following types of extensions of K, we determine the element in $\mathrm{H}^2(\mathrm{Q}, \bar{\mathrm{N}})$ classifying the extension (19) and determine the resulting subspace $\mathrm{Ker}(\bar{d}_2)$ of $\mathrm{Ker}(d_2)$: ray class, cyclotomic, Kummer, Heisenberg, and U_4 extensions.

4.2. Information from ray class, cyclotomic, and Kummer extensions of K

4.2.1. The ray class group of K

Let $\Phi(G) = G^p[G, G]$ denote the Frattini subgroup of G. Let $\tilde{L}$ be the fixed field of E over K by $\Phi(G)$. By definition, $\tilde{G} = \mathrm{Gal}(\tilde{L}/K)$ is the elementary abelian p-group

$G/\Phi(G)$. Also $\tilde{L}$ is the maximal elementary abelian p-group extension of K ramified only over ν. Note that $L \subseteq \tilde{L}$. Let $\rho \in \mathbb{Z}^{\geq 0}$ be such that $\deg(\tilde{L}/L) = p^\rho$.

Note that $\Phi(G) \subset N$ since Q is an elementary abelian p-group. Let $\tilde{N} = N/\Phi(G)$. By definition, $\tilde{L}/L$ is Galois with group $\tilde{N} = \mathrm{Gal}(\tilde{L}/L)$.

By Lemma 4.3, $\mathrm{Ker}(\tilde{d}_2) \subset \mathrm{Ker}(d_2)$, where $\tilde{d}_2 : \mathrm{H}^1(\tilde{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{M})$.

Proposition 4.4. *Suppose M is a G-module on which $\tilde{N}$ acts trivially. If $\deg(\tilde{L}/L) = p^\rho$, then $\mathrm{Ker}(\tilde{d}_2) = \mathrm{H}^1(\tilde{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}} \simeq (\mathrm{M}^{\mathrm{Q}})^\rho$.*

Proof. By Lemma 4.1, $\mathrm{H}^1(\tilde{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}} \simeq (\mathrm{M}^{\mathrm{Q}})^\rho$. Since $\tilde{G}$ is an elementary abelian p-group, the images $\tilde{a}_i, \tilde{c}_{j,k} \in \tilde{N}$ of $a_i, c_{j,k} \in N$ are all trivial. The conditions in Theorem 3.7 for ϕ to be in $\mathrm{Ker}(\tilde{d}_2)$ are all satisfied, by taking $m_i = 0$ for $0 \leq i \leq r$. Thus $\mathrm{Ker}(\tilde{d}_2) = \mathrm{H}^1(\tilde{\mathrm{N}}, \mathrm{M})^{\mathrm{Q}}$. □

Example 4.5. Using Magma [2], we compute that $\rho = 0$ for $p < 37$ and $\rho = 1$ for $p = 37$, with the computation for $p \geq 23$ depending on the generalized Riemann hypothesis. To see this, consider the ray class group of K for the modulus $\mathfrak{m} = (1 - \zeta_p)^i$. By [19, Theorem 1] or [24, Theorem 1], the rank of its maximal elementary abelian p-group quotient stabilizes beyond some index i. Also $i = e + \lfloor \frac{e}{p-1} \rfloor + 1$, where $e = p - 1$ is the ramification index of $\langle 1 - \zeta_p \rangle$ of K above p, so $i = p + 1$. From this, it follows that $\rho = \dim_{\mathbb{F}_p} \mathrm{Cl}_{(1-\zeta_p)^i}(K)[p] - (r + 1)$.

4.2.2. A cyclotomic extension of K

Let $v = \zeta_{p^3}$. Let $w = v^p = \zeta_{p^2}$ and note that $w \in L$. Let $L^* = L(v)$. Let $r = (p-1)/2$.

Lemma 4.6. *The extension L^*/K is Galois and is ramified only over ν. The Galois group $G^* = \mathrm{Gal}(L^*/K)$ is isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^r$.*

Proof. This is because L^*/K is the compositum of the $\mathbb{Z}/p^2\mathbb{Z}$-extension $K(v)/K$ and the $\mathbb{Z}/p\mathbb{Z}$-extensions $K(\sqrt[p]{t_i})/K$ where $t_i = 1 - \zeta_p^{-i}$ for $1 \leq i \leq r$. These extensions are disjoint and each ramified only over ν. □

By Lemma 4.6, $L \subset L^* \subset E$. Then $N^* = \mathrm{Gal}(L^*/L)$ is a quotient of N. Let $a_i^*, c_{j,k}^*$ denote the images of $a_i, c_{j,k} \in N$ in $N^* = \mathrm{Gal}(L^*/L)$ for $0 \leq i \leq r$ and $0 \leq j < k \leq r$.

Lemma 4.7. *With notation as above, N^* is generated by a_0^*. Also, a_i^* is trivial for $1 \leq i \leq r$ and $c_{j,k}^*$ is trivial for $0 \leq j < k \leq r$.*

Proof. By Lemma 4.6, $G^* = \mathrm{Gal}(L^*/K)$ is abelian and generated by automorphisms τ_i^* whose image in Q is τ_i for $0 \leq i \leq r$; also τ_0^* has order p^2 and τ_i^* has order p for $1 \leq i \leq r$.

In particular, $\tau_0^*(v) = v^e$ for some exponent $e \in \mathbb{Z}/p^3\mathbb{Z}$ such that $p \nmid e$. The relation $v^p = w$ implies that $\tau_0^*(w) = w^e$. Thus $e \equiv p + 1 \bmod p^2$.

By definition, $a_0^* = (\tau_0^*)^p(v)/v$. Now $\tau_0^*(v) = v^{e^p}$. The condition $e \equiv p+1 \bmod p^2$ implies that $e^p \equiv 1+p^2 \bmod p^3$. Thus $a_0^* = v^{e^p-1} = v^{p^2} = \zeta_p$. Thus a_0^* is non-trivial and thus generates N^*.

By definition, $c_{j,k}^* = \tau_k^*\tau_j^*(\tau_k^*)^{-1}(\tau_j^*)^{-1}(v)/v$. Since G^* is abelian, $c_{j,k}^*$ is trivial.

For $1 \le i \le r$, by definition, $a_i^* = (\tau_i^*)^p(v)/v$. Since τ_i^* has order p, a_i^* is trivial. □

Proposition 4.8. *If M is a G-module on which N^* acts trivially, then $\mathrm{H}^1(\mathrm{N}^*, \mathrm{M})^{\mathrm{Q}} \simeq \mathrm{M}^{\mathrm{Q}}$.*

Proof. This follows from Lemma 4.1 and Lemma 4.7, with the isomorphism $\mathrm{H}^1(\mathrm{N}^*, \mathrm{M})^{\mathrm{Q}} \simeq \mathrm{M}^{\mathrm{Q}}$ identifying $\bar{\phi}^*$ with the value $\mu^* = \bar{\phi}^*(a_0^*) \in M^Q$. □

By Lemma 4.3, $\mathrm{Ker}(d_2^*) \subset \mathrm{Ker}(d_2)$ where $d_2^* : \mathrm{H}^1(\mathrm{N}^*, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{M})$.

Proposition 4.9. *Let X be the Fermat curve of degree p. Suppose M is a subquotient of the relative homology $\mathrm{H}_1(\mathrm{U}, \mathrm{Y}; \mathbb{Z}/\mathrm{p}\mathbb{Z})$.*

1. *If $p \ge 5$, then $\mathrm{Ker}(d_2^*) = 0$. The same is true for $p = 3$ when $M = \mathrm{H}_1(\mathrm{X}; \mathbb{Z}/3\mathbb{Z})$.*
2. *If $p = 3$ and $M = \mathrm{H}_1(\mathrm{U}; \mathbb{Z}/3\mathbb{Z})$ or $M = \mathrm{H}_1(\mathrm{U}, \mathrm{Y}; \mathbb{Z}/3\mathbb{Z})$, then $\mathrm{Ker}(d_2^*)$ has dimension 1 and is generated by the homomorphism $\phi^* : N^* \to M$ such that $\phi^*(a_0^*) = y_0^2 y_1^2$.*

Proof. A Q-invariant morphism $\phi^* : N^* \to M$ is determined by its image on the generator a_0^* of N^*. Theorem 3.7 contains the conditions for ϕ^* to be in $\mathrm{Ker}(d_2^*)$. By Theorem 3.8, $N_{\tau_i} = 0$ for $1 \le i \le r$. Since $c_{j,k}^* = 0$, and $a_i^* = 0$ for $1 \le i \le r$, these conditions are satisfied if and only if $\phi^*(a_0^*) = -N_{\tau_0} m_0$ for some $m_0 \in M$. If $p \ge 5$ then $N_{\tau_0} = 0$. If $p = 3$, then $N_{\tau_0} = y_0^2 y_1^2$, which is trivial in $\mathrm{H}_1(\mathrm{X}; \mathbb{Z}/3\mathbb{Z})$, but not in $\mathrm{H}_1(\mathrm{U}; \mathbb{Z}/3\mathbb{Z})$ or $\mathrm{H}_1(\mathrm{U}, \mathrm{Y}; \mathbb{Z}/3\mathbb{Z})$. □

The theory of higher ramification groups for a ramified prime in an extension of number fields can be found in [25, Chapter 4]. For ramification of order p^e, there are e jumps in the filtration which can be indexed in either the upper or lower numbering. The first jump is the same in both numbering systems and the conductor is one more than the last lower jump.

Lemma 4.10. *When p is a regular prime, then the conductor of L^*/L is $p^3 - 2p^2 + 2p$.*

Proof. The facts in this proof about jumps in ramification filtrations can be found in [25, Chapter 4]. The extension $K(w)/K$ has jump $p-1$. The extension $K(\sqrt[p]{t_i})/K$ has jump p for $1 \le i \le r$. Let $K^\circ = K(\sqrt[p]{t_1}, \dots \sqrt[p]{t_r})$. Then $L = K(w)K^\circ$.

When p is a regular prime, then there is a unique prime of L above p by Proposition 3.1. It is totally ramified since the residue field degrees of $K(w)/K$ and $K(\sqrt[p]{t_i})/K$ are all trivial. So L/K has $r+1$ upper jumps, and they are $u_1 = p-1$ and $u_2 = p$ (with multiplicity r). By Herbrand's formula, the lower jumps j_1 and j_2 satisfy $j_2 - j_1 = p(u_2 - u_1)$. So L/K has lower jumps $j_1 = p-1$ and $j_2 = 2p-1$ (with multiplicity r).

Thus $L/K(w)$ has lower jump $2p-1$ with multiplicity r. The jump of $K(v)/K(w)$ is p^2-1. Note that $L^* = K(v)K^\circ$. So $L^*/K(w)$ has upper jumps $U_1 = 2p-1$ (with multiplicity r) and $U_2 = p^2-1$. By Herbrand's formula, this has lower jumps $J_1 = 2p-1$ (with multiplicity r) and $J_2 = p^3-2p^2+2p-1$. Thus L^*/L has jump J_2 and conductor J_2+1. □

We use Lemma 4.10 in Notation 5.2 and Remark 5.8 to identify the non-trivial homomorphism $\phi^* \in \mathrm{Ker}(d_2^*)$ in $\mathrm{Ker}(d_2)$ when $p=3$, in which case the conductor of L^*/L is 15.

4.2.3. Kummer extensions

In this section, we show that some other Kummer extensions of L do not increase the dimension of $\mathrm{Ker}(d_2)$.

Let $K_0 = \mathbb{Q}(\zeta_{p^2})$ and $K_0^* = \mathbb{Q}(\zeta_{p^3})$. From Section 4.2.2, τ_0 lifts to an automorphism τ_0^* of K_0^* such that $\tau_0^*(\zeta_{p^3}) = \zeta_{p^3}^e$ for some integer e such that $e \equiv p+1 \bmod p^2$. Also $\tau_0^*(\zeta_{p^2}) = \zeta_{p^2}^e$.

Let $F_i^* = K(\sqrt[p^2]{t_i})$ where $t_i = 1-\zeta_p^{-i}$. Note that F_i^*/K is not Galois, but $F_i^*K_0$ is Galois over K_0. Also F_i^* is ramified only over $\nu = \langle 1-\zeta_p \rangle$.

Let F^* be the compositum of F_i^* for $0 \le i \le r$. Let $\tilde{G}^* = \mathrm{Gal}(F^*/K)$. Then $\tilde{G}^*$ is generated by the lifts τ_i^* of τ_i, each of which has order p^2. Let G° be the subgroup of $\tilde{G}^*$ generated by τ_i^* for $1 \le i \le r$. Since K_0^*/K is Galois, G° is normal and there is a short exact sequence

$$1 \to G^\circ \to \tilde{G}^* \to \langle \tau_0^* \rangle \to 1.$$

For $1 \le i \le r$, the conjugate of τ_i^* by τ_0^* is $(\tau_i^*)^e$ because

$$\tau_0^*\tau_i^*(\tau_0^*)^{-1}(\sqrt[p^2]{t_i}) = \tau_0^*(\zeta_{p^2}\sqrt[p^2]{t_i}) = \zeta_{p^2}^e\sqrt[p^2]{t_i} = (\tau_i^*)^e(\sqrt[p^2]{t_i}).$$

Note that F^* is an elementary abelian p-group extension of L which is ramified only above p. So $\bar{N}^* = \mathrm{Gal}(F^*/L)$ is a quotient of N. Let $\bar{a}_i^*$, $\bar{c}_{j,k}^*$ denote the images of a_i, $c_{j,k}$ in $\bar{N}^*$.

Proposition 4.11. *With notation as above:*

1. $\bar{N}^* \simeq (\mathbb{Z}/p\mathbb{Z})^{r+1}$ *and a basis for* $\bar{N}^*$ *is given by* $\bar{a}_i^*$ *for* $0 \le i \le r$;
2. *if* $j \neq 0$, *then* $\bar{c}_{j,k}^*$ *is trivial; if* $j = 0$, *then* $\bar{c}_{0,k}^* = \bar{a}_k^*$.
3. *If* M *is a subquotient of the relative homology of the Fermat curve, then the kernel of* $\bar{d}_2^*$ *on* $\bar{N}^*$ *equals* $\mathrm{Ker}(d_2^*)$ *from Proposition 4.9.*

Proof. 1. First $\bar{N}^* \simeq \times_{i=0}^r \bar{N}_i^*$ where $\bar{N}_i^* = \mathrm{Gal}(LK_i^*/L)$. By Lemma 4.7, $\bar{N}_0^* = N^*$ is generated by a_0^*. For $1 \le i \le r$, the image of $\bar{a}_i^*$ in $\bar{N}_i^*$ is non-trivial because $(\tau_i^*)^p(\sqrt[p^2]{t_i})/\sqrt[p^2]{t_i} = \zeta_p$; but the image of $\bar{a}_i^*$ in $\bar{N}_j^*$ for $i \neq j$ is trivial.

2. If $j \neq 0$, then $\bar{c}^*_{j,k}$ is trivial because τ^*_j and τ^*_k commute. If $j = 0$, then

$$\tau^*_0 \tau^*_k (\tau^*_0)^{-1} (\tau^*_k)^{-1} (\sqrt[p^2]{t_i}) / \sqrt[p^2]{t_i} = (\tau^*_k)^{e-1} (\sqrt[p^2]{t_i}) / (\sqrt[p^2]{t_i}) = \zeta_{p^2}^{e-1} = \zeta_p.$$

3. Suppose $\phi \in \bar{d}^*_2$. Then $\phi(\bar{a}^*_i) = 0$ for $1 \leq i \leq r$. So ϕ is zero on $\times_{i=1}^r \bar{N}^*$, and is thus determined by its image on $\bar{N}^*_0$. □

4.3. Review of Heisenberg extensions

Let H_p denote the mod p Heisenberg group, namely the multiplicative group of upper triangular 3×3 matrices with coefficients in $\mathbb{Z}/p\mathbb{Z}$ and diagonal entries equal to 1. Let U_p denote the central subgroup of H_p consisting of those matrices for which the upper right corner is the only non-zero entry off the diagonal.

Let $q : H_p \to H_p/U_p \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ denote the quotient map. The two coordinate projections $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ produce two classes ι_1, ι_2 in $\mathrm{H}^1(\mathbb{Z}/\mathrm{p}\mathbb{Z} \times \mathbb{Z}/\mathrm{p}\mathbb{Z}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$. The cup product $\iota_1 \cup \iota_2$ in $\mathrm{H}^2(\mathbb{Z}/\mathrm{p}\mathbb{Z} \times \mathbb{Z}/\mathrm{p}\mathbb{Z}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$ classifies the extension

$$1 \to U_p \to H_p \xrightarrow{q} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to 1. \tag{21}$$

Heisenberg extensions appear in many places in the literature. We follow the notation of [26]. The next result is a special case of [26, Proposition 2.3]. Let $K = \mathbb{Q}(\zeta_p)$.

Proposition 4.12. *Suppose $L_{\alpha,\beta} = K(\sqrt[p]{\alpha}, \sqrt[p]{\beta})$ is a field extension of K with $\mathrm{Gal}(L_{\alpha,\beta}/K) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then there is a Galois field extension R/K dominating $L_{\alpha,\beta}/K$ such that $\mathrm{Gal}(R/K) \to \mathrm{Gal}(L_{\alpha,\beta}/K)$ is isomorphic to $q : H_p \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ if and only if $\kappa(\alpha) \cup \kappa(\beta) = 0$ in $\mathrm{H}^2(\mathrm{G_K}, (\mathbb{Z}/\mathrm{p}\mathbb{Z})(2)) \cong \mathrm{H}^2(\mathrm{G_K}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$.*

Furthermore, by [26, Section 2.4], the extension R/K can be constructed explicitly, and in some sense uniquely, as follows. Let $K_\alpha = K(\sqrt[p]{\alpha})$ and $K_\beta = K(\sqrt[p]{\beta})$. Then $L_{\alpha,\beta} = K_\alpha K_\beta$. Let $\tau_\alpha \in \mathrm{Gal}(K_\alpha/K)$ be multiplication by ζ_p on $\sqrt[p]{\alpha}$ and let $\tau_\beta \in \mathrm{Gal}(K_\beta/K)$ be multiplication by ζ_p on $\sqrt[p]{\beta}$. These determine 2 characters χ_α and χ_β.

Consider the surjection $\bar{\rho} : G_K \to \mathrm{Gal}(L_{\alpha,\beta}/K)$. By [26, Section 2.4], $\bar{\rho}$ lifts to $\rho : G_K \to H_p$ if and only if the cup product $\chi_\alpha \cup \chi_\beta$ is zero. Also, the cup product equals the norm residue symbol (α, β) which is trivial if and only if $\beta \in N_{K_\alpha/K}(K^*_\alpha)$ [25, XIV.2]. In this case, let $\underline{\beta} \in K^*_\alpha$ be such that $\beta = N_{K_\alpha/K}(\underline{\beta})$. Then, let

$$\gamma_{\alpha,\beta} = \prod_{j=0}^{p-1} \tau_\alpha^j(\underline{\beta})^j. \tag{22}$$

By [26, Lemma 2.4], $\sigma(\gamma_{\alpha,\beta}) \equiv \gamma_{\alpha,\beta} \bmod (L^*_{\alpha,\beta})^p$ for all $\sigma \in \mathrm{Gal}(L_{\alpha,\beta}/K)$.

By [26, Theorem 2.5], the Heisenberg relation ρ has the property that, for all $\xi \in G_{L_{\alpha,\beta}}$,

$$\rho(\xi) = \mathrm{Ind}\frac{\xi(\sqrt[p]{\gamma_{\alpha,\beta}})}{\sqrt[p]{\gamma_{\alpha,\beta}}}.$$

This means that ρ factors through the extension $R_{\alpha,\beta} = L_{\alpha,\beta}(\sqrt[p]{\gamma_{\alpha,\beta}})$. Furthermore, $\gamma_{\alpha,\beta}$ is unique up to multiplication by an element of $K^*(L^*_{\alpha,\beta})^p$.

Finally, by [26, Equation 2.4],

$$\tau_\alpha(\gamma_{\alpha,\beta}) = \frac{\underline{\beta}^p}{N_{K_\alpha/K}(\underline{\beta})}\gamma_{\alpha,\beta}. \tag{23}$$

4.4. Heisenberg extensions of K

We apply this to the $(\mathbb{Z}/p\mathbb{Z})^2$-extensions of K in L. The Steinberg relation is that the cup product $\kappa(\alpha) \cup \kappa(1-\alpha) = 0$ is zero for any $\alpha \in K^* - \{1\}$, see [15, section 11]. Let $1 \le I \le r$. Choose $\alpha = \zeta_p^{-I}$ and $\beta = 1 - \zeta_p^{-I}$. Let

$$F_I = K(\sqrt[p]{\zeta_p^{-I}}, \sqrt[p]{1-\zeta_p^{-I}}).$$

Applying Proposition 4.12, there is a field extension R_I/K dominating F_I/K such that $\mathrm{Gal}(R_I/K) \to \mathrm{Gal}(F_I/K)$ is isomorphic to $q : H_p \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Lemma 4.13. *Let $w = \zeta_{p^2}$ and $\underline{\beta}_I = 1 - w^{-I}$. Let $K_\alpha = K(\sqrt[p]{\zeta_p^{-I}}) = K(w)$. Then $N_{K_\alpha/K}(\underline{\beta}_I) = 1 - \zeta_p^{-I}$.*

Proof. By definition, $N_{K_\alpha/K}(\underline{\beta}_I) = \prod_{\ell=0}^{p-1} \tau_0^\ell(\underline{\beta}_I)$. Because $\tau_0(w) = \zeta_p w$, this simplifies to

$$(1-w^{-I})(1-\zeta_p^{-I}w^{-I})\cdots(1-\zeta_p^{-I(p-1)}w^{-I}) = 1-\zeta_p^{-I}. \quad \square \tag{24}$$

By definition, τ_β acts by multiplication by ζ_p on $\sqrt[p]{\beta}$ where $\beta = 1-\zeta_p^{-I}$. So $\tau_\beta = \tau_I$. By definition, τ_α acts by multiplication by ζ_p on $\sqrt[p]{\alpha}$ where $\alpha = \zeta_p^{-I}$. So $\tau_\alpha = \tau_0^J$ where J is such that $-IJ \equiv 1 \bmod p$.

In particular, $\tau_\alpha(w) = \zeta_p^J w$. Write $\underline{\beta} = \underline{\beta}_I = 1 - w^{-I}$. So

$$\tau_\alpha^j(\underline{\beta}) = 1 - (\zeta_p^{jJ}w)^{-I} = 1 - \zeta_p^j w^{-I}.$$

Let $\gamma_I = \gamma_{\alpha,\beta}$. By (22),

$$\gamma_I = \prod_{j=0}^{p-1} \tau_\alpha^j(\underline{\beta})^j = \prod_{j=1}^{p-1}(1-\zeta_p^j w^{-I})^j = \prod_{j=1}^{p-1}(1-w^{pj-I})^j. \tag{25}$$

By (23) and Lemma 4.13,

$$\tau_\alpha(\gamma_I) = \frac{(1-w^{-I})^p}{1-\zeta_p^{-I}}\gamma_I. \tag{26}$$

Let $\tilde{R}_I = LR_I$. Both R_I/F_I and $\tilde{R}_I/L$ are generated by $\sqrt[p]{\gamma_I}$.

Lemma 4.14. *The Heisenberg extension R_I/K is ramified only over $1-\zeta_p$. Thus $\tilde{R}_I \subset E$.*

Proof. The field $\tilde{R}_I$ is a $\mathbb{Z}/p\mathbb{Z}$-Galois extension of L. The second statement follows directly from the first, since it guarantees that the ramification of $\tilde{R}_I$ occurs only at primes above p.

Recall that F_I over K is ramified only over p [6, Lemma 3.2]. So it suffices to prove that all the ramification of R_I over F_I lies above p. By [4, Lemma 5, Section 3.2], a prime η of F_I is unramified in R_I if $\eta \nmid p\gamma_I$. But γ_I is a product of powers of the conjugates of $\underline{\beta}_I$ under σ. Each of these conjugates of $\underline{\beta}_I$ is a generator for the unique prime ideal of K_I above p. Thus the primes of F_I which are ramified in R_I all lie above $\underline{\beta}_I$ which lies above p. Since there are no real places of K, there is no ramification of K over any infinite place. □

The following result is useful because the conductor is the same as the index of the modulus for which this extension appears in the ray class field.

Lemma 4.15. *The conductor of R_I/F_I is $p^2 + p(p-1)/2$.*

Proof. Take $z = \sqrt[p]{\gamma_I}$. Then z generates R_I/F_I. The conductor is the valuation in F_I of $g(z) - z = (\zeta_p - 1)z$, where g generates $\mathrm{Gal}(R_I/F_I)$. The valuation of z in F_I equals the valuation of γ_I in $\mathbb{Z}[\zeta_{p^2}]$ which is $1 + \cdots + (p-1) = p(p-1)/2$. So the conductor is $p^2 + p(p-1)/2$. □

We use Lemma 4.15 in Notation 5.2 and Remark 5.8 when $p = 3$, with conductor 12.

4.5. The Heisenberg classifying element

Recall that R_I/K is an H_p-Galois extension dominating F_I/K and $\tilde{R}_I = LR_I$. Let $N_I = \mathrm{Gal}(\tilde{R}_I/L) = \mathrm{Gal}(R_I/F_I) \simeq \mathbb{Z}/p\mathbb{Z}$.

Let $\tilde{R}$ be the compositum of $\tilde{R}_I$ for $I \in \mathcal{I} := \{1, \ldots, (p-1)/2\}$. Note that $\tilde{R}/K$ is Galois because the action of Q permutes the fields F_I, and thus permutes the Heisenberg extensions R_I. Thus Q stabilizes $\tilde{R}$. Let $\bar{N}_H = \mathrm{Gal}(\tilde{R}/L)$.

Proposition 4.16. *Let $\bar{a}_i, \bar{c}_{j,k}$ be the images of $a_i, c_{j,k}$ in $\bar{N}_H$. Then $\bar{N}_H \simeq \times_{I\in\mathcal{I}} N_I \simeq (\mathbb{Z}/p\mathbb{Z})^r$ and a basis for $\bar{N}_H$ is given by $\{\bar{c}_{0,k} \mid 1 \le k \le r\}$. In particular,*

1. *$\bar{a}_i$ is trivial for $0 \leq i \leq r$;*
2. *$\bar{c}_{j,k}$ is trivial if $j \neq 0$;*
3. *and the image of $\bar{c}_{0,k}$ in N_I is non-trivial if and only if $k = I$.*

Proof. With some risk of confusion, we use the same notation $\bar{a}_i$ and $\bar{c}_{j,k}$ to denote the images of $\bar{a}_i$ and $\bar{c}_{j,k}$ in $\mathrm{Gal}(R_I/F_I)$. The claim is that $\bar{a}_i$ and $\bar{c}_{j,k}$ are trivial for each I when $j \neq 0$ and that $\bar{c}_{0,k}$ is non-zero if and only if $k = I$.

The last part of this claim implies the main statement of Proposition 4.16. If $\bar{c}_{0,I}$ has a non-trivial image in N_I but a trivial image in N_k for $k \neq I$, then R_I is disjoint from the compositum of $\{R_k \mid 1 \leq k \leq r, k \neq I\}$.

Let $w = \zeta_{p^2}$ and let $t_I = \beta$. Recall that $F_I = K(w, \sqrt[p]{t_I})$ and that $\mathrm{Gal}(F_I/K)$ is generated by $\sigma = \tau_0$ and $\tau_\beta = \tau_I$ where $\sigma(w) = \zeta_p w = w^{1+p}$ and $\sigma(\sqrt[p]{t_I}) = \sqrt[p]{t_I}$ and $\tau_\beta(w) = w$ and $\tau_\beta(\sqrt[p]{t_I}) = \zeta_p \sqrt[p]{t_I}$. For $\ell \neq 0, I$, the other automorphisms τ_ℓ generating Q act trivially on F_I.

Recall that R_I/K is a Heisenberg extension and that σ and $\tau_1, \ldots, \tau_r$ extend to $\tilde{\sigma}$ and $\tilde{\tau}, \ldots, \tilde{\tau}_r$ in $\mathrm{Gal}(R_I/K)$. By definition, the elements $\bar{a}_i$ and $\bar{c}_{j,k}$ in N_I are

$$\bar{a}_i = \tilde{\tau}_i^p(\sqrt[p]{\gamma_I})/\sqrt[p]{\gamma_I},$$

and

$$\bar{c}_{j,k} = \tilde{\tau}_k \tilde{\tau}_j \tilde{\tau}_k^{-1} \tilde{\tau}_j^{-1}(\sqrt[p]{\gamma_I})/\sqrt[p]{\gamma_I}.$$

1. Then $\bar{a}_i$ is trivial because $\tilde{\tau}_i$ has order p in the Heisenberg group H_p.
2. If $j \neq 0$, then $\tilde{\tau}_j$ and $\tilde{\tau}_k$ fix $\sqrt[p]{\gamma_I}$, so $\bar{c}_{j,k}$ is trivial.
3. We compute $\bar{c}_{0,k}$ in N_I. Now $\bar{c}_{0,k} = [\tilde{\tau}_k, \tilde{\sigma}](\sqrt[p]{\gamma_I})/\sqrt[p]{\gamma_I}$. Since $\tilde{\sigma} = \tilde{\tau}_\alpha^{-I}$, the following quantity is non-trivial exactly when $\bar{c}_{0,k}$ is non-trivial:

$$[\tilde{\tau}_k, \tilde{\tau}_\alpha](\sqrt[p]{\gamma_I})/\sqrt[p]{\gamma_I} = \tilde{\tau}_k \tilde{\tau}_\alpha \tilde{\tau}_k^{-1} \tilde{\tau}_\alpha^{-1}(\sqrt[p]{\gamma_I})/\sqrt[p]{\gamma_I}. \tag{27}$$

By (26), for some $z \in \mu_p$,

$$\tilde{\tau}_\alpha(\sqrt[p]{\gamma_I}) = z\frac{1 - w^{-I}}{\sqrt[p]{1 - \zeta_p^{-I}}}\sqrt[p]{\gamma_I} = z\frac{1 - w^{-I}}{\sqrt[p]{t_I}}\sqrt[p]{\gamma_I}.$$

The value of z is not important since it is fixed by Q; set $z = 1$.
If $k \neq I$, then $\tilde{\tau}_k$ fixes $\sqrt[p]{t_I}$ and ω and thus commutes with the action of $\tilde{\tau}_\alpha$ on $\sqrt[p]{\gamma_I}$. Thus the quantity in (27) is trivial and $\bar{c}_{0,k}$ is trivial in N_I when $k \neq I$.
Now consider the case that $k = I$. The result is stated in [26, Equation 2.5]; since no details are included there, we include a proof for the benefit of the reader.
Note that $\tilde{\tau}_\alpha$ fixes $\sqrt[p]{t_k}$. Thus

$$\tilde{\tau}_\alpha^2(\sqrt[p]{\gamma_k}) = \frac{(1 - \tilde{\tau}_\alpha(w)^{-k})}{\sqrt[p]{t_k}}\frac{(1 - w^{-k})}{\sqrt[p]{t_k}}\sqrt[p]{\gamma_k}.$$

It follows that

$$\tilde{\tau}_\alpha^{p-1}(\sqrt[p]{\gamma_k}) = \frac{1}{(\sqrt[p]{t_k})^{p-1}}(1-w^k)(1-\tilde{\tau}_\alpha(w^k))\cdots(1-\tilde{\tau}_\alpha^{p-2}(w^k))\sqrt[p]{\gamma_k}.$$

Recall that $\tilde{\tau}_k$ acts by multiplication by ζ_p on $\sqrt[p]{t_k}$. By modifying $\tilde{\tau}_k$ by an element of $\mathrm{Gal}(\tilde{R}/L)$, we may assume that $\tilde{\tau}_k(\sqrt[p]{\gamma_k}) = \zeta_p\sqrt[p]{\gamma_k}$. It follows that

$$\tilde{\tau}_k^{p-1}\tilde{\tau}_\alpha^{p-1}(\sqrt[p]{\gamma_k}) = \frac{1}{\zeta_p(\sqrt[p]{t_k})^{p-1}}(1-w^k)(1-\tilde{\tau}_\alpha(w^k))\cdots(1-\tilde{\tau}_\alpha^{p-2}(w^k))\zeta_p\sqrt[p]{\gamma_k}. \quad (28)$$

Applying $\tilde{\tau}_\alpha$ to the right hand side of (28) yields

$$\frac{1}{(\sqrt[p]{t_k})^{p-1}}(1-\tilde{\tau}_\alpha(w^k))(1-\tilde{\tau}_\alpha^2(w^k))\cdots(1-\tilde{\tau}_\alpha^{p-1}(w^k))\frac{1-w^{-k}}{t_k}\sqrt[p]{\gamma_k}. \quad (29)$$

By Lemma 4.13,

$$\tilde{\tau}_\alpha\tilde{\tau}_k^{p-1}\tilde{\tau}_\alpha^{p-1}(\sqrt[p]{\gamma_k}) = \frac{1}{t_k}N_{K_\alpha/K}(1-w^k)\sqrt[p]{\gamma_k} = \sqrt[p]{\gamma_k}.$$

Thus

$$[\tilde{\tau}_k,\tilde{\tau}_\alpha](\sqrt[p]{\gamma_k}) = \tilde{\tau}_k\tilde{\tau}_\alpha\tilde{\tau}_k^{p-1}\tilde{\tau}_\alpha^{p-1}(\sqrt[p]{\gamma_k}) = \zeta_p\sqrt[p]{\gamma_k}.$$

Thus $\bar{c}_{0,k}$ is non-trivial in N_k, which completes the proof. □

Proposition 4.17. *If M is a G-module on which $\bar{N}_H$ acts trivially, then* $\mathrm{H}^1(\bar{\mathrm{N}}_\mathrm{H},\mathrm{M})^\mathrm{Q} \simeq (\mathrm{M}^\mathrm{Q})^\mathrm{r}$.

Proof. Since M is a trivial $\bar{N}_H$-module, $\mathrm{H}^1(\bar{\mathrm{N}}_\mathrm{H},\mathrm{M})^\mathrm{Q} \simeq \mathrm{Hom}(\bar{\mathrm{N}}_\mathrm{H},\mathrm{M})^\mathrm{Q}$. By Proposition 4.16, $\bar{N}_H$ has basis $\{\bar{c}_{0,k} \mid 1 \le k \le r\}$. Thus $\bar{\phi}$ is determined uniquely by the values $\mu_k = \bar{\phi}(\bar{c}_{0,k}) \in M$. Since $\bar{N}_I \simeq U_p$ is central in H_p, the homomorphism $\bar{\phi}$ is Q-invariant if and only if $\mu_k \in M^Q$ for $1 \le k \le r$ by Lemma 4.1. □

4.6. The kernel of d_2 for Heisenberg extensions

Consider the map

$$d_{2,H} : \mathrm{H}^1(\bar{\mathrm{N}}_\mathrm{H},\mathrm{M})^\mathrm{Q} \to \mathrm{H}^2(\mathrm{Q},\mathrm{M}).$$

By Lemma 4.3, $\mathrm{Ker}(d_{2,H}) \subset \mathrm{Ker}(d_2)$. By Proposition 4.17, we can study the isomorphic image of $\mathrm{Ker}(d_{2,H})$ in $(M^Q)^r$.

Theorem 4.18. *Let X be the Fermat curve of degree p. Let M be a subquotient of $\mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/\mathrm{p}\mathbb{Z})$. Then $\mathrm{Ker}(d_{2,H})$ is isomorphic to the set of all $(\mu_1,\ldots,\mu_r)\in(M^Q)^r$ such that*

$$(\mu_1,\ldots,\mu_r)=((1-\tau_1)m_0-(1-\tau_0)m_1,\ldots,(1-\tau_r)m_0-(1-\tau_0)m_r),$$

for some $m_0,\ldots,m_r\in M$ such that $(1-\tau_k)m_j-(1-\tau_j)m_k=0$ for all $1\le j<k\le r$. When $p=3$, we further require that $y_0^2y_1^2m_0=0$.

Proof. By Proposition 4.17, there is an isomorphism $\mathrm{H}^1(\bar{\mathrm{N}}_{\mathrm{H}},\mathrm{M})^{\mathrm{Q}}\to(\mathrm{M}^{\mathrm{Q}})^{\mathrm{r}}$, where $\bar\phi\mapsto(\mu_1,\ldots,\mu_r)$ where $\mu_k=\bar\phi(\bar c_{0,k})$. Recall the conditions on the tuple $(\mu_1,\ldots,\mu_r)$ in Theorem 3.7 which are equivalent to $\bar\phi$ being in $\mathrm{Ker}(\bar d_{2,H})$. By Theorem 3.8, the constraint $\bar\phi(\bar a_i)=-N_{\tau_i}m_i$ gives no constraint when $p\ge5$, because both sides equal zero; when $p=3$, then the constraint is only satisfied if $0=\bar\phi(\bar a_0)=-y_0^2y_1^2m_0$. □

Remark 4.19. By [1, 9.6 and 10.5.2], $1-\tau_k\in\langle y_0y_1\rangle$. By [6, Proposition 6.2], $\langle y_0y_1\rangle\simeq\mathrm{H}_1(\mathrm{U};\mathbb{Z}/\mathrm{p}\mathbb{Z})$. So $(\mu_1,\ldots,\mu_r)\in(\mathrm{H}_1(\mathrm{U};\mathbb{Z}/\mathrm{p}\mathbb{Z})^{\mathrm{Q}})^{\mathrm{r}}$.

4.7. Computing $\mathrm{Ker}(d_{2,H})$ *for small p*

We compute $\mathrm{Ker}(d_{2,H})$ for small p by finding matrices for the action of $\mathrm{Gal}(L/K)$ on $\mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/\mathrm{p}\mathbb{Z})$; the explicit formulas for this action are found in [7, Theorem 3.5]. From this, we determine matrices for the action on $\mathrm{H}_1(\mathrm{U};\mathbb{Z}/\mathrm{p}\mathbb{Z})$ and $\mathrm{H}_1(\mathrm{X};\mathbb{Z}/\mathrm{p}\mathbb{Z})$. We did these computations using Magma [2].

Example 4.20. When $p=3$, then $\bar\phi\in\mathrm{H}^1(\bar{\mathrm{N}}_{\mathrm{H}},\mathrm{M})$ is determined by $\mu_1=\bar\phi(\bar c_{0,1})$. Also, $\bar\phi$ is Q-invariant if and only if $\mu_1\in M^Q$.

Now $\bar\phi\in\mathrm{Ker}(d_{2,H})$ if and only if μ_1 is in the image of the map $T:M^2\to M$ given by $(m_0,m_1)\mapsto(1-\tau)m_0-(1-\sigma)m_1$ (condition $c_{0,1}$) and $y_0^2y_1^2m_0=0$ (condition a_0).

For $p=3$, we compute the dimension of $\mathrm{Ker}(d_{2,H})$ for several choices of M:

M	$\mathrm{H}_1(\mathrm{U},\mathrm{Y})$	$\mathrm{H}_1(\mathrm{U})$	$\mathrm{H}_1(\mathrm{X})$
$\dim(M^Q)$	5	3	2
$\dim(\mathrm{im}(T\mid_{\text{cond }a_0}))$	4	1	0
$\dim(\mathrm{Ker}(d_{2,H}))=\dim(M^Q\cap\mathrm{im}(T\mid_{\text{cond }a_0}))$	3	1	0

In particular, when $M=H_1(U,Y;\mathbb{Z}/3\mathbb{Z})$, then $\bar\phi\in\mathrm{Ker}(\bar d_{2,H})$ if and only if $\mu_1\in\mathrm{H}_1(\mathrm{U})^{\mathrm{Q}}$.

Example 4.21. When $p=5$, then $\bar\phi\in\mathrm{H}^1(\bar{\mathrm{N}}_{\mathrm{H}},\mathrm{M})$ is determined by $\mu_1=\bar\phi(\bar c_{0,1})$ and $\mu_2=\bar\phi(\bar c_{0,2})$. Also, $\bar\phi$ is Q-invariant if and only if $\mu_1,\mu_2\in M^Q$.

Now $\bar\phi\in\mathrm{Ker}(d_{2,H})$ if and only if (μ_1,μ_2) is in the image of the map $T:M^3\to M^2$ given by

$$(m_0, m_1, m_2) \mapsto ((1-\tau_1)m_0 - (1-\tau_0)m_1, (1-\tau_2)m_0 - (1-\tau_0)m_2),$$

(condition $c_{0,1}$, $c_{0,2}$) and $(1-\tau_2)m_1 - (1-\tau_1)m_2 = 0$ (condition $c_{1,2}$). For $p = 5$, we compute:

M	$\mathrm{H}_1(\mathrm{U};\mathrm{Y})$	$\mathrm{H}_1(\mathrm{U})$	$\mathrm{H}_1(\mathrm{X})$
$\dim(M^Q)$	11	9	8
$\dim((M^Q)^r)$	22	18	16
$\dim(\mathrm{im}(T\mid_{\mathrm{cond}\ c_{1,2}}))$	16	8	4
$\dim(\mathrm{Ker}(d_{2,H})) = \dim((M^Q)^r \cap \mathrm{im}(T\mid_{\mathrm{cond}\ c_{1,2}}))$	11	7	4

Example 4.22. For $p = 7$, we compute:

M	$\mathrm{H}_1(\mathrm{U};\mathrm{Y})$	$\mathrm{H}_1(\mathrm{U})$	$\mathrm{H}_1(\mathrm{X})$
$\dim(M^Q)$	17	15	14
$\dim((M^Q)^r)$	51	45	42
$\dim(\mathrm{im}(T\mid_J))$	36	23	16
$\dim(\mathrm{Ker}(d_{2,H})) = \dim((M^Q)^r \cap \mathrm{im}(T\mid_J))$	19	14	10

Here the image of $T : M^4 \to M^3$ are the triples (μ_1, μ_2, μ_3) satisfying conditions $c_{0,1}$, $c_{0,2}$, and $c_{0,3}$, and J denotes the conditions coming from $c_{1,2}$, $c_{1,3}$, and $c_{2,3}$.

Remark 4.23. In Theorem 4.18, taking $m_0 \in M$ and $m_i = 0$ for $1 \le i \le r$, we see that $\mathrm{Ker}(d_{2,H})$ contains a subspace isomorphic to the set

$$\{(\mu_1, \ldots, \mu_r) \in (M^Q)^r \mid (\mu_1, \ldots, \mu_r) = ((1-\tau_1)m_0, \ldots, (1-\tau_r)m_0)\}.$$

Thus,

$$\dim(\mathrm{Ker}(d_{2,H})) \ge \dim(\mathrm{Im}((B_{\tau_1} - 1)|_M) \cap M^Q). \tag{30}$$

When $p = 3, 5, 7$ and when $M = \mathrm{H}_1(\mathrm{X})$, the lower bound in (30) is in fact an equality.

4.8. Other unitary extensions

Recall that R_I/K is a Heisenberg degree p^3 extension for $1 \le I \le r$. Consider the group U_4 which has order p^6 and exponent p. Using the results of [16, Section 3.1], it is possible to construct a U_4-Galois extension of K from R_I/K and R_J/K, when $1 \le I < J \le r$. For $p \ge 5$, this yields a degree p^3 elementary abelian p-group extension $\bar{E}_U/L$. Let $\bar{N}_U = \mathrm{Gal}(\bar{E}_U/L)$. By [16, Claim, page 1036-1037], the lifts of τ_I and τ_J commute in U_4. This implies that the image of $c_{I,J}$ is trivial in $\bar{N}_U$. From this, we expect that $\dim(\mathrm{Ker}(d_2))$ grows by at least $\dim(M^Q)$ in the passage from $\bar{N}_H$ to $\bar{N}_U$.

5. The kernel of the transgression map when $p = 3$

In this section, $p = 3$. Then $K = \mathbb{Q}(\zeta_3)$ and L is the splitting field of $1 - (1 - x^3)^3$. Let $\sigma = \tau_0$ and $\tau = \tau_1$ be the generators of $Q = \mathrm{Gal}(L/K) \simeq (\mathbb{Z}/3\mathbb{Z})^2$ from Section 2.2.

Then E/L is the maximal elementary abelian 3-group extension of L ramified only over 3. Also $G = \mathrm{Gal}(E/K)$ and $N = \mathrm{Gal}(E/L)$. In Corollary 5.1, we show that $\dim_{\mathbb{F}_3}(N) = 10$.

Let $M = \mathrm{H}_1(\mathrm{U}, \mathrm{Y}; \mathbb{Z}/3\mathbb{Z})$ be the relative homology of the Fermat curve of degree 3. In Lemma 5.3, we find a basis for $\mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}}$; it has dimension 18.

In Proposition 5.6, we determine the element $\omega \in \mathrm{H}^2(\mathrm{Q}, \mathrm{N})$ classifying the exact sequence

$$1 \to N \to G \to Q \to 1. \tag{31}$$

Recall that $d_2 : \mathrm{H}^1(\mathrm{N}, \mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q}, \mathrm{N})$ is the transgression map.

The main result of the section is Corollary 5.7, in which we determine $\mathrm{Ker}(d_2)$ completely when $p = 3$: in particular, we show that it has dimension 5 and is determined by a degree 3^5 extension of K whose Galois group is non-abelian and has exponent 9; replacing M by $\mathrm{H}_1(\mathrm{X}; \mathbb{Z}/3\mathbb{Z})$, we show that $\mathrm{Ker}(d_2)$ is determined by the Heisenberg extension of K.

Similar calculations for $p = 5$ appear out of reach, since $\deg(L/\mathbb{Q}) = 500$ in that case.

5.1. Ray class fields when $p = 3$

A Magma computation shows that $\mathrm{Cl}(L)$ is trivial. By Proposition 3.1, there is a unique prime $\mathfrak{p}$ of L above p. We compute that $\mathfrak{p} = \langle \zeta_9, \sqrt[3]{t_1} \rangle$.

Let $L_{\mathbf{m}}$ (resp. $\mathrm{Cl}_{\mathbf{m}}(L)$) denote the ray class field (resp. group) of L of modulus $\mathbf{m}$.

Corollary 5.1. *When $p = 3$, then $N = \mathrm{Cl}_{\mathfrak{p}^{28}}(L)$ and $\dim_{\mathbb{F}_3}(N) = 10$.*

Proof. When $p = 3$, then $e = d = 18$, $f = 1$, and $e_1 = 9$. By Proposition 3.1, $\dim_{\mathbb{F}_3}(N) = 10$. By Lemma 3.2, $(\mathcal{O}_L/\mathfrak{p}^i)^\times$ has 3-rank 19 for $i \geq 28$. A Magma computation [2] shows that $\mathrm{Cl}_{\mathfrak{p}^{28}}(L) \simeq (\mathbb{Z}/3\mathbb{Z})^{10}$; in particular, $\mathrm{Cl}_{\mathfrak{p}^{28}}(L)$ has 3-rank 10. Thus $N = \mathrm{Cl}_{\mathfrak{p}^{28}}(L)$ since, by Lemmas 3.2 and 3.4, the rank does not increase for modulus $\mathfrak{p}^i$ for $i > 28$. □

More generally, we compute the 3-rank of the ray class group $\mathrm{Cl}_{\mathfrak{p}^i}(L)$ with modulus $\mathfrak{p}^i$ for $1 \leq i \leq 28$. The rank increases at modulus $\mathfrak{p}^i$ when i is one of the following values $m_1, \ldots, m_{10}$: 12, 15, 18, 20, 21, 23, 24, 26, 27, 28.

Notation 5.2. For $1 \leq \ell \leq 10$, let L_ℓ denote the maximal elementary abelian extension of L of modulus $\mathfrak{p}^{m_\ell}$ and consider $N_\ell = \mathrm{Gal}(L_\ell/L)$. By Lemma 4.15, $N_1 = \bar{N}_H$, where $\bar{N}_H$ is the quotient of N arising from the Heisenberg extension of K. By Lemma 4.10, $N_2 = N_1 N^*$, where N^* is the quotient of N arising from the cyclotomic extension of K.

5.2. Computation of $\mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$

Let $M = \mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/3\mathbb{Z})$. Then $\dim_{\mathbb{F}_3}(M) = 9$. Recall the definition of $y_0, y_1 \in \Lambda_1$ from Section 2.5 and the identification of M with Λ_1 from Section 2.6. We consider the following ordered basis V_M of M:

$$\left[1, y_1, y_1^2, y_0, y_0y_1, y_0y_1^2, y_0^2, y_0^2y_1, y_0^2y_1^2\right].$$

Let $B_\sigma, B_\tau \in \Lambda_1$ be such that $\sigma \cdot \beta = B_\sigma\beta$ and $\tau \cdot \beta = B_\tau\beta$. By [7, Example 3.7],

$$B_\sigma - 1 = y_0y_1(1 - y_0 - y_1),\ B_\tau - 1 = y_0y_1(-y_0 - y_1 + y_0y_1).$$

By [7, Example 5.5(1)], when $p = 3$ then $\{y_0^2, y_0^2y_1, y_0^2y_1^2, y_0y_1^2, y_0^2y_1^2\}$ is a basis for M^Q.

Lemma 5.3. *Let $p = 3$ and $M = \mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/3\mathbb{Z})$.*

1. *Then $\mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}} = \mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}}$ and $\dim_{\mathbb{F}_3}(\mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}}) = 18$.*
2. *There is a basis $\xi_1,\dots,\xi_7$ for N_7 (also the images of $\{\xi_1,\dots,\xi_\ell\}$ in N_ℓ are a basis for N_ℓ for $1 \le \ell \le 7$), such that $\mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}}$ is spanned by the image of the 10-dimensional $\mathrm{Hom}(N_2, M^Q)$ and the 8 maps $A_{11},\dots,A_{18}$:*

$$\begin{array}{llll}
A_{11}: \xi_1 \mapsto y_1 & \xi_4 \mapsto y_0y_1^2 + y_0^2y_1^2 & \xi_5 \mapsto y_0y_1^2 & \xi_7 \mapsto -y_0y_1^2 - y_0^2y_1^2 \\
A_{12}: \xi_1 \mapsto y_0 & \xi_4 \mapsto y_0^2y_1 + y_0^2y_1^2 & \xi_5 \mapsto y_0^2y_1 & \xi_7 \mapsto -y_0y_1^2 - y_0^2y_1^2 \\
A_{13}: \xi_1 \mapsto y_0y_1 & \xi_4 \mapsto y_0^2y_1^2 & \xi_5 \mapsto y_0^2y_1^2 & \xi_7 \mapsto -y_0^2y_1^2 \\
A_{14}: \xi_3 \mapsto y_1^2 & \xi_4 \mapsto -y_1^2 & \xi_5 \mapsto y_1^2 & \xi_7 \mapsto y_1^2 \\
A_{15}: \xi_3 \mapsto y_0y_1^2 & \xi_4 \mapsto -y_0y_1^2 & \xi_5 \mapsto y_0y_1^2 & \xi_7 \mapsto y_0y_1^2 \\
A_{16}: \xi_3 \mapsto y_0^2 & \xi_4 \mapsto -y_0^2 & \xi_5 \mapsto y_0^2 & \xi_7 \mapsto y_0^2 \\
A_{17}: \xi_3 \mapsto y_0^2y_1 & \xi_4 \mapsto -y_0^2y_1 & \xi_5 \mapsto y_0^2y_1 & \xi_7 \mapsto y_0^2y_1 \\
A_{18}: \xi_3 \mapsto y_0^2y_1^2 & \xi_4 \mapsto -y_0^2y_1^2 & \xi_5 \mapsto y_0^2y_1^2 & \xi_7 \mapsto y_0^2y_1^2
\end{array}$$

   (All basis elements ξ_i not listed map to 0).
3. *If $M_U = \mathrm{H}_1(\mathrm{U};\mathbb{Z}/3\mathbb{Z})$, then $\mathrm{H}^1(\mathrm{N},\mathrm{M_U})^{\mathrm{Q}}$ is spanned by the image of the 6-dimensional $\mathrm{Hom}(N_2, M_U^Q)$ and $\{A_{13}, A_{15}, A_{17}, A_{18}\}$; in particular, $\dim_{\mathbb{F}_3}(\mathrm{H}^1(\mathrm{N},\mathrm{M_U})^{\mathrm{Q}}) = 10$.*
4. *If $M_X = \mathrm{H}_1(\mathrm{X};\mathbb{Z}/3\mathbb{Z})$, then $\mathrm{H}^1(\mathrm{N},\mathrm{M_X})^{\mathrm{Q}}$ is spanned by the image of the 4-dimensional $\mathrm{Hom}(N_2, M_X^Q)$ and $\{A_{13}, A_{15}\}$; in particular, it follows that $\dim_{\mathbb{F}_3}(\mathrm{H}^1(\mathrm{N},\mathrm{M_X})^{\mathrm{Q}}) = 6$.*

Proof. We prove each statement using a Magma calculation [2]. Here are some details for part (1). By Corollary 5.1, N is a ray class group with $N \simeq (\mathbb{Z}/3\mathbb{Z})^{10}$. Using Magma, we find a basis for N and 10×10 matrices $M_{\sigma,10}$ and $M_{\tau,10}$ for the conjugation action of σ and τ on N with respect to that basis.

Since N acts trivially on M, an element of $\mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$ can be uniquely represented as a Q-invariant homomorphism $\phi : N \to M$. Since $\dim_{\mathbb{F}_3}(N) = 10$ and $\dim_{\mathbb{F}_3}(M) = 9$, ϕ is given by a 9×10 matrix A_ϕ with respect to the bases for M and N. Then ϕ is Q-invariant if and only if, for every $\vec{n} \in N$,

$$A_\phi(\vec{n}^\sigma) = B_\sigma \cdot A_\phi(\vec{n}),\ A_\phi(\vec{n}^\tau) = B_\tau \cdot A_\phi(\vec{n}).$$

To find the Q-invariant homomorphisms, we follow [22, pages 21-22] and set

$$A_{\sigma,10} = M_{\sigma,10} \otimes I_9 - I_{10} \otimes B_\sigma^t,\ A_{\tau,10} = M_{\tau,10} \otimes I_9 - I_{10} \otimes B_\tau^t.$$

Then ϕ is Q-invariant if and only if $A_\phi \in \mathrm{Ker}(A_{\sigma,10}) \cap \mathrm{Ker}(A_{\tau,10})$. Using Magma, we compute that $\dim(\mathrm{Ker}(A_{\sigma,10}) \cap \mathrm{Ker}(A_{\tau,10})) = 18$. Thus $\dim_{\mathbb{F}_p}(\mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}) = 18$.

By an analogous calculation, $\dim_{\mathbb{F}_p}(\mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}}) = 18$. By Lemma 4.2, the natural map $\mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$ is injective. Thus $\mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}} = \mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$. □

Remark 5.4. Recall that $\bar{N}_H$ (resp. N^*) is the quotient of N arising from the Heisenberg (resp. cyclotomic) extension of K. By Propositions 4.8 and 4.17 and Notation 5.2, $\mathrm{H}^1(\mathrm{N}_2,\mathrm{M})^{\mathrm{Q}} = \mathrm{H}^1(\bar{\mathrm{N}}_{\mathrm{H}},\mathrm{M})^{\mathrm{Q}} \oplus \mathrm{H}^1(\mathrm{N}^*,\mathrm{M})^{\mathrm{Q}}$. Furthermore, by Propositions 4.9 and Example 4.20, it follows that $\mathrm{Ker}(d_{2,H}) \simeq \mathrm{H}_1(\mathrm{U})^{\mathrm{Q}}$ has dimension 3 and $\mathrm{Ker}(d_2^*) \simeq \langle y_0^2 y_1^2 \rangle$ has dimension 1.

Example 5.5. Here are the matrices computed for the action of σ and τ on N_7:

$$M_{\sigma,7} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}; \text{ and } M_{\tau,7} = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (32)$$

For $1 \le \ell \le 7$, σ and τ act on N_ℓ via the upper-left $\ell \times \ell$ submatrices of $M_{\sigma,7}$ and $M_{\tau,7}$.

5.3. *Computing* $\mathrm{Ker}(d_2)$ *when* $p = 3$

By a Magma computation, $\dim_{\mathbb{F}_3}(\mathrm{H}^2(\mathrm{Q},\mathrm{N})) = 1$. The extension in (7) therefore corresponds to an element of $\mathbb{F}_3^*$. We make an arbitrary choice of element of $\mathbb{F}_3^*$ and compute an explicit 2-cocycle ω' representing $\omega \in \mathrm{H}^2(\mathrm{Q},\mathrm{N})$. Since the elements of $\mathbb{F}_3^*$ negate each other, $\mathrm{Ker}(d_2)$ is not affected by this choice.

By Section 3.4, the element $\omega \in H^2(Q,N)$ classifying (31) is determined by the elements $a, b, c \in N$ such that $a = s(\sigma)^3$, $b = s(\tau)^3$ and $c = [s(\sigma), s(\tau)]$.

Proposition 5.6. *Let a_7, b_7, c_7 denote the images of a, b, c in N_7. In terms of the basis $\xi_1, \ldots, \xi_7$,*

$$a_7 = [0,2,0,2,1,0,2],\ b_7 = [0,0,0,0,0,0,2],\ \text{and}\ c_7 = [2,1,2,0,2,1,0]. \tag{33}$$

Proof. Using Magma, we compute a 2-cocycle ω' for $\omega \in H^2(Q,N)$. Using Lemma 3.5, we compute $a = \omega'(\sigma,\sigma) + \omega'(\sigma^2,\sigma)$; $b = \omega'(\tau,\tau) + \omega'(\tau^2,\tau)$; and $c = \omega'(\tau,\sigma) - \omega'(\sigma,\tau)$. □

Corollary 5.7. *Let $p = 3$.*

1. *If $M = \mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/3\mathbb{Z})$ or $\mathrm{H}_1(\mathrm{U};\mathbb{Z}/3\mathbb{Z})$, then $\mathrm{Ker}(d_2) = \mathrm{Ker}(d_{2,3})$ and $\dim_{\mathbb{F}_3}(\mathrm{Ker}(d_2)) = 5$.*
2. *If $M = \mathrm{H}_1(\mathrm{X};\mathbb{Z}/3\mathbb{Z})$, then $\dim_{\mathbb{F}_3}(\mathrm{Ker}(d_2)) = 2$.*

Proof. By Lemma 5.3, a class $\phi \in \mathrm{H}^1(\mathrm{N},\mathrm{M})^{\mathrm{Q}}$ is uniquely determined by a Q-invariant homomorphism $\bar{\phi} : N_7 \to M$. Also $\phi \in \mathrm{Ker}(d_2)$ if and only if $\bar{\phi} \in \mathrm{Ker}(\bar{d}_2)$ where $\bar{d}_2 : \mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}} \to \mathrm{H}^2(\mathrm{Q},\mathrm{M})$. It thus suffices to compute using $H^1(N_7,M)^Q$, which is explicitly described in Lemma 5.3.

Let $\bar{\phi} \in \mathrm{H}^1(\mathrm{N}_7,\mathrm{M})^{\mathrm{Q}}$. By Theorem 3.7, when $p = 3$, then $\bar{\phi}$ is in $\mathrm{Ker}(\bar{d}_2)$ if and only if there exist m_0 and m_1 in M such that:

$$\bar{\phi}(a_7) = -N_\sigma m_0,\ \bar{\phi}(b_7) = -N_\tau m_1,\ \text{and}\ \bar{\phi}(c_7) = (1-\tau)m_0 - (1-\sigma)m_1.$$

Using Magma, this simplifies to $\bar{\phi}(a_7) \in \langle y_0^2 y_1^2 \rangle$ and $\bar{\phi}(b_7) = 0$ and $\bar{\phi}(c_7) \in \mathrm{H}_1(\mathrm{U})^{\mathrm{Q}}$.

The calculations for N_7 and N_3 have the same outcome. For N_3, we compute using Magma that these conditions are satisfied if and only if

$$\bar{\phi} \in \mathrm{Span}\{A_2, A_4, A_5, A_{10}, A_{13} + A_{18}\},$$

where $A_2 : \xi_1 \mapsto y_0 y_1^2$, $A_4 : \xi_1 \mapsto y_0^2 y_1$, $A_5 : \xi_1 \mapsto y_0^2 y_1^2$, $A_{10} : \xi_2 \mapsto y_0^2 y_1^2$, and

$$A_3 + A_{18} : \xi_1 \mapsto y_0 y_1,\ \xi_3 \mapsto y_0^2 y_1^2$$

(all generators not listed map to zero). Thus $\dim_{\mathbb{F}_3}(\mathrm{Ker}(d_2)) = 5$.

Replacing M by $\mathrm{H}_1(\mathrm{U})$, the images of the maps $A_2, A_4, A_5, A_{10}, A_{13} + A_{18}$ are in $\mathrm{H}_1(\mathrm{U})$ and $\mathrm{Ker}(d_2)$ is again 5-dimensional. Next, we replace M by $\mathrm{H}_1(\mathrm{X})$, which is 2-dimensional, say with basis v_1 and v_2. In this case, $\mathrm{Ker}(d_2)$ has dimension 2 and a basis is given by $\phi_1 : \xi_1 \mapsto v_1$ and $\phi_2 : \xi_1 \mapsto v_2$, where all generators not listed map to zero. □

Remark 5.8. When $M = \mathrm{H}_1(\mathrm{X};\mathbb{Z}/3\mathbb{Z})$, this shows that $\mathrm{Ker}(d_2)$ is determined by the Heisenberg extension of K. When $M = \mathrm{H}_1(\mathrm{U},\mathrm{Y};\mathbb{Z}/3\mathbb{Z})$, then $\mathrm{Ker}(d_2)$ is determined by the extension L_3/K. Note that $G_3 = \mathrm{Gal}(L_3/K)$ is non-abelian since $c_3 = [2,1,2]$ is non-trivial and has exponent 9 since $a_3 = [0,2,0]$ is non-trivial. In Magma notation, the group G_3 is **SmallGroup**$(243,13)$.

References

[1] G.W. Anderson, Torsion points on Fermat jacobians, roots of circular units and relative singular homology, Duke Math. J. (ISSN 0012-7094) 54 (2) (1987) 501–561, https://doi.org/10.1215/S0012-7094-87-05422-6.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. (ISSN 0747-7171) 24 (3–4) (1997) 235–265, https://doi.org/10.1006/jsco.1996.0125.

[3] K.S. Brown, Cohomology of Groups, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York-Berlin, ISBN 0-387-90688-6, 1982.

[4] Cassels, Fröhlich, Algebraic Number Theory, Academic Press, London, 1967.

[5] H. Cohen, Advanced Topics in Computational Number Theory, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, ISBN 0-387-98727-4, 2000.

[6] R. Davis, R. Pries, V. Stojanoska, K. Wickelgren, Galois action on the homology of Fermat curves, in: Directions in Number Theory, in: Assoc. Women Math. Ser., vol. 3, Springer, Cham, 2016, pp. 57–86.

[7] R. Davis, R. Pries, V. Stojanoska, K. Wickelgren, The Galois action and cohomology of a relative homology group of Fermat curves, J. Algebra (ISSN 0021-8693) 505 (2018) 33–69, https://doi.org/10.1016/j.jalgebra.2018.02.021.

[8] J. Ellenberg, 2-nilpotent quotients of fundamental groups of curves, Preprint, 2000.

[9] G. Gras, Remarks on K_2 of number fields, J. Number Theory (ISSN 0022-314X) 23 (3) (1986) 322–335, https://doi.org/10.1016/0022-314X(86)90077-6.

[10] G. Gras, Class Field Theory, Springer Monographs in Mathematics, Springer-Verlag, Berlin, ISBN 3-540-44133-6, 2003. From theory to practice, translated from the French manuscript by Henri Cohen.

[11] G. Gras, Test of Vandiver's conjecture with Gauss sums – heuristics, arXiv:1808.03443, 2018.

[12] G. Gras, Practice of incomplete p-ramification over a number field – history of abelian p-ramification, arXiv:1904.10707, 2019.

[13] G. Gras, J.-F. Jaulent, Sur les corps de nombres réguliers, Math. Z. (ISSN 0025-5874) 202 (3) (1989) 343–365, https://doi.org/10.1007/BF01159964.

[14] H. Koch, Galois Theory of p-Extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin, ISBN 3-540-43629-4, 2002. With a foreword by I.R. Shafarevich, translated from the 1970 German original by Franz Lemmermeyer, with a postscript by the author and Lemmermeyer.

[15] J. Milnor, Introduction to Algebraic K-Theory, Annals of Mathematics Studies, vol. 72, Princeton University Press/University of Tokyo Press, Princeton, N.J./Tokyo, 1971.

[16] J. Mináč, N.D. Tân, Construction of unipotent Galois extensions and Massey products, Adv. Math. (ISSN 0001-8708) 304 (2017) 1021–1054, https://doi.org/10.1016/j.aim.2016.09.014.

[17] A. Movahhedi, Sur les p-extensions des corps p-rationnels, Math. Nachr. (ISSN 0025-584X) 149 (1990) 163–176, https://doi.org/10.1002/mana.19901490113.

[18] A. Movahhedi, T. Nguyen-Quang-Do, Sur l'arithmétique des corps de nombres p-rationnels, in: Séminaire de Théorie des Nombres, Paris 1987–88, in: Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, pp. 155–200.

[19] N. Nakagoshi, The structure of the multiplicative group of residue classes modulo $\mathfrak{p}^{N+1}$, Nagoya Math. J. (ISSN 0027-7630) 73 (1979) 41–60, http://projecteuclid.org/euclid.nmj/1118785731.

[20] W. Narkiewicz, Global Class-Field Theory, Handbook of Algebra, vol. 1, North-Holland, Amsterdam, 1996, pp. 365–393.

[21] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, second edition, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), vol. 323, Springer-Verlag, Berlin, ISBN 978-3-540-37888-4, 2008, http://dx.doi.org/10.1007/978-3-540-37889-1.

[22] J.R. Ruí z Tolosa, E. Castillo, From Vectors to Tensors, Universitext, Springer-Verlag, Berlin, ISBN 3-540-22887-X, 2005.

[23] A. Schmidt, K. Wingberg, On the fundamental group of a smooth arithmetic surface, Math. Nachr. (ISSN 0025-584X) 159 (1992) 19–36, https://doi.org/10.1002/mana.19921590103, http://dx.doi.org/10.1002/mana.19921590103.

[24] M.H. Şengün, The nonexistence of certain representations of the absolute Galois group of quadratic fields, Proc. Am. Math. Soc. (ISSN 0002-9939) 137 (1) (2009) 27–35, https://doi.org/10.1090/S0002-9939-08-09435-5.

[25] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, ISBN 0-387-90424-7, 1979. Translated from the French by Marvin Jay Greenberg.

[26] R.T. Sharifi, Twisted Heisenberg representations and local conductors, Thesis (Ph.D.)–The University of Chicago, ProQuest LLC, Ann Arbor, MI, ISBN 978-0599-32437-4, 1999, http://gateway.proquest.com/openurl?url_ver=Z39.88-2004%26rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation%26res_dat=xri:pqdiss%26rft_dat=xri:pqdiss:9934118.
[27] L.C. Washington, Introduction to Cyclotomic Fields, second edition, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, ISBN 0-387-94762-0, 1997.
[28] J.G. Zarhin, Noncommutative cohomology and Mumford groups, Mat. Zametki (ISSN 0025-567X) 15 (1974) 415–419.