

ABSTRACT

Title of dissertation: RANKS OF p -CLASS GROUPS IN CYCLIC
 p -EXTENSIONS OF ANTI-CYCLOTOMIC
 \mathbb{Z}_2 -EXTENSIONS

ARIELLA KIRSCH
Doctor of Philosophy, 2019

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

In [17], Iwasawa proved a structure theorem for the ℓ -class group in \mathbb{Z}_ℓ -extensions. In this thesis, we consider instead the p -class group in \mathbb{Z}_ℓ -extensions, particularly when $\ell = 2$ and $p = 3$. Fixing $K_0 = \mathbb{Q}(i)$, we let L_0/K_0 be a cyclic degree p extension and let L_∞/L_0 be the lift of the anti-cyclotomic \mathbb{Z}_2 -extension of K_0 . The rank of the ambiguous ideal class group is given by Chevalley's formula. We study the question, does Chevalley's formula in fact explain the entire growth in the rank of the class group? We study the ranks of the class groups of L_0 and L_1 , proving results that give the rank of the class group when $p = 3$ and developing heuristics. We also consider the unit structure of K_n and prove that if a relative unit of K_n is the norm of an element in L_n^\times modulo p^{th} powers, then all of the relative units must be norms modulo p^{th} powers. Additionally, we include computational results and evidence that Iwasawa's structure theorem does not extend to the p -class group in \mathbb{Z}_ℓ -extensions.

RANKS OF p -CLASS GROUPS IN CYCLIC p -EXTENSIONS OF
ANTI-CYCLOTOMIC \mathbb{Z}_2 -EXTENSIONS

by

ARIELLA KIRSCH

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2019

Advisory Committee:

Professor Lawrence C. Washington, Chair/Advisor

Professor Patrick Brosnan

Professor William Gasarch

Professor Thomas Haines

Professor Niranjan Ramachandran

Acknowledgments

I would like to first thank Dr. Lawrence Washington, who was an incredibly helpful and patient advisor. I've been so very lucky to have his guidance over these last years. He was always supportive and willing to spend as much time answering my questions as I needed. I am very grateful.

I also want to thank Dr. Jill Pipher, who encouraged me to go to grad school and whose support has meant so much.

Thanks also to my cohort in 4202 and beyond, who made graduate school fun and full of new activities. Thanks in particular to Sean and Ryan for the many hours of coffee and games.

Thank you to my colleagues and supervisors, who were nothing but encouraging and outrageously flexible with my schedule.

I've been very lucky to have such a supportive network of friends and family, not all of whom I can name here. A huge thank you to Claire, Caitlin and Maddie, who've been cheering me on for years. Thank you to the amazingly enthusiastic Baltimore crowd. Thank you to Kate and Elizabeth for so much support in this last final push. Thank you, Jason, for always believing in me. Thank you to Ali, Sarah, Erica, Angela, Rachelle and Grace: it's so great to come home to you.

Finally, I owe so much to my family. The unconditional love and support of my parents and siblings, as well as my larger family, have made me who I am and I would never have made it to this point without you. Thank you for always being there for me.

Table of Contents

Dedication	ii
Acknowledgements	ii
Table of Contents	iii
List of Tables	v
List of Symbols	vi
1 Introduction	1
2 Cyclic extensions of imaginary quadratic fields	7
2.1 The Hilbert symbol and $(\sigma - 1)^2$ -rank of A	9
2.2 Symmetries	11
2.3 An example	14
3 Cubic extensions of $\mathbb{Q}(\zeta_8)$	20
3.1 Case 1: $e = 0$	27
3.2 Case 2: $e = 1$	33
3.3 Symmetries	45
3.3.1 Columns corresponding to type 1 primes.	45
3.3.2 Columns corresponding to type 2 primes.	46
3.3.3 Row corresponding to the extra generator	55
3.3.4 Matrix structure	56
3.4 An example	57
4 Galois structure of units	60
4.1 Units of K_1 and L_1	60
4.1.1 Units as norms of units	60
4.1.2 Galois module structure	65
4.2 Units of L_n/K_n	76
4.2.1 Preliminaries	77
4.2.2 Units as norms	79

5	Data	98
5.1	The anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$	98
5.2	L_0/K_0	99
5.3	L_1/K_1	101
5.3.1	Cubic extensions	105
5.3.2	Quintic extensions	109
5.4	L_2/K_2	110
6	Heuristics	113
6.1	L_0/K_0	113
6.2	L_1/K_1	127
6.2.1	Strongly ambiguous ideals	128
6.2.2	One rational prime ramifies	132
6.2.3	At least one type 2 prime	138
6.3	L_n/K_n	146
6.3.1	A conjecture	150
6.4	Group structure	157
7	The structure theorem	163
	Bibliography	167

List of Tables

5.1	Class Group Rank Statistics for $t_i = 0, t_s = 1$	100
5.2	Class Group Rank Statistics for $t_i = 2, t_s = 0$	100
5.3	Class Group Rank Statistics for $t_i = 1, t_s = 1$	100
5.4	Class Group Rank Statistics for $t_i = 0, t_s = 2$	101
5.5	Class Group Rank Statistics for $L_1, p = 3, t = 1, p_1 \equiv 7 \pmod{24}$. . .	106
5.6	Class Group Statistics for $L_1, p = 3, t = 1, p_1 \equiv 7 \pmod{24}$	106
5.7	Class Group Rank Statistics for $L_1, p = 3, t = 1, p_1 \equiv 19 \pmod{24}$. .	107
5.8	Class Group Statistics for $L_1, p = 3, t = 1, p_1 \equiv 19 \pmod{24}$	107
5.9	Class Group Rank Statistics for $L_1, p = 3, t = 2, p_i \equiv 7 \pmod{24}$. . .	108
5.10	Class Group Rank Statistics for $L_1, p = 3, t = 2, p_i \equiv 19 \pmod{24}$. . .	108
5.11	Class Group Statistics for $L_1, p = 3, t = 2, p_i \equiv 19 \pmod{24}$	108
5.12	Class Group Rank Statistics for $L_1, p = 3, t = 2, p_1 \equiv 7 \pmod{24},$ $p_2 \equiv 19 \pmod{24}$	109
5.13	Class Group Rank Statistics for $L_1, p = 3, t = 3, p_i \equiv 7 \pmod{24}$. . .	109
5.14	Class Group Rank Statistics for $L_1, p = 5, t = 1, p_1 \equiv 31 \pmod{40}$. .	110
5.15	Class Group Rank Statistics for $L_1, p = 5, t = 1, p_1 \equiv 11 \pmod{40}$. .	110
5.16	Class Group Rank Statistics for $L_2, p = 3, t = 1, p_1 \equiv 7 \pmod{24}$. . .	110
5.17	Class Group Rank Statistics for $L_2, p = 3, t = 1, p_1 \equiv 19 \pmod{24}$. .	111
5.18	Class Group Rank Statistics for $L_2, p = 3, t = 1, p_1 \equiv 7 \pmod{24}$. . .	111
5.19	Class Group Rank Statistics for $L_2, p = 3, t = 1, p_1 \equiv 19 \pmod{24}$. .	112
6.1	$P(\text{3-rank} = 2t_s + t_i - 1)$	126
6.2	$P(\text{3-rank} = 2t_s + t_i)$	126
6.3	$P(\text{3-rank} = 2t_s + t_i + 1)$	127
6.4	Expected Rank Probabilities for $t = 1, p_1 \equiv 3 \pmod{8}$	133
6.5	Expected Rank Probabilities for $t = 1, p_1 \equiv 7 \pmod{8}$	138

List of Symbols

$(\frac{\tilde{L}}{L})_{\mathfrak{p}_i}$	Artin symbol
$(\frac{x, \alpha}{\mathfrak{p}'})$	Hilbert symbol
$(\frac{u_j}{\mathfrak{p}_i})$	norm residue symbol
$(\frac{\varepsilon}{\mathfrak{p}_i})_p$	p^{th} residue symbol
A	p -Sylow subgroup of the class group
$\mathcal{C}\ell(K)$	class group of K
$\mathcal{C}\ell_{\mathfrak{p}_i}(K)$	ray class group of K at \mathfrak{p}_i
Δ	$\text{Gal}(L/K)$
E_K	unit group of K
E_n	unit group of K_n
$E(L/K)$	$[E_K : E_K \cap N_{L/K}(L^\times)]$
ε	a fundamental unit
L	cyclic degree p extension of K
\mathcal{O}_K	ring of integers in K
ω	primitive cube root of unity
P	probability
p_i	a rational prime
\mathfrak{p}_i	a prime in a number field
σ	generator of $\text{Gal}(L/K)$
t	number of rational ramified primes
t_1	number of rational type 1 ramified primes in L_1/K_1
t_2	number of rational type 2 ramified primes in L_1/K_1
t_i	number of rational ramified primes in L_0/K_0 which are inert in K_0
t_s	number of rational ramified primes in L_0/K_0 which split in K_0
U_K	unit group of K modulo p^{th} powers
U_n	unit group of K_n modulo p^{th} powers

Chapter 1: Introduction

In 1959, Iwasawa published his paper, *On Γ -extensions of algebraic number fields* [17], which contained the following fundamental theorem of Iwasawa theory:

Theorem 1.1 (Iwasawa, [17]). *Let K be a number field and let K_∞/K be a \mathbb{Z}_ℓ -extension. K_n is the unique subfield of K_∞ which is degree ℓ^n over K . Let*

$$h(K_n) = \ell^{e_n} r,$$

where $\ell \nmid r$, be the class number of K_n . Then there exist $\mu \geq 0, \lambda \geq 0, \nu$ independent of n and an integer n_0 such that for $n > n_0$,

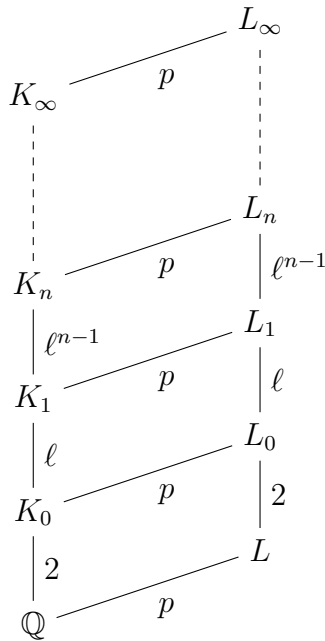
$$e_n = \mu \ell^n + \lambda n + \nu.$$

Iwasawa originally conjectured that the μ -invariant is zero in all \mathbb{Z}_ℓ -extensions, but in 1973 he proved that there exist extensions with arbitrarily large μ -invariants.

Theorem 1.2 (Iwasawa, [18]). *Let K be the cyclotomic field of ℓ^{th} roots of unity if $\ell > 2$ or the field of 4^{th} roots of unity if $\ell = 2$. For any integer $N \geq 1$, there exists a cyclic extension L of degree ℓ over K and a \mathbb{Z}_ℓ -extension L_∞ over L such that $\mu(L_\infty/L) \geq N$.*

However, in 1979 Ferrero and Washington [8] proved that the μ -invariant is in fact zero in cyclotomic \mathbb{Z}_ℓ -extensions of abelian number fields. This leads naturally to the question, what about non-cyclotomic \mathbb{Z}_ℓ -extensions?

We let K be an imaginary quadratic field and let K_∞/K be the anti-cyclotomic \mathbb{Z}_ℓ -extension. This extension is pro-dihedral (see [1]), or equivalently, it is the \mathbb{Z}_ℓ -extension in which $\text{Gal}(K/\mathbb{Q})$ acts by -1 on $\text{Gal}(K_\infty/K)$ (see [16]). We will consider degree p cyclic extensions L/K and then investigate the behavior of the p -class group in L_∞/L , where $L_\infty = LK_\infty$. Let K_n be the unique subfield of K_∞ which has degree ℓ^n over K_0 and let L_n be the unique subfield of L_∞ which has degree ℓ^n over L_0 .



Hubbard and Washington’s 2017 paper [16] addressed the Iwasawa invariants in degree ℓ Galois extensions of anti-cyclotomic \mathbb{Z}_ℓ -extensions of some imaginary quadratic fields.

Much less is known for the $\ell \neq p$ situation. However, in his 1975 paper, Washington made the following conjecture:

Conjecture 1.3 (Washington [25]). *Let $\ell \neq p$ be primes. Let L/K be a degree p extension. Let K_∞/K be a \mathbb{Z}_ℓ -extension and let K_n be the unique subfield of K_∞ which is degree ℓ^n over K . Let $L_\infty = LK_\infty$ and let $L_n = LK_n$ be the unique subfield of L_∞ which is degree ℓ^n over L . Let $h(L_n) = p^{e_n} r$, $p \nmid r$ be the class number of L_n . Then for sufficiently large n , there exist $A \geq 0$ and B independent of n such that $e_n = A\ell^n + B$.*

Washington [25] also showed that if $e_n \leq Mp^n$ for some constant M independent of n , then the exponent of A_n is bounded. Then all of the growth in the class group comes from an increase in rank.

Proving the conjecture using the methods required to prove Theorem 1.1 would be difficult, since it would require a determination of the structure of $\mathbb{Z}_\ell[[\mathbb{Z}_p]]$ ([25]). Instead, we'll consider explicitly the first layers of the extensions, L_0/K_0 and L_1/K_1 , and then develop some additional results and heuristics concerning L_n/K_n .

One of our main tools will be Chevalley's formula, which allows us to relate the class groups of K_n and L_n .

Theorem 1.4 (Chevalley's Formula, [4]). *Let L/K be a cyclic extension of number fields; $\Delta = \text{Gal}(L/K)$; $n = [L : K]$; C_L is the ideal class group of L ; $h(K)$ is the class number of K ; $e(L/K) = \prod_P e_P$ is the product over all primes P of K , including archimedean ones, where e_P is the ramification index of P in L/K ; and $E(L/K) = [E_K : E_K \cap N_{L/K}(L^\times)]$, where E_K is the group of units of K . Then*

$$|C_L^\Delta| = \frac{h(K) \cdot e(L/K)}{n \cdot E(L/K)}.$$

We can force growth in the class group by creating a tower in which $e(L_n/K_n)$ grows as n grows. Then Chevalley's formula ensures that the p -rank of the class group increases. Iwasawa used this to prove that there exist extensions with $\mu > 0$. In particular, Hubbard and Washington [16] showed that in the anti-cyclotomic \mathbb{Z}_ℓ -extension,

$$\mu \geq t - 1$$

and raised the question, can a non-zero μ be explained entirely by Chevalley's formula?

In [26], Washington showed that the p -class group is bounded in the cyclotomic \mathbb{Z}_ℓ -extension of an abelian number field with $\ell \neq p$. Furthermore, in [25], Washington pointed out that Chevalley's formula can be used to show that there can be unbounded growth in the p -class group using the anti-cyclotomic \mathbb{Z}_ℓ -extension when $\ell \neq p$.

In this thesis, we study the analogue of the above question, does Chevalley's formula in fact explain the entire growth in the $\ell \neq p$ case?

If $\ell \neq p$, we don't have the advantage of the structure theorem (Theorem 1.2), but there are other conditions which become easier when $\ell \neq p$. We will more generally attempt to understand how the p -class groups behave as one moves up the tower $L_0 \subseteq L_1 \subseteq \dots \subseteq L_n \subseteq \dots \subseteq L_\infty$.

In Chapter 2, we discuss the class group of a cyclic degree p extension L_0/K_0 , where K_0 is an imaginary quadratic field and L_0 is abelian over \mathbb{Q} .

Beginning in Chapter 3, we will fix $\ell = 2$ and we will consider only cubic

extensions L_n/K_n , where K_n is the n^{th} step in the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$. This is primarily for computational reasons. We want to be able to accumulate data to inform and check our heuristics, so choosing the smallest possible primes maximizes the number of computations we can perform. We choose $K_0 = \mathbb{Q}(i)$ since we know the first layers of the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$ from Hubbard and Washington [16] as well as from personal correspondence with Broker [2]. We also restrict the ramified primes in L_n/K_n so that a prime ramifies in L_n/K_n if and only if it is inert in K_0/\mathbb{Q} . This is the most interesting situation, since as we will see in Chapter 3, if a prime is inert in K_0/\mathbb{Q} then it splits completely in K_n/K_0 . This maximizes the number of primes which ramify in L_n/K_n and, as one can see from Chevalley's formula, maximizes the possible growth of the rank of the p -class group as we move up the tower.

We expect our algebraic results to hold in general, since with only minor modifications, almost all proofs should extend to the case where K_0 is an arbitrary imaginary quadratic field and $p \neq 3$. We chose to fix these parameters to make the proofs less technical and because this was the case in which we could obtain the most data.

Chapter 3 addresses L_1/K_1 and Chapter 4 contains results on the unit norms in both L_1/K_1 and the general L_n/K_n case. From Chevalley's formula, we can see that the unit norm index

$$E(L_n/K_n) = [E_K : E_K \cap N_{L/K}(L^\times)]$$

affects the rank of the class group, and much of Chapter 4 focuses on determining $E(L_n/K_n)$.

We used Sage [7] to compute the class groups of many cubic and some quintic extensions L_n/K_n for $0 \leq n \leq 2$, always with $K_0 = \mathbb{Q}(i)$ and K_∞/K_0 the anti-cyclotomic \mathbb{Z}_2 -extension. The results of these computations are found in Chapter 5.

In Chapter 6, we use this data and the results from Chapters 2 - 4 to develop heuristics for the ranks of the class groups in these extensions.

Finally, in Chapter 7 we present some evidence that Iwasawa's structure theorem (Theorem 1.1) for the p -class group of \mathbb{Z}_p -extensions does not extend to the p -class group of \mathbb{Z}_ℓ -extensions.

Chapter 2: Cyclic extensions of imaginary quadratic fields

Let p be an odd prime. Let $K = \mathbb{Q}(\sqrt{-D}) \neq \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field (so K does not contain p^{th} order roots of unity) and let L' be a cyclic number field of degree p . We assume that p does not divide the class number of K . Lift L' to an extension L of K ; therefore the Galois group of L/\mathbb{Q} is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Let σ be a generator for the Galois group of L/K :

$$\Delta = \text{Gal}(L/K) = \langle \sigma \rangle.$$

In this chapter, we will prove some results concerning the structure of the class group of L . This structure will depend on the number of ramified primes and on their behavior in K/\mathbb{Q} .

We let $\{\mathfrak{p}_j\}$ be the set of primes of K which ramify in L . Let

$$t = 2t_s + t_i$$

be the number of ramified primes in L/K where t_s is the number of rational primes dividing the discriminant of L/K which are split in K and t_i is the number which are inert in K . We write p_j for the rational prime lying under \mathfrak{p}_j . We make the

assumption that primes lying over p and those that are ramified in K/\mathbb{Q} are not ramified in L/K .

We wish to study the p -class group of L , which we denote by A . Following Gerth [11], we use the notation

$$A^{(\sigma-1)^j} = \{a^{(\sigma-1)^j} \mid a \in A\}.$$

Proposition 2.1 (Gras [13]). $A^{(\sigma-1)^j}/A^{(\sigma-1)^{j+1}}$ is an elementary abelian p -group and

$$\text{rank } A = \sum_{j=1}^{p-1} \text{rank } (A^{(\sigma-1)^{j-1}}/A^{(\sigma-1)^j}).$$

Here rank is used to denote the p -rank of the group. By studying the ranks on the right-hand side, we can better understand the full p -rank of the p -class group of L .

We now want to apply Chevalley's formula (Theorem 1.4). If we consider just the p -part of the class group, then since $p \nmid h(K)$, and $[L : K] = p$, we have

$$|A^\Delta| = \frac{e(L/K)}{p \cdot E(L/K)}.$$

Since K is an imaginary quadratic field and does not contain any p^{th} roots of unity, $E(L/K) = 1$. Furthermore, $e(L/K) = p^t$. Therefore

$$|A/A^{(\sigma-1)}| = |A^\Delta| = p^{t-1}.$$

In what follows, we investigate the rank of $A^{(\sigma-1)}/A^{(\sigma-1)^2}$, the $(\sigma - 1)^2$ -rank of A .

2.1 The Hilbert symbol and $(\sigma - 1)^2$ -rank of A

Recall that K is an imaginary quadratic field. We now make the assumption that $K \neq \mathbb{Q}(\sqrt{-3})$ and K has class number 1.

In order to define Hilbert symbols, we need to construct a Kummer extension. Following Wittmann [28], we let L_j/K be a cyclic extension of degree p such that \mathfrak{p}_j is the only prime that ramifies in L_j/K . Let

$$K' = K(\zeta)$$

where ζ is a primitive p^{th} root of unity. We write \mathfrak{p}'_j for any prime of K' lying over \mathfrak{p}_j . Assume there exists a Kummer generator $\alpha_j \in K'$ such that

$$L'_j = L_j K' = K'(\sqrt[p]{\alpha_j})$$

and only the prime \mathfrak{p}'_j ramifies in L'_j/K' . We also choose α_j such that $v_{\mathfrak{p}'_j}(\alpha_j) = 1$.

Then let

$$L' = LK' = K'(\sqrt[p]{\alpha})$$

be a Kummer extension where

$$\alpha = \alpha_1^{\nu_1} \dots \alpha_t^{\nu_t}$$

and $\nu_i \in \{1, \dots, p-1\}$. Without loss of generality, we may assume $\nu_1 = 1$.

$$\begin{array}{ccc}
 & & L' = K'(\sqrt[p]{\alpha}) \\
 & \nearrow^{p-1} & \downarrow p \\
 L & & K' = K(\zeta) \\
 \downarrow p & \nearrow^{p-1} & \downarrow 2 \\
 K = \mathbb{Q}(\sqrt{-D}) & & \mathbb{Q}(\zeta) \\
 \downarrow 2 & \nearrow^{p-1} & \\
 \mathbb{Q} & &
 \end{array}$$

Then we can compute the Hilbert symbol

$$\left(\frac{x, \alpha}{\mathfrak{p}'} \right)$$

for $x \in K'$ and $\mathfrak{p}' \in K'$.

The theorem below, due to Wittmann, will allow us to construct a matrix whose rank will determine the $(\sigma - 1)^2$ -rank of A . These matrices are sometimes called Rédei matrices (see [22], [24]). This theorem is a more general result which does not require the class number of K to be trivial.

Theorem 2.2 (Wittmann [28, Theorem 4.2.5]). *Let h_K be the class number of K .*

For $1 \leq j \leq t$ let $\pi_j \in \mathcal{O}_K$ be the generator of the principal ideal $\mathfrak{p}_j^{h_K}$. Let $M = (m_{ij})$

be the $t \times t$ matrix over \mathbb{F}_p defined by the Hilbert symbols

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}_i'} \right) = \zeta^{m_{ij}}.$$

Then

$$\dim_{\mathbb{F}_p} (A^{\sigma-1}/A^{(\sigma-1)^2}) = t - 1 - \text{rank} (M).$$

When $i \neq j$, we can compute $\left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right)$ using the formula for the tame Hilbert symbol.

Proposition 2.3 ([28, Equation 52]). *The tame Hilbert symbol is given explicitly as*

$$\left(\frac{x, \alpha}{\mathfrak{p}'}\right) = \left((-1)^{v_{\mathfrak{p}'}(x)v_{\mathfrak{p}' }(\alpha)} \cdot \alpha^{v_{\mathfrak{p}'}(x)} \cdot x^{-v_{\mathfrak{p}' }(\alpha)}\right)^{(N(\mathfrak{p}')-1)/p} \pmod{\mathfrak{p}'}$$

Recall that $\nu_i = v_{\mathfrak{p}'_i}(\alpha)$. Then we apply the proposition. For $i \neq j$:

$$\begin{aligned} \left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right) &\equiv \left((-1)^{v_{\mathfrak{p}'_i}(\pi_j)v_{\mathfrak{p}'_i}(\alpha)} \cdot \alpha^{v_{\mathfrak{p}'_i}(\pi_j)} \cdot \pi_j^{-v_{\mathfrak{p}'_i}(\alpha)}\right)^{(N(\mathfrak{p}'_i)-1)/p} \pmod{\mathfrak{p}'_i} \\ &\equiv (\pi_j^{-\nu_i})^{(N(\mathfrak{p}'_i)-1)/p} \pmod{\mathfrak{p}'_i}. \end{aligned}$$

When $i = j$, we use Hilbert's reciprocity law:

$$\prod_{\mathfrak{p}} \left(\frac{x, \alpha}{\mathfrak{p}}\right) = 1.$$

Then since the Hilbert symbol is trivial at unramified primes,

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}_j}\right) = \prod_{i \neq j} \left(\frac{\pi_j, \alpha}{\mathfrak{p}_i}\right)^{-1}.$$

2.2 Symmetries

First, a lemma.

Lemma 2.4. *Let τ be an element of $K'/\mathbb{Q}(\zeta)$ that restricts to a generator of $\text{Gal}(K/\mathbb{Q})$. Let $v_{\mathfrak{p}'_i}(x)$ be the \mathfrak{p}'_i -adic valuation of x . Then $v_{\mathfrak{p}'_i}(\alpha) \equiv v_{\mathfrak{p}'_i \tau}(\alpha) \pmod{p}$.*

Proof. First, the generator of $\text{Gal}(K'/K)$ acts trivially on the generator of $\text{Gal}(L'/K')$ and inverts ζ , and therefore the Kummer pairing implies that the generator of $\text{Gal}(K'/K)$ must act by inversion on α modulo p^{th} powers. So if we let \mathfrak{p}'_i and $\bar{\mathfrak{p}}'_i$ be the two primes of K' lying over $\mathfrak{p}_i \in K$, the Kummer generator α must generate an ideal of the form

$$\mathfrak{p}_1'^{\nu_1} \bar{\mathfrak{p}}_1'^{-\nu_1} \mathfrak{p}_2'^{\nu_2} \bar{\mathfrak{p}}_2'^{-\nu_2} \dots \mathfrak{p}_{2i+1}'^{\nu_{2i+1}} \bar{\mathfrak{p}}_{2i+1}'^{-\nu_{2i+1}} \mathfrak{p}_{2i+2}'^{\nu_{2i+2}} \bar{\mathfrak{p}}_{2i+2}'^{-\nu_{2i+2}} \dots \quad (2.1)$$

modulo p^{th} powers. Now note that τ acts trivially on the generator of $\text{Gal}(L'/K')$ and fixes ζ . Therefore by the Kummer pairing, τ must act trivially on α modulo p^{th} powers. Therefore if we write the ideal generated by α as in Equation 2.1, using the convention that $\tau \mathfrak{p}'_{2i+1} = \mathfrak{p}'_{2i+2}$, then applying τ to the ideal yields

$$\mathfrak{p}_2'^{\nu_1} \bar{\mathfrak{p}}_2'^{-\nu_1} \mathfrak{p}_1'^{\nu_2} \bar{\mathfrak{p}}_1'^{-\nu_2} \dots \mathfrak{p}_{2i+2}'^{\nu_{2i+2}} \bar{\mathfrak{p}}_{2i+2}'^{-\nu_{2i+2}} \mathfrak{p}_{2i+1}'^{\nu_{2i+1}} \bar{\mathfrak{p}}_{2i+1}'^{-\nu_{2i+1}} \dots$$

modulo p^{th} powers. Therefore $\nu_{2i+1} \equiv \nu_{2i+2} \pmod{p}$. □

Let $\tau \neq 1$ be an element of $\text{Gal}(K'/\mathbb{Q}(\zeta))$ which restricts to a generator of $\text{Gal}(K/\mathbb{Q})$. For $i \neq j$, we have

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i} \right) \equiv (\pi_j^{-\nu_i})^{(N(\mathfrak{p}'_i)-1)/p} \pmod{\mathfrak{p}'_i}.$$

Since τ fixes the p^{th} roots of unity, we have

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right) = \tau \left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right).$$

If \mathfrak{p}_i and \mathfrak{p}_j are inert in K/\mathbb{Q} , we have no new information. If \mathfrak{p}_i is split and \mathfrak{p}_j is inert, let $\tau\mathfrak{p}_i = \bar{\mathfrak{p}}_i$. Then $\tau\mathfrak{p}_j = \mathfrak{p}_j$ (and $\tau\pi_j = \pi_j$). Then by applying τ and using Lemma 2.4 we have

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right) = \tau \left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right) \equiv (\pi_j^{-\nu_i})^{(N(\bar{\mathfrak{p}}'_i)-1)/p} \pmod{\bar{\mathfrak{p}}'_i} \equiv \left(\frac{\pi_j, \alpha}{\bar{\mathfrak{p}}'_i}\right).$$

Similarly, if \mathfrak{p}_i is inert (and so $\mathfrak{p}_i = \bar{\mathfrak{p}}_i$) and \mathfrak{p}_j is split, we have

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right) \equiv (\bar{\pi}_j^{-\nu_i})^{(N(\mathfrak{p}'_i)-1)/p} \pmod{\mathfrak{p}'_i} \equiv \left(\frac{\bar{\pi}_j, \alpha}{\mathfrak{p}'_i}\right).$$

If both \mathfrak{p}_i and \mathfrak{p}_j are split, we have

$$\left(\frac{\pi_j, \alpha}{\mathfrak{p}'_i}\right) \equiv (\bar{\pi}_j^{-\nu_i})^{(N(\bar{\mathfrak{p}}'_i)-1)/p} \pmod{\bar{\mathfrak{p}}'_i} \equiv \left(\frac{\bar{\pi}_j, \alpha}{\bar{\mathfrak{p}}'_i}\right).$$

So if we order the primes which ramify in L/K as the $2t_s$ split primes followed by the t_i inert primes, with the condition that pairs of split primes are adjacent, then when we construct the matrix from Theorem 2.2 we get a matrix of the form

$$M = \left(\begin{array}{c|c} M_1 & M_2 \\ \hline M_3 & M_4 \end{array} \right).$$

The symmetries above show us that M_1 is a $2t_s \times 2t_s$ matrix composed of blocks of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

M_2 is a $2t_s \times t_i$ matrix of blocks of the form

$$\begin{pmatrix} a \\ a \end{pmatrix}$$

and M_3 is a $t_i \times 2t_s$ matrix of blocks of the form

$$\begin{pmatrix} a & a \end{pmatrix}.$$

Finally M_4 is a $t_i \times t_i$ matrix with no forced structure.

2.3 An example

Let $K = \mathbb{Q}(i)$ and L be a cyclic cubic extension where only primes lying above 13 and 19 ramify. 19 is inert in $\mathbb{Q}(i)$ but 13 splits: $13 = (3 + 2i)(3 - 2i)$.

So we have $\mathfrak{p}_{19} = (19)$, $\mathfrak{p}_{13} = (3 + 2i)$, and $\bar{\mathfrak{p}}_{13} = (3 - 2i)$. Additionally we have $\pi_{19} = 19$, $\pi_{13} = 3 + 2i$ and $\bar{\pi}_{13} = 3 - 2i$.

First, we need to fix cube roots of unity modulo the primes: $\zeta_{13} = 3$ and $\zeta_{19} = 7$.

We're looking for the values m_{ij} such that $\zeta^{m_{ij}} \equiv \pi_j^{(N\mathfrak{p}_i - 1)/p} \pmod{\mathfrak{p}_i}$. Note that $N\mathfrak{p}_{13} = N\bar{\mathfrak{p}}_{13} = 13$ and $N\mathfrak{p}_{19} = 361$.

We have the following results:

$$\zeta_{13}^m \equiv \bar{\pi}_{13}^{(13-1)/3} \pmod{\mathfrak{p}_{13}} \equiv (3-2i)^4 \equiv -119-120i \equiv 61 \pmod{(3+2i)}$$

$$\equiv 9 \pmod{13} \implies m = 2$$

$$\zeta_{13}^m \equiv \pi_{19}^{(13-1)/3} \pmod{\mathfrak{p}_{13}} \equiv (19)^4 \equiv 9 \pmod{(3+2i)}$$

$$\implies m = 2$$

$$\zeta_{13}^m \equiv \pi_{13}^{(13-1)/3} \pmod{\bar{\mathfrak{p}}_{13}} \equiv (3+2i)^4 \equiv -119+120i \equiv 61 \pmod{(3-2i)}$$

$$\equiv 9 \pmod{13} \implies m = 2$$

$$\zeta_{13}^m \equiv \pi_{19}^{(13-1)/3} \pmod{\bar{\mathfrak{p}}_{13}} \equiv (19)^4 \equiv 9 \pmod{(3-2i)}$$

$$\implies m = 2$$

$$\zeta_{19}^m \equiv \pi_{13}^{(361-1)/3} \pmod{\mathfrak{p}_{19}} \equiv (3+2i)^{120} \equiv 11 \pmod{19}$$

$$\implies m = 2$$

$$\zeta_{19}^m \equiv \bar{\pi}_{13}^{(361-1)/3} \pmod{\mathfrak{p}_{19}} \equiv (3-2i)^{120} \equiv 11 \pmod{19}$$

$$\implies m = 2$$

We now change our notation slightly: let α , the Kummer generator for L'/K' ,

be

$$\alpha = \alpha_{13}^{\nu_{13}} \bar{\alpha}_{13}^{\bar{\nu}_{13}} \alpha_{19}^{\nu_{19}}$$

where α_{13} , $\bar{\alpha}_{13}$, α_{19} are the Kummer generators for the extensions in which only \mathfrak{p}_{13} , $\bar{\mathfrak{p}}_{13}$ and \mathfrak{p}_{19} ramify respectively. By Lemma 2.4, $\nu_{13} = \bar{\nu}_{13}$. We can assume $\nu_{13} = 1$.

Therefore

$$\alpha = \alpha_{13}\bar{\alpha}_{13}\alpha_{19}^{\nu_{19}}.$$

So the matrix determined by the Hilbert symbols is

$$\begin{pmatrix} - & 2 & 2 \\ 2 & - & 2 \\ 2\nu_{19} & 2\nu_{19} & - \end{pmatrix}.$$

Filling in the missing positions so columns sum to zero:

$$M = \begin{pmatrix} 1 + \nu_{19} & 2 & 2 \\ 2 & 1 + \nu_{19} & 2 \\ 2\nu_{19} & 2\nu_{19} & 2 \end{pmatrix}.$$

Since $\nu_{19} \in \{1, 2\}$ we have two distinct possible matrices:

$$\begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 1 & 1 & 2 \end{pmatrix}$$

and so we expect to find two fields, each corresponding to one of the matrices above.

The two choices of $\nu_{19} = 1$ and $\nu_{19} = 2$ each give a different Kummer generator corresponding to a different field. The first matrix has rank 1 and the second has rank 2, which tells us that the field corresponding to the first has $(\sigma - 1)^2$ rank 1 and the second has rank 0.

Combining this result with Chevalley's formula, the 3-rank of the class group should be $(t - 1) + (t - 1 - \text{rank } M) = 4 - \text{rank } M$. Therefore we should have one class group with 3-rank 3 and one with 3-rank 2.

In fact, we can find explicitly two cubic cyclic extensions in which primes over 13 and 19 ramify.

First, we can find cyclic cubic extensions in which only primes over ℓ ramify for $\ell \equiv 1 \pmod{3}$ by finding a, b such that $\ell \equiv \frac{a^2 + 27b^2}{4}$, $b > 0$, $a \equiv 1 \pmod{3}$ (see [14]). Then

$$x^3 + x^2 + \frac{1 - \ell}{3}x - \frac{\ell(3 + a) - 1}{27}$$

gives the extension.

To find cyclic cubic extensions in which primes over 13 and 19 ramify, we take the composite of the field in which just primes over 13 ramify, given by

$$x^3 + x^2 - 4x + 1,$$

and the field in which just primes over 19 ramify, given by

$$x^3 + x^2 - 6x - 7.$$

Then we can use Sage [7] to find its degree 3 subfields. Two of these have discriminant $13^2 19^2$ and are in fact cyclic cubic number fields in which only 13 and

19 ramify. These fields are given by the polynomials

$$f_1(x) = x^3 - 64x^2 + 1036x - 4952,$$

$$f_2(x) = x^3 - 64x^2 + 1036x - 2976.$$

The field defined by f_1 has 3-class group

$$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

and the field defined by f_2 has 3-class group

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

We can also find the corresponding Kummer generators for the lifts of these fields.

$$f_1 : \quad \alpha = 2964\sqrt{-3} + 30628$$

$$f_2 : \quad \alpha = 17784\sqrt{-3} + 3952$$

If we fix the primes in K' as

$$\mathfrak{p}'_{13} = \frac{1}{2}(\sqrt{3} - 3i + 2)$$

$$\bar{\mathfrak{p}}'_{13} = \frac{1}{2}(-\sqrt{-3} - 2i + 3)$$

$$\mathfrak{p}'_{19} = \frac{1}{2}(-5\sqrt{-3} + 1)$$

then for f_1 , the valuation of α is 1 at each of the primes. For f_2 , the valuation at \mathfrak{p}'_{13} and $\bar{\mathfrak{p}}'_{13}$ is 1 but the valuation at \mathfrak{p}'_{19} is 2.

Chapter 3: Cubic extensions of $\mathbb{Q}(\zeta_8)$

We now consider cubic extensions of

$$K = \mathbb{Q}(\zeta_8),$$

which is the first step in both the cyclotomic and anti-cyclotomic \mathbb{Z}_2 -extensions of $\mathbb{Q}(i)$. We want to develop heuristics for the class group in extensions of the anti-cyclotomic \mathbb{Z}_2 -extension, and so want to be able to actually compute the class groups. We choose the \mathbb{Z}_2 -extension because we know explicitly what the fields in the tower are up to $n = 4$ due to Hubbard and Washington [16] and Broker [2]. We choose cubic extensions since this gives us the minimal possible degree for L/\mathbb{Q} . The theory and results in this extension should extend very similarly to arbitrary prime cyclic extensions of anti-cyclotomic \mathbb{Z}_ℓ -extensions of imaginary quadratic fields.

Let L/K be a cyclic cubic extension such that $\text{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z}$.

$$\begin{array}{c} L \\ \left| \begin{array}{c} 3 \\ 2 \times 2 \end{array} \right. \\ K = \mathbb{Q}(\zeta_8) \\ \left| \begin{array}{c} 2 \times 2 \\ \mathbb{Q} \end{array} \right. \end{array}$$

Let p_1, \dots, p_t be the rational primes which ramify in L/K , where $p_i \equiv 1 \pmod{3}$.

We only consider primes which are inert in $\mathbb{Q}(i)$, which means $p_i \equiv 3 \pmod{4}$.

Proposition 3.1 (Hubbard-Washington [16, Lemma 1]). *Let K_0 be an imaginary quadratic field and let K_∞/K_0 be the anti-cyclotomic extension of K_0 . If p is inert in K_0/\mathbb{Q} then p splits completely in K_∞/K_0 .*

Therefore there are two primes in K above every rational prime congruent to $3 \pmod{4}$: let $\mathfrak{p}_1, \dots, \mathfrak{p}_{2t}$ be the primes of K that ramify in L . We will always assume that conjugate primes are adjacent: \mathfrak{p}_{2n+1} and \mathfrak{p}_{2n+2} lie over the same rational prime.

Let $\Delta = \text{Gal}(L/K) = \langle \sigma \rangle$. Let A again be the p -class group of L .

By Chevalley's Formula (Theorem 1.4),

$$|A^\Delta| = \frac{h(K) \prod_{\mathfrak{p}} e_{\mathfrak{p}}}{[L : K][E_K : E_K \cap N_{L/K}L^\times]} = \frac{3^{2t-1}}{[E_K : E_K \cap N_{L/K}L^\times]} = \frac{3^{2t-1}}{E(L/K)}.$$

To determine $E(L/K)$, we can use the Hasse norm theorem. Since L/K is cyclic, an element is a global norm if and only if it is a local norm everywhere. Units are automatically local norms at unramified primes, so we need only to check the ramified primes. Since there is one fundamental unit, $\sqrt{2} + 1$, $E(L/K) = 1$ or $E(L/K) = 3$. Therefore

$$|A^\Delta| = 3^{2t-1-e}$$

where $[E_K : E_K \cap N_{L/K}L^\times] = 3^e$, $e \in \{0, 1\}$.

We will also need to again construct Kummer extensions. Let

$$K' = \mathbb{Q}(\zeta_8, \zeta_3) = \mathbb{Q}(\zeta_8, \sqrt{-3}).$$

Then let $L' = LK'$ and let α be a Kummer generator for the extension:

$$L' = K'(\sqrt[3]{\alpha}).$$

We will address the following two cases separately:

Case 1: $[E_K : E_K \cap N_{L/K}L^\times] = 1$, i.e. $e = 0$.

Case 2: $[E_K : E_K \cap N_{L/K}L^\times] = 3$, i.e. $e = 1$.

This is because of the proposition below. First, let

$$\mathcal{Cl}_{\mathfrak{p}_i}(K)$$

be the ray class group of K at \mathfrak{p}_i .

Proposition 3.2. *The fundamental unit $\sqrt{2} + 1$ of K is the norm of an element of L^\times (i.e. $e = 0$) if and only if 3 divides $|\mathcal{Cl}_{\mathfrak{p}_i}(K)|$ for all i .*

Proof. Let \mathfrak{p}_i be an arbitrary prime of K which ramifies in L/K . Consider the following exact sequence from class field theory:

$$1 \rightarrow U_{K,\mathfrak{p}_i}^{(1)} \rightarrow \mathcal{O}_K^\times \xrightarrow{\psi} (\mathcal{O}_K/\mathfrak{p}_i)^\times \rightarrow \mathcal{Cl}_{\mathfrak{p}_i}(K) \rightarrow \mathcal{Cl}(K) \rightarrow 1$$

where $U_{K,\mathfrak{p}_i}^{(1)}$ are the elements of \mathcal{O}_K^\times which are congruent to 1 mod \mathfrak{p}_i . Then since $h(K) = 1$, if

$$\varepsilon = \sqrt{2} + 1$$

is the fundamental unit of K , then

$$\mathcal{C}l_{\mathfrak{p}_i}(K) \simeq (\mathcal{O}_K/\mathfrak{p}_i)^\times / \psi(\varepsilon).$$

Therefore $|\mathcal{C}l_{\mathfrak{p}_i}(K)|$ is divisible by 3 if and only if ε is a cube mod \mathfrak{p}_i :

$$3 \mid |\mathcal{C}l_{\mathfrak{p}_i}(K)| \iff \left(\frac{\varepsilon}{\mathfrak{p}_i} \right)_3 = 1.$$

Since $p_i \equiv 7 \pmod{12}$, p_i splits completely in $\mathbb{Q}(\sqrt{-3})$ and therefore splits in K'/K . The explicit formula for the cubic residue symbol is

$$\left(\frac{\varepsilon}{\mathfrak{p}_i} \right)_3 \equiv \varepsilon^{(N\mathfrak{p}_i-1)/3} \pmod{\mathfrak{p}_i},$$

and therefore since $N\mathfrak{p}_i = N\mathfrak{p}'_i$, where \mathfrak{p}'_i is an arbitrary prime of K' above \mathfrak{p}_i ,

$$\left(\frac{\varepsilon}{\mathfrak{p}_i} \right)_3 = 1 \iff \left(\frac{\varepsilon}{\mathfrak{p}'_i} \right)_3 = 1.$$

Now, as stated above, $L' = K'(\sqrt[3]{\alpha})$. Then as in [3, Exercise 2.8], we can relate the power residue symbol to the Hilbert symbol

$$\left(\frac{\varepsilon}{\mathfrak{p}'_i} \right)_3^{v_{\mathfrak{p}'_i}(\alpha)} = \left(\frac{\varepsilon, \alpha}{\mathfrak{p}'_i} \right).$$

Since $v_{\mathfrak{p}'_i}(\alpha) \not\equiv 0 \pmod{3}$,

$$\left(\frac{\varepsilon}{\mathfrak{p}'_i}\right)_3 = 1 \iff \left(\frac{\varepsilon, \alpha}{\mathfrak{p}'_i}\right) = 1.$$

Therefore, we have so far shown that 3 divides $|\mathcal{C}\ell_{\mathfrak{p}_i}(K)|$ if and only if $\left(\frac{\varepsilon, \alpha}{\mathfrak{p}'_i}\right) = 1$. Then 3 divides $|\mathcal{C}\ell_{\mathfrak{p}_i}(K)|$ for all i if and only if $\left(\frac{\varepsilon, \alpha}{\mathfrak{p}'_i}\right) = 1$ for all i . But the second condition is true if and only if ε is the norm of an element of L' : there is an $a \in L'$ such that $N_{L'/K'}(a) = \varepsilon$. Note that $N_{K'/K}(\varepsilon) = \varepsilon^2$.

We have the following commutative diagram:

$$\begin{array}{ccc} L' & \xrightarrow{N_{L'/K'}} & K' \\ N_{L'/L} \downarrow & & \downarrow N_{K'/K} \\ L & \xrightarrow{N_{L/K}} & K \end{array}$$

Therefore,

$$N_{K'/K}(N_{L'/K'}(a)) = \varepsilon^2 \implies N_{L/K}(N_{L'/L}(a)) = \varepsilon^2$$

where $N_{L'/L}(a) \in L$. But since L/K has degree 3, ε^2 is the norm of an element in L if and only if ε is the norm of an element in L . Therefore

$$\varepsilon \text{ is the norm of an element in } L \iff 3 \text{ divides } |\mathcal{C}\ell_{\mathfrak{p}_i}(K)| \text{ for all } i.$$

□

We will also need to address the issue of strongly ambiguous ideal classes.

Definition 3.3. *The ideal classes of A^Δ are called the ambiguous ideal classes. An ambiguous ideal class $[\mathfrak{a}]$ is called strongly ambiguous if it contains an ideal fixed by $\sigma: \mathfrak{a}^{\sigma^{-1}} = (1)$. Denote the strongly ambiguous class group as A_{str}^Δ .*

Proposition 3.4 ([20]). $[A^\Delta : A_{str}^\Delta] = [E_K : N_{L/K}E_L] / [E_K : E_K \cap N_{L/K}L^\times]$.

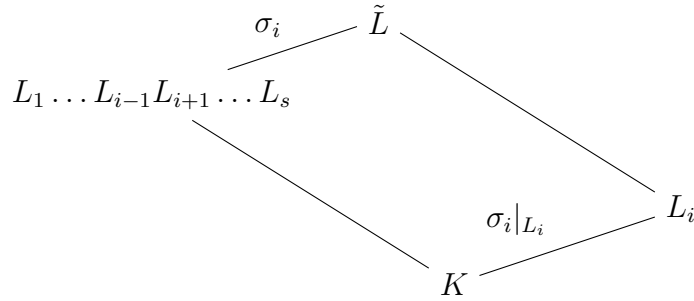
If $[E_K : N_{L/K}E_L] \leq 3$ and $[E_K : E_K \cap N_{L/K}L^\times] = 3$, then

$$[A^\Delta : A_{str}^\Delta] = 1$$

and so every ambiguous class is strongly ambiguous. We will continue to use the notation

$$[E_K : E_K \cap N_{L/K}L^\times] = 3^e.$$

Now let \tilde{L} be the genus field of L/K , i.e. the maximal unramified extension of L which is abelian over K . Assume that we can decompose \tilde{L} as the compositum of fields L_1, \dots, L_s for some s . Let $\sigma_1, \dots, \sigma_s$ be the generators of $\text{Gal}(\tilde{L}/K)$ such that σ_i restricted to L_i generates $\text{Gal}(L_i/K)$ and σ_j restricted to L_i for $i \neq j$ is trivial. For each i we have a diagram:



The core result of this chapter is the following theorem.

Theorem 3.5. *Let L/K be a cyclic cubic extension. Let $\{\mathfrak{P}_i\}_{i \in I}$ be the ideal classes which generate A^Δ . Let \tilde{L} be the genus field of L/K such that*

$$\text{Gal}(\tilde{L}/L) = \left\{ \prod_{j=1}^s \sigma_j^{n_j} \mid \sum_{j=1}^s n_j = 0 \right\}$$

where each σ_j has order 3. Then the 3-rank of A is

$$2(\text{rank } A^\Delta) - \text{rank } M,$$

where M is a matrix (a_{ij}) such that the a_{ij} are the exponents on the generators of the Galois group as given by the Artin symbol:

$$\left(\frac{\tilde{L}/L}{\mathfrak{P}_i} \right) = \prod_{j=1}^s \sigma_j^{a_{ij}}.$$

Proof. Consider the map $\varphi : A^\Delta \rightarrow A/A^{\sigma-1}$. Then we have an exact sequence

$$1 \rightarrow \ker \varphi = A^\Delta \cap A^{\sigma-1} \rightarrow A^{\sigma-1} \xrightarrow{\sigma-1} A^{(\sigma-1)^2} \rightarrow 1$$

and therefore

$$\dim(\ker(\varphi)) = \dim(A^{\sigma-1}/A^{(\sigma-1)^2}).$$

We can now define, as in Wittmann [28], a map

$$\Phi : A^\Delta \xrightarrow{\varphi} A/A^{\sigma-1} \xrightarrow{\cong} \text{Gal}(\tilde{L}/L) \hookrightarrow \text{Gal}(\tilde{L}/K) \simeq \mathbb{F}_3^s$$

where the middle isomorphism is given by the Artin map.

If we apply the Artin map to the generating classes $[\mathfrak{P}_i]$ of A^Δ , we get elements of $\text{Gal}(\tilde{L}/K)$

$$\left(\frac{\tilde{L}/L}{\mathfrak{P}_i}\right) = \prod_{j=1}^s \sigma_j^{a_{ij}}$$

with the condition that $\sum_{j=1}^s a_{ij} = 0$ and $a_{ij} \in \mathbb{F}_3$. Mapping the generating classes of A^Δ to \mathbb{F}_3^s we may construct a matrix $M = (a_{ij})$ whose rank equals $\dim(\text{im}(\varphi))$.

Therefore $\dim(\ker(\varphi)) = \text{rank } A^\Delta - \text{rank } M$ and so the 3-rank of A is then

$$\text{rank } A/A^{\sigma-1} + \text{rank } A^{\sigma-1}/A^{(\sigma-1)^2} = \text{rank } A^\Delta + \text{rank } A^\Delta - \text{rank } M.$$

□

3.1 Case 1: $e = 0$

Recall that $K = \mathbb{Q}(\zeta_8)$ and L/K is a cyclic cubic extension which is the lift of a cyclic cubic number field. There are t rational primes which ramify in the cyclic cubic number field. We make the assumption that each rational prime is inert in $\mathbb{Q}(i)$ and therefore splits completely in $K/\mathbb{Q}(i)$, so there are $2t$ primes which ramify in L/K . Recall that \tilde{L} is the genus field for L/K : the maximal unramified extension of L which is abelian over K .

By genus theory and Chevalley's formula,

$$[\tilde{L} : L] = |A/A^{\sigma-1}| = 3^{2t-1}.$$

By Proposition 3.2, since $e = 0$, 3 divides $|\mathcal{C}\ell_{\mathfrak{p}_i}(K)|$ for all i , and therefore there exists a degree 3 extension of K which is ramified only at \mathfrak{p}_i . Call this field L_i .

Let L_R be the ray class field over K at $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_{2t}$. By class field theory, $L \subseteq L_R$ since L is ramified at exactly the primes $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_{2t}$. Then, using the notation of Proposition 3.2,

$$[L_R : K] = \left| (\mathcal{O}_K/\mathfrak{p}_1 \dots \mathfrak{p}_{2t})^\times / \psi(\varepsilon) \right|.$$

By the Chinese Remainder Theorem,

$$(\mathcal{O}_K/\mathfrak{p}_1 \dots \mathfrak{p}_{2t})^\times / \psi(\varepsilon) \simeq \left((\mathcal{O}_K/\mathfrak{p}_1)^\times \times \dots \times (\mathcal{O}_K/\mathfrak{p}_{2t})^\times \right) / \psi(\varepsilon).$$

Since 3 divides

$$|\mathcal{C}\ell_{\mathfrak{p}_i}(K)| = |(\mathcal{O}_K/\mathfrak{p}_i)^\times / \psi(\varepsilon)|$$

for all i , the above has rank $2t$. We also know that $L_1 \dots L_{2t} \subseteq L_R$. The fields $\{L_i\}$ for $1 \leq i \leq 2t$ are disjoint, and therefore $[L_1 \dots L_{2t} : K] = 3^{2t}$. We therefore know that $L_1 \dots L_{2t}$ must be the maximal elementary 3-extension contained in L_R . Therefore $L \subseteq L_1 \dots L_{2t}$, since otherwise the extension would not be maximal, and so we have $[L_1 \dots L_{2t} : L] = 3^{2t-1}$.

Therefore since $L_1 \dots L_{2t} \subseteq \tilde{L}$, and both fields have degree 3^{2t-1} over L , the genus field \tilde{L} must be $L_1 \dots L_{2t}$.

Let \mathfrak{P}_i be the unique prime of L lying over \mathfrak{p}_i .

Proposition 3.6 ([28, Lemma 4.2.2]). *The ideal classes $\mathfrak{P}_1, \dots, \mathfrak{P}_{2t}$ generate the strongly ambiguous ideal class group.*

There are some subtleties here. When the ambiguous ideal class group does not equal the strongly ambiguous class group (we call this the ‘not strong’ or ‘weak’ situation), then we need to find an additional generator for the ambiguous ideal class group. We can determine if we need an additional generator by using the unit indices.

By Proposition 3.4, if $[E_K : N_{L/K}E_L] = 1$, the ambiguous ideal class group is exactly the strongly ambiguous ideal class group, and therefore $[\mathfrak{P}_1], \dots, [\mathfrak{P}_{2t}]$ generate A^Δ . If $[E_K : N_{L/K}E_L] = 3$, we need an additional generating ideal class, which we call $[\mathfrak{P}_0]$.

Now let σ_j be a generator of

$$\text{Gal}(\tilde{L}/L_1 \dots L_{j-1}L_{j+1} \dots L_{2t}) \simeq \text{Gal}(L_j/K)$$

for $j = 1, \dots, 2t$. Then we can write

$$\text{Gal}(\tilde{L}/K) = \{\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_{2t}^{n_{2t}}\}.$$

Then there must be some set of μ_j , $1 \leq j \leq 2t$, such that

$$\text{Gal}(\tilde{L}/L) = \{\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_{2t}^{n_{2t}} \mid \mu_1 n_1 + \dots + \mu_{2t} n_{2t} = 0\}.$$

If $\sigma_j \in \text{Gal}(\tilde{L}/L)$, that would imply $L \subseteq L_1 \dots L_{j-1} L_{j+1} \dots L_{2t}$ which cannot be true, since \mathfrak{p}_j is ramified in L/K . Therefore $\sigma_j \notin \text{Gal}(\tilde{L}/L)$ and so $\mu_j \neq 0$. Therefore we replace σ_j with $\sigma_j^{\mu_j^{-1}}$ as the generator of

$$\text{Gal}(\tilde{L}/L_1 \dots L_{j-1} L_{j+1} \dots L_{2t}) \simeq \text{Gal}(L_j/K).$$

Then

$$\text{Gal}(\tilde{L}/L) = \{\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_{2t}^{n_{2t}} \mid n_1 + \dots + n_{2t} = 0\}.$$

Now we can apply Theorem 3.5. If all ambiguous classes are strongly ambiguous, A^Δ is generated by $\{[\mathfrak{P}_i]\}$ for $1 \leq i \leq 2t$. Otherwise, we require an additional generator, which we call $[\mathfrak{P}_0]$.

Since $|A^\Delta| = 3^{2t-1}$, the 3-rank of A is $4t - 2 - \text{rank } M$, where $M = (a_{ij})$ such that

$$\left(\frac{\tilde{L}/L}{\mathfrak{P}_i} \right) = \sigma_1^{a_{i1}} \sigma_2^{a_{i2}} \dots \sigma_{2t}^{a_{i,2t}}.$$

In order to compute the Artin symbols and determine the matrix M , we need to consider L'/K' instead of L/K .

Recall that $K' = \mathbb{Q}(\zeta_8, \sqrt{-3})$ and $L' = LK' = K'(\sqrt[3]{\alpha})$. Let $L'_j = L_j K'$ for all j . Then we may find Kummer generators:

$$L'_j = K'(\sqrt[3]{\alpha_j}).$$

The generator α can be decomposed as a product of α_j , since L' is contained in the

compositum of the Kummer extensions $\{L'_j\}$:

$$\alpha = \alpha_1^{\nu_1} \alpha_2^{\nu_2} \dots \alpha_{2t}^{\nu_{2t}}.$$

Each α_j must divide α to ensure that $\mathfrak{p}'_1, \dots, \mathfrak{p}'_{2t}$ all ramify in L'/K' and therefore $\nu_j \neq 0$ for all j .

Let $\text{Gal}(L'/K') = \langle \sigma' \rangle$ such that $\sigma'|_L = \sigma$. Let $\text{Gal}(\tilde{L}'/K') = \langle \sigma'_1, \dots, \sigma'_{2t} \rangle$ such that $\sigma'_j|_{\tilde{L}} = \sigma_j$.

Fix a primitive cube root of unity ω . Specify the Galois action of σ'_j as

$$\sigma'_j(\sqrt[3]{\alpha_j}) = \omega^{\lambda_j} \sqrt[3]{\alpha_j}$$

where $\lambda_j \in \{1, 2\}$ and $\sigma'_j(\sqrt[3]{\alpha_i}) = \sqrt[3]{\alpha_i}$ for $i \neq j$.

Proposition 3.7 (Wittmann [28]). *There exists an $r \in \mathbb{F}_3^\times$ such that for all $1 \leq j \leq 2t$, $\lambda_j \nu_j = r$.*

Proof. For $i \neq j$, $\sigma'_i \sigma'_j{}^{-1} \in \text{Gal}(\tilde{L}'/L')$. Therefore

$$\sigma'_i \sigma'_j{}^{-1} \sqrt[3]{\alpha} = \sqrt[3]{\alpha},$$

but we may also express the action as

$$\sigma'_i \sigma'_j{}^{-1} \sqrt[3]{\alpha} = \sigma'_i \sqrt[3]{\alpha_i^{\nu_i}} \sigma'_j{}^{-1} \sqrt[3]{\alpha_j^{\nu_j}} \prod_{k \neq i, j} \sqrt[3]{\alpha_k^{\nu_k}} = \omega^{\lambda_i \nu_i - \lambda_j \nu_j} \sqrt[3]{\alpha}.$$

Therefore $\lambda_i \nu_i - \lambda_j \nu_j \equiv 0 \pmod{3}$ and so there must be some value r such that

$\lambda_j \nu_j \equiv r \pmod{3}$ for all j . Since $\nu_j \neq 0$ for all j and $\lambda_j \neq 0$ for all j , $r \not\equiv 0 \pmod{3}$. □

Now we need a way to explicitly compute the Artin symbols. We will do this by using the relationship between Artin symbols and Hilbert symbols in Kummer extensions. Let $K'(\sqrt[3]{x})$ be a Kummer extension of K' . Let $\mathfrak{p}' = (\pi')$ be a prime ideal which is unramified in $K'(\sqrt[3]{x})/K'$. Then

$$\left(\frac{K'(\sqrt[3]{x})/K'}{\mathfrak{p}'} \right) \sqrt[3]{x} = \left(\frac{\pi', x}{\mathfrak{p}'} \right) \sqrt[3]{x}.$$

We will also need the valuations of the α_j at the ramified primes. For $1 \leq j \leq 2t$, $v_{\mathfrak{p}'_j}(\alpha_j) = 1$ and $v_{\mathfrak{p}'_i}(\alpha_j) = 0$ for $i \neq j$. Note also that $K'(\sqrt[3]{\alpha_j})/K'$ is unramified outside of primes above \mathfrak{p}_j . Therefore for $i \neq j$,

$$\left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j} = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j}.$$

By the product rule for Hilbert symbols,

$$\left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_i} \right) = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_j} \right)^{-1}$$

since the product can be restricted to only the primes which divide α_j and π'_i .

Our expressions for the entries of the matrix will all be given in terms of Hilbert symbols of the form $\left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)$. By the explicit formula for the tame Hilbert

symbol, for $i \neq j$,

$$\left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)^{-1} \equiv (\pi'_i)^{(N\mathfrak{p}'_j-1)/3} \pmod{\mathfrak{p}'_j},$$

which is easily computable.

Theorem 3.5 defines the matrix giving the rank in terms of the Artin symbol $\left(\frac{\tilde{L}/L}{\mathfrak{P}_i} \right)$, where \mathfrak{P}_i is the unique prime of L lying over \mathfrak{p}_i . But by the restriction map, we may consider $\left(\frac{\tilde{L}'/L'}{\mathfrak{P}'_i} \right)$ instead of $\left(\frac{\tilde{L}/L}{\mathfrak{P}_i} \right)$. We can restrict the Artin symbol as follows:

$$\left(\frac{\tilde{L}'/L'}{\mathfrak{P}'_i} \right) \mapsto \left(\frac{\tilde{L}/L}{\mathfrak{P}_i} \right) \mapsto \left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_i} \right).$$

Then

$$\left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_i} \right)^{\nu_j} \sqrt[3]{\alpha_j} = \sigma_j'^{a_{ij}}(\sqrt[3]{\alpha_j}) = \omega^{a_{ij}\lambda_j} \sqrt[3]{\alpha_j}$$

and then by raising each side to the ν_j power,

$$\omega^{ra_{ij}} = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_j} \right)^{-\nu_j} = \left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)^{-\nu_j}$$

The factor r is a constant that will be present in each entry and therefore does not affect the rank of M .

3.2 Case 2: $e = 1$

We now consider the case where $e = 1$. This section will proceed similarly to §3.1, but there a few key differences.

We call a prime \mathfrak{p}_j

type 1 if 3 divides $|\mathcal{C}\ell_{\mathfrak{p}_j}(K)|$ and type 2 otherwise.

Let t_1 be the number of pairs of type 1 primes and let t_2 be the number of pairs of type 2 primes: $2t = 2t_1 + 2t_2$. Order the primes such that the first $2t_1$ primes are type 1 and the last $2t_2$ primes are type 2. By Proposition 3.2, we know $t_2 > 0$ since $e = 1$.

Let \tilde{L} again be the genus field for L/K : the maximal unramified extension of L which is abelian over K . By genus theory and Chevalley's formula,

$$[\tilde{L} : L] = |A/A^{\sigma-1}| = 3^{2t-2}.$$

For $1 \leq i \leq 2t_1$, 3 divides $|\mathcal{C}\ell_{\mathfrak{p}_i}(K)|$, and therefore there is a unique cyclic cubic extension of K in which only \mathfrak{p}_i ramifies. Call this extension L_i for $1 \leq i \leq 2t_1$.

For $2t_1 < i \leq 2t$, there is no degree 3 extension of K in which only \mathfrak{p}_i ramifies. However, for $2t_1 < i < 2t$, there do exist cyclic cubic extensions of K in which only \mathfrak{p}_i and \mathfrak{p}_{2t} ramify. To see this, consider

$$(\mathcal{O}_K/\mathfrak{p}_i\mathfrak{p}_j)^\times / \psi(\varepsilon)$$

where $i \neq j$. The numerator is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the denominator

$\psi(\varepsilon)$ annihilates at most one factor, and so

$$3 \mid |(\mathcal{O}_K/\mathfrak{p}_i\mathfrak{p}_j)^\times/\psi(\varepsilon)|.$$

Therefore the ray class field at two primes must exist. We will call these extensions L_i as well for $2t_1 < i < 2t$. The fields L_i for $1 \leq i < 2t$ are disjoint, and therefore $[L_1 \dots L_{2t-1} : K] = 3^{2t-1}$.

We now need to show that $L \subseteq L_1 \dots L_{2t-1}$. Let L_R again be the ray class field over K at $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_{2t}$. Then $L \subseteq L_R$ and

$$[L_R : K] = |(\mathcal{O}_K/\mathfrak{p}_1 \dots \mathfrak{p}_{2t})^\times/\psi(\varepsilon)|.$$

By the Chinese Remainder Theorem,

$$(\mathcal{O}_K/\mathfrak{p}_1 \dots \mathfrak{p}_{2t})^\times/\psi(\varepsilon) \simeq \left((\mathcal{O}_K/\mathfrak{p}_1)^\times \times \dots \times (\mathcal{O}_K/\mathfrak{p}_{2t})^\times \right) / \psi(\varepsilon).$$

Since $|\mathcal{C}\ell_{\mathfrak{p}_i}(K)|$ is not divisible by 3 for at least one i , the above has rank at most $2t - 1$. We also know that $L_1 \dots L_{2t} \subseteq L_R$. Since $[L_1 \dots L_{2t-1} : K] = 3^{2t-1}$, $L_1 \dots L_{2t-1}$ must be the maximal elementary 3-extension contained in L_R . Therefore $L \subseteq L_1 \dots L_{2t-1}$, since otherwise the extension would not be maximal. Since $[L : K] = 3$, $[L_1 \dots L_{2t-1} : L] = 3^{2t-2}$. Therefore since $L_1 \dots L_{2t-1} \subseteq \tilde{L}$, the genus field \tilde{L} must be exactly $L_1 \dots L_{2t-1}$.

Let σ_j be a generator of

$$\text{Gal}(\tilde{L}/L_1 \dots L_{j-1} L_{j+1} \dots L_{2t-1}) \simeq \text{Gal}(L_j/K)$$

for $1 \leq j \leq 2t - 1$. Then we can write

$$\text{Gal}(\tilde{L}/K) = \{\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_{2t-1}^{n_{2t-1}}\}.$$

Then, exactly as before, there must be some set of μ_j , $1 \leq j \leq 2t - 1$, such that

$$\text{Gal}(\tilde{L}/L) = \{\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_{2t-1}^{n_{2t-1}} \mid \mu_1 n_1 + \dots + \mu_{2t-1} n_{2t-1} = 0\}.$$

If $\sigma_j \in \text{Gal}(\tilde{L}/L)$, that would imply $L \subseteq L_1 \dots L_{j-1} L_{j+1} \dots L_{2t-1}$ which cannot be true, since \mathfrak{p}_j is ramified in L/K . Therefore $\sigma_j \notin \text{Gal}(\tilde{L}/L)$ and so $\mu_j \neq 0$. Therefore we may replace σ_j with $\sigma_j^{\mu_j^{-1}}$ as the generator of

$$\text{Gal}(\tilde{L}/L_1 \dots L_{j-1} L_{j+1} \dots L_{2t-1}) \simeq \text{Gal}(L_j/K).$$

Then

$$\text{Gal}(\tilde{L}/L) = \{\sigma_1^{n_1} \sigma_2^{n_2} \dots \sigma_{2t-1}^{n_{2t-1}} \mid n_1 + \dots + n_{2t-1} = 0\}.$$

Now we can apply Theorem 3.5. Since $\text{rank } A^\Delta = 2t - 2$, the 3-rank of A is

$4t - 4 - \text{rank } M$, where $M = (a_{ij})$ for $1 \leq i \leq 2t$ such that

$$\left(\frac{\tilde{L}/L}{\mathfrak{P}_i} \right) = \sigma_1^{a_{i1}} \sigma_2^{a_{i2}} \dots \sigma_{2t-1}^{a_{i,2t-1}}.$$

In order to compute the Artin symbols and determine the matrix M , we again need to consider L'/K' instead of L/K . Let $K' = \mathbb{Q}(\zeta_8, \sqrt{-3})$. Then let $L' = LK'$ and $L'_j = L_j K'$ for all j . Then we may find Kummer generators:

$$L' = K'(\sqrt[3]{\alpha}), \quad L'_j = K'(\sqrt[3]{\alpha_j}).$$

The generator α can be decomposed as a product of α_j :

$$\alpha = \alpha_1^{\nu_1} \alpha_2^{\nu_2} \dots \alpha_{2t-1}^{\nu_{2t-1}}.$$

Each α_j must divide α to ensure the correct ramification properties and therefore $\nu_j \neq 0$ for all j .

Let $\text{Gal}(L'/K') = \langle \sigma' \rangle$ such that $\sigma'|_L = \sigma$. Let $\text{Gal}(\tilde{L}'/K') = \langle \sigma'_1, \dots, \sigma'_{2t-1} \rangle$ such that $\sigma'_j|_{\tilde{L}} = \sigma_j$.

Fix a primitive cube root of unity ω . We again specify the Galois action of σ'_j as

$$\sigma'_j(\sqrt[3]{\alpha_j}) = \omega^{\lambda_j} \sqrt[3]{\alpha_j}$$

where $\lambda_j \in \{1, 2\}$ and $\sigma'_j(\sqrt[3]{\alpha_i}) = \sqrt[3]{\alpha_i}$ for $i \neq j$.

By Proposition 3.7, there exists an $r \in \mathbb{F}_3^\times$ such that for all $1 \leq j \leq 2t - 1$,

$$\lambda_j \nu_j = r.$$

Again let $K'(\sqrt[3]{x})$ be a Kummer extension of K' . Let $\mathfrak{p}' = (\pi')$ be a prime ideal which is unramified in $K'(\sqrt[3]{x})/K'$. Then

$$\left(\frac{K'(\sqrt[3]{x})/K'}{\mathfrak{p}'} \right) \sqrt[3]{x} = \left(\frac{\pi', x}{\mathfrak{p}'} \right) \sqrt[3]{x}.$$

For $1 \leq j \leq 2t_1$, $v_{\mathfrak{p}'_j}(\alpha_j) = 1$ and $v_{\mathfrak{p}'_i}(\alpha_j) = 0$ for $i \neq j$. For $2t_1 < j < 2t_1 + 2t_2$, $v_{\mathfrak{p}'_j}(\alpha_j) = 1$, and $v_{\mathfrak{p}'_i}(\alpha_j) = 0$ for $i \neq j, 2t$. Let

$$w_j = v_{\mathfrak{p}'_{2t}}(\alpha_j)$$

where $w_j \in \{1, 2\}$.

If \mathfrak{p}_j is a type 1 prime, then $K'(\sqrt[3]{\alpha_j})/K'$ is unramified outside of primes above \mathfrak{p}_j . Therefore for $i \neq j$,

$$\left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j} = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j}.$$

By the product rule for Hilbert symbols,

$$\left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_i} \right) = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_j} \right)^{-1}$$

since the product can be restricted to the primes which divide α_j and π'_i .

By the same argument as in the previous section,

$$\omega^{ra_{ij}} = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_j} \right)^{-\nu_j} = \left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)^{-\nu_j}$$

where the factor r is a constant that is present in each entry and so does not affect the rank of M .

Next, we address the columns corresponding to type 2 primes. If \mathfrak{p}_j is a type 2 prime, then the Kummer generator α_j is divisible by \mathfrak{p}'_j and \mathfrak{p}'_{2t} . Recall that $w_j = v_{\mathfrak{p}'_{2t}}(\alpha_j) \in \{1, 2\}$ and $v_{\mathfrak{p}'_j}(\alpha_j) = 1$. Then for $i \neq j, i \neq 2t$,

$$\left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j} = \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j}.$$

Now by the Hilbert product rule, and using the fact that α_j is divisible by \mathfrak{p}'_j and \mathfrak{p}'_{2t} ,

$$\begin{aligned} \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_i} \right) &= \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_j} \right)^{-1} \left(\frac{\pi'_i, \alpha_j}{\mathfrak{p}'_{2t}} \right)^{-1} \\ &= \left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)^{-1} \left(\frac{\pi'_i, \pi'_{2t} w_j}{\mathfrak{p}'_{2t}} \right)^{-1} \\ &= \left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)^{-1} \left(\frac{\pi'_i, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_j} \end{aligned}$$

Then since

$$\left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_i} \right) \sqrt[3]{\alpha_j} = \sigma_j^{a_{ij}}(\sqrt[3]{\alpha_j}) = \omega^{a_{ij}\lambda_j} \sqrt[3]{\alpha_j}$$

we have

$$\omega^{ra_{ij}} = \left(\frac{\pi'_i, \pi'_j}{\mathfrak{p}'_j} \right)^{-\nu_j} \left(\frac{\pi'_i, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_j \nu_j}.$$

When $i = j$, we can use the fact that $\sum_j a_{ij} = 0$ to fill in the missing element in the row.

Now we need to determine the values in the last row in the matrix, when $i = 2t$, and where \mathfrak{p}_j is a type 2 prime. Here, we cannot restrict

$$\left(\frac{\tilde{L}'/L'}{\mathfrak{P}'_{2t}} \right) \nrightarrow \left(\frac{K'(\sqrt[3]{\alpha_j})/K'}{\mathfrak{p}'_{2t}} \right)$$

since the Artin symbol is only defined at unramified primes, and \mathfrak{p}'_{2t} ramifies in $K'(\sqrt[3]{\alpha_j})$ for $2t_1 < j < 2t$.

Instead, we construct auxiliary fields in which only \mathfrak{p}'_{2t_1+1} and \mathfrak{p}'_k ramify, for $2t_1 + 2 \leq k \leq 2t - 1$. In particular, \mathfrak{p}'_{2t} does not ramify in any of these extensions.

We construct these extensions as $K'(\sqrt[3]{\alpha_{2t_1+1} \alpha_k^{m_k}})$, where $m_k \in \{1, 2\}$ is chosen to ensure that \mathfrak{p}'_{2t} does not ramify in the extension. Then we can restrict our Artin symbol as

$$\left(\frac{\tilde{L}'/L'}{\mathfrak{P}'_{2t}} \right) \mapsto \left(\frac{K'(\sqrt[3]{\alpha_{2t_1+1} \alpha_k^{m_k}})/K'}{\mathfrak{p}'_{2t}} \right).$$

We have

$$\left(\frac{\tilde{L}'/L'}{\mathfrak{P}'_i} \right) = \sigma_1^{a_{i1}} \sigma_2^{a_{i2}} \dots \sigma_{2t-1}^{a_{i,2t-1}}.$$

We also have

$$\sigma'_j(\sqrt[3]{\alpha_j}) = \omega^{\lambda_j} \sqrt[3]{\alpha_j}$$

and for $i \neq j$,

$$\sigma'_j(\sqrt[3]{\alpha_i}) = \sqrt[3]{\alpha_i}.$$

The new Artin symbol then acts as

$$\begin{aligned} & \left(\frac{K'(\sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}})/K'}{\mathfrak{p}'_{2t}} \right) \sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}} \\ &= \sigma_{2t_1+1}^{a_{2t,2t_1+1}} \sigma_k^{a_{2t,k}} \left(\sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}} \right) \\ &= \omega^{a_{2t,2t_1+1}\lambda_{2t_1+1} + a_{2t,k}\lambda_k m_k} \sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}} \end{aligned}$$

We also use its relationship to the Hilbert symbol:

$$\left(\frac{K'(\sqrt[3]{\alpha_{2t_1+1}\alpha_k})/K'}{\mathfrak{p}'_{2t}} \right) \sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}} = \left(\frac{\pi'_{2t}, \alpha_{2t_1+1}\alpha_k^{m_k}}{\mathfrak{p}'_{2t}} \right) \sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}}.$$

Then, since $v_{\mathfrak{p}'_i}(\alpha_{2t_1+1}\alpha_k^{m_k}) = 0$ for $i \neq 2t_1 + 1, k$,

$$\begin{aligned} \left(\frac{\pi'_{2t}, \alpha_{2t_1+1}\alpha_k^{m_k}}{\mathfrak{p}'_{2t}} \right) &= \left(\frac{\pi'_{2t}, \alpha_{2t_1+1}\alpha_k^{m_k}}{\mathfrak{p}'_{2t_1+1}} \right)^{-1} \left(\frac{\pi'_{2t}, \alpha_{2t_1+1}\alpha_k^{m_k}}{\mathfrak{p}'_k} \right)^{-1} \\ &= \left(\frac{\pi'_{2t}, \pi'_{2t_1+1}}{\mathfrak{p}'_{2t_1+1}} \right)^{-1} \left(\frac{\pi'_{2t}, \pi'_k}{\mathfrak{p}'_k} \right)^{-m_k} \end{aligned}$$

If we write

$$\left(\frac{\pi'_{2t}, \pi'_{2t_1+1}}{\mathfrak{p}'_{2t_1+1}} \right)^{-1} \left(\frac{\pi'_{2t}, \pi'_k}{\mathfrak{p}'_k} \right)^{-m_k} = \omega^{b_k}$$

for $2t_1 + 1 < k \leq 2t - 2$, we get the following equations:

$$a_{2t,2t_1+1}\lambda_{2t_1+1} + a_{2t,k}\lambda_k m_k \equiv b_k \pmod{3}$$

and using the relation $\lambda_j \nu_j = r$ for all j , as well as $\nu_j^2 \equiv 1 \pmod{3}$ since $\nu_j \in \{1, 2\}$,

$$\nu_{2t_1+1} r a_{2t, 2t_1+1} + \nu_k m_k r a_{2t, k} \equiv b_k \pmod{3}.$$

By Hilbert reciprocity, we also have the property that

$$\sum_{j=1}^{2t-1} a_{2t, j} = 0$$

and so we have an additional relation:

$$r a_{2t, 2t_1+1} + \cdots + r a_{2t, 2t-1} = - \sum_{j=1}^{2t_1} r a_{2t, j}.$$

Let

$$b = - \sum_{j=1}^{2t_1} r a_{2t, j}.$$

Then in total we have the following system of equations over \mathbb{F}_3 :

$$\begin{pmatrix} \nu_{2t_1+1} & \nu_{2t_1+2} m_{2t_1+2} & 0 & \cdots & 0 \\ \nu_{2t_1+1} & 0 & \nu_{2t_1+3} m_{2t_1+3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \nu_{2t_1+1} & 0 & 0 & \cdots & \nu_{2t-1} m_{2t-1} \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \begin{pmatrix} r a_{2t, 1} \\ r a_{2t, 2} \\ \vdots \\ r a_{2t, 2t-2} \\ r a_{2t, 2t-1} \end{pmatrix} = \begin{pmatrix} b_{2t_1+2} \\ b_{2t_1+3} \\ \vdots \\ b_{2t-1} \\ b \end{pmatrix}$$

This system has a unique solution if the determinant of the matrix is non-zero.

Note that since $\nu_k, m_j \in \{1, 2\}$,

$$\begin{aligned}
& \begin{pmatrix} \nu_{2t_1+1} & \nu_{2t_1+2}m_{2t_1+2} & 0 & \dots & 0 \\ \nu_{2t_1+1} & 0 & \nu_{2t_1+3}m_{2t_1+3} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \nu_{2t_1+1} & 0 & 0 & \dots & \nu_{2t_1-1}m_{2t_1-1} \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix} \\
& \sim \begin{pmatrix} \nu_{2t_1+1}\nu_{2t_1+2}m_{2t_1+2} & 1 & 0 & \dots & 0 \\ \nu_{2t_1+1}\nu_{2t_1+3}m_{2t_1+3} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \nu_{2t_1+1}\nu_{2t_1-1}m_{2t_1-1} & 0 & 0 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix} \\
& \sim \begin{pmatrix} \nu_{2t_1+1}\nu_{2t_1+2}m_{2t_1+2} & 1 & 0 & \dots & 0 \\ \nu_{2t_1+1}\nu_{2t_1+3}m_{2t_1+3} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \nu_{2t_1+1}\nu_{2t_1-1}m_{2t_1-1} & 0 & 0 & \dots & 1 \\ 1 - \sum_{k=2t_1+2}^{2t-1} \nu_{2t_1+1}\nu_k m_k & 0 & 0 & \dots & 0 \end{pmatrix}
\end{aligned}$$

which has determinant

$$1 - \sum_{k=2t_1+2}^{2t-1} \nu_{2t_1+1}\nu_k m_k.$$

Now recall that $w_j = v_{\mathfrak{p}'_{2t}}(\alpha_j)$. By definition $w_j = 0$ for $1 \leq j \leq 2t_1$. We know $v_{\mathfrak{p}'_{2t}}(\alpha_{2t_1+1}\alpha_k^{m_k}) = 0$ for $2t_1 + 2 \leq k \leq 2t - 1$ since \mathfrak{p}'_{2t} does not ramify in

$K'(\sqrt[3]{\alpha_{2t_1+1}\alpha_k^{m_k}})$, and therefore

$$w_{2t_1+1} + m_k w_k = 0 \implies w_k = -m_k w_{2t_1+1}$$

for $2t_1 + 2 \leq k \leq 2t - 1$. Furthermore,

$$v_{\mathfrak{p}_{2t}}(\alpha) = \sum_{k=1}^{2t-1} \nu_k w_k \neq 0.$$

Then using the fact that $\nu_j^2 \equiv 1 \pmod{3}$,

$$\begin{aligned} 0 \not\equiv \sum_{k=1}^{2t-1} \nu_k w_k &= \sum_{k=2t_1+1}^{2t-1} \nu_k w_k = \nu_{2t_1+1} w_{2t_1+1} - \sum_{k=2t_1+2}^{2t-1} \nu_k m_k w_{2t_1+1} \\ &\equiv w_{2t_1+1} \nu_{2t_1+1} \left(1 - \sum_{k=2t_1+2}^{2t-1} \nu_{2t_1+1} \nu_k m_k\right) \pmod{3}, \end{aligned}$$

and so the determinant of the matrix is non-zero. We can therefore solve the system of equations to determine $a_{2t,j}$ for all j .

At this point, we know how to find the entries of the matrix from Theorem 3.5 in both the $e = 0$ and $e = 1$ cases, and so we can determine the 3-rank for a given extension (see the example in §3.4).

In the next section, we will show that the entries of the matrix are not completely independent, leading to symmetries in the matrix structure. These symmetries will be used in Chapter 6 where we develop a heuristic model for the ranks of the class groups.

3.3 Symmetries

Recall that we're considering cyclic cubic extensions of $K = \mathbb{Q}(\zeta_8)$. Let σ be a non-trivial element of $\text{Gal}(K/\mathbb{Q})$ which fixes $\mathbb{Q}(i)$. Then there are two primes in K lying over every rational prime congruent to 3 mod 4: \mathfrak{p}_n and \mathfrak{p}_n^σ . Let \mathfrak{p}'_{2n+1} and \mathfrak{p}'_{2n+2} be primes of $K' = K(\sqrt{-3})$ above \mathfrak{p}_n and \mathfrak{p}_n^σ respectively.

3.3.1 Columns corresponding to type 1 primes.

Let $0 \leq m \leq t-1$ and $0 \leq n \leq t_1-1$. Then we have

$$\omega^{ra_{2m+1,2n+1}} = \left(\frac{\pi'_{2m+1}, \pi'_{2n+1}}{\mathfrak{p}'_{2m+1}} \right)^{-\nu_{2n+1}}.$$

Apply σ , a non-trivial element of $\text{Gal}(K/\mathbb{Q})$ which fixes $\mathbb{Q}(i)$, to both sides.

We may also assume that σ fixes the cube roots of unity.

Lemma 3.8. $\nu_{2n+1} = \nu_{2n+2}$.

Proof. The proof is identical to that of Lemma 2.4. □

$$\begin{aligned} \omega^{ra_{2m+1,2n+1}} &= \sigma(\omega^{ra_{2m+1,2n+1}}) = \left(\frac{\pi'^{\sigma}_{2m+1}, \pi'^{\sigma}_{2n+1}}{\mathfrak{p}'^{\sigma}_{2n+1}} \right)^{-\nu_{2n+1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}} \\ &= \omega^{ra_{2m+2,2n+2}}. \end{aligned}$$

By the same reasoning,

$$\omega^{ra_{2m+1,2n+2}} = \omega^{ra_{2m+2,2n+1}}.$$

Therefore for $0 \leq m \leq t-1$ and $0 \leq n \leq t_1-1$,

$$a_{2m+1,2n+1} = a_{2m+2,2n+2}, \quad a_{2m+1,2n+2} = a_{2m+2,2n+1}.$$

Therefore if we consider just the columns corresponding to type 1 primes, our matrix has blocks of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

3.3.2 Columns corresponding to type 2 primes.

First, we prove the following lemma. Recall that $w_j = v_{p_{2t}}(\alpha_j) \neq 0$ for $2t_1+1 \leq j \leq 2t-1$.

Lemma 3.9. *For $t_1 \leq n < t-1$, $w_{2n+1} + w_{2n+2} \equiv 0 \pmod{3}$.*

Proof. We prove that $w_1 + w_2 \equiv 0 \pmod{3}$; the result can easily be extended to $w_{2n+1} + w_{2n+2}$. We define α as

$$\alpha = \prod_{j=1}^{2t-1} \alpha_j^{\nu_j}.$$

Each set of $\{\nu_j\}$ gives a different extension, independent of the values of w_j .

We require the ramified primes to be congruent to 1 mod 3. Then there are 2^{t-1} cyclic cubic number fields \hat{L}/\mathbb{Q} in which the ramified primes are p_1, \dots, p_t (see

Chapter 3 of [27]).

Recall that $\nu_j \neq 0$, since otherwise \mathfrak{p}'_j won't ramify, and we choose α such that $\nu_1 = 1$. Recall also that conjugate primes have the same valuation by Lemma 3.8.

Therefore we can pick values for

$$\nu_1, \nu_3, \dots, \nu_{2t-1},$$

and then $\nu_{2j+1} = \nu_{2j+2}$ for $0 \leq j \leq t-2$. So there are 2^{t-1} choices for the $\{\nu_j\}$, since $\nu_j \in \{1, 2\}$ and each choice of $\{\nu_j\}$ gives a different α . Therefore the 2^{t-1} choices for $\{\nu_j\}$ correspond exactly to the 2^{t-1} extensions $K'(\sqrt[3]{\alpha})/K'$ which are lifts of the cubic number fields \hat{L}/\mathbb{Q} .

For each obtained α we have $v_{\mathfrak{p}'_{2t}}(\alpha) \neq 0$ since \mathfrak{p}'_{2t} ramifies in $K'(\sqrt[3]{\alpha})/K'$.

Then

$$v_{\mathfrak{p}'_{2t}}(\alpha) = \sum_{j=1}^{2t-1} \nu_j v_{\mathfrak{p}'_{2t}}(\alpha_j) = \sum_{j=1}^{2t-1} \nu_j w_j \not\equiv 0 \pmod{3}.$$

Now let's consider particular extensions where we have chosen $\nu_j = 1$ for $1 \leq j < 2t - 1$. Then we have the equation

$$\nu_{2t-1} w_{2t-1} + \sum_{j=1}^{2t-2} w_j \not\equiv 0 \pmod{3}.$$

We need this equations to hold (i.e. be non-zero) for either possible value of ν_{2t-1} .

This means

$$w_{2t-1} + \sum_{j=1}^{2t-2} w_j \not\equiv 0 \pmod{3},$$

$$2w_{2t-1} + \sum_{j=1}^{2t-2} w_j \not\equiv 0 \pmod{3}.$$

The first equation tells us that $\sum_{j=1}^{2t-2} w_j \not\equiv 2w_{2t-1} \pmod{3}$ and the second equation tells us that $\sum_{j=1}^{2t-2} w_j \not\equiv w_{2t-1} \pmod{3}$. Since $w_{2t-1} \neq 0$, this implies that

$$\sum_{j=1}^{2t-2} w_j \equiv 0 \pmod{3}.$$

Now consider other extensions where we have chosen $\nu_1 = \nu_2 = 1$ and $\nu_j = 2$ for $2 < j < 2t - 1$. Then we have

$$\nu_{2t-1}w_{2t-1} + w_1 + w_2 + 2 \sum_{j=3}^{2t-2} w_j \not\equiv 0 \pmod{3}.$$

Then

$$\sum_{j=1}^{2t-2} w_j \equiv 0 \pmod{3} \implies 2w_1 + 2w_2 + 2 \sum_{j=3}^{2t-2} w_j \equiv 0 \pmod{3}.$$

Therefore we have

$$\begin{aligned} \nu_{2t-1}w_{2t-1} + w_1 + w_2 + 2 \sum_{j=3}^{2t-2} w_j &\equiv \nu_{2t-1}w_{2t-1} + 2w_1 + 2w_2 \pmod{3} \\ &\not\equiv 0 \pmod{3}. \end{aligned}$$

Again this equation must hold for either possible value of ν_{2t-1} .

$$\nu_{2t-1} = 1 \implies w_{2t-1} + 2w_1 + 2w_2 \not\equiv 0 \pmod{3}$$

$$\nu_{2t-1} = 2 \implies 2w_{2t-1} + 2w_1 + 2w_2 \not\equiv 0 \pmod{3}$$

Since $w_{2t-1} \neq 0$, we must have $2w_1 + 2w_2 \equiv 0 \pmod{3} \implies w_1 + w_2 \equiv 0 \pmod{3}$.

□

We now need the following lemma.

Lemma 3.10. *We may assume $w_{2t-1} = 1$.*

Proof. First, recall that we can also decompose α as

$$\alpha = \alpha_1 \alpha_2 \alpha_3^{\nu_3} \dots \alpha_{2t-1}^{\nu_{2t-1}}$$

recalling that $\nu_{2j+1} = \nu_{2j+2}$.

We also know that the generator of $\text{Gal}(K'/K) = \text{Gal}(K(\omega)/K)$ acts trivially on the generator of $\text{Gal}(L'/K')$ and acts by inversion on ω . Therefore by the Kummer pairing, the generator of $\text{Gal}(K'/K)$ acts by inversion on the Kummer generator modulo cubes.

Therefore if we let $\mathfrak{p}'_i, \bar{\mathfrak{p}}'_i$ be the two primes of K' lying over $\mathfrak{p}_i \in K$, the Kummer generator α generates an ideal of the form

$$\mathfrak{p}_1^{m_1} \bar{\mathfrak{p}}_1^{-n_1} \mathfrak{p}_2^{m_2} \bar{\mathfrak{p}}_2^{-n_2} \dots \mathfrak{p}_{2t-1}^{m_{2t-1}} \bar{\mathfrak{p}}_{2t-1}^{-n_{2t-1}} \mathfrak{p}_{2t}^{m_{2t}} \bar{\mathfrak{p}}_{2t}^{-n_{2t}}$$

where ν is determined by the decomposition of α .

Then since $v_{\mathfrak{p}'_i}(\alpha_i) = 1$ and $v_{\mathfrak{p}'_i}(\alpha_j) = 0$ for $j \neq i$, for $2t_1 + 1 \leq j \leq 2t - 1$, we must have

$$\alpha_j = \mathfrak{p}'_j \bar{\mathfrak{p}}_j'^2 \mathfrak{p}'_{2t} \bar{\mathfrak{p}}_{2t}'^2 \quad \text{or} \quad \alpha_j = \mathfrak{p}'_j \bar{\mathfrak{p}}_j'^2 \mathfrak{p}'_{2t} \bar{\mathfrak{p}}_{2t}'$$

We choose the prime \mathfrak{p}'_{2t} in K' lying over \mathfrak{p}_{2t} to be the one such that

$$v_{\mathfrak{p}'_{2t}}(\alpha_{2t-1}) = 1.$$

Therefore $w_{2t-1} = 1$. □

Now let's return to the symbols we compute to construct our matrix. For $0 \leq m \leq t - 1$ and $t_1 + 1 \leq n < t - 1$,

$$\omega^{ra_{2m+1,2n+1}} = \left(\frac{\pi'_{2m+1}, \pi'_{2n+1}}{\mathfrak{p}'_{2n+1}} \right)^{-\nu_{2n+1}} \left(\frac{\pi'_{2m+1}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_{2n+1}\nu_{2n+1}}.$$

Then, by applying σ , and since $\nu_{2n+1} = \nu_{2n+2}$,

$$\begin{aligned} \omega^{ra_{2m+1,2n+1}} &= \sigma(\omega^{ra_{2m+1,2n+1}}) = \left(\frac{\pi'^\sigma_{2m+1}, \pi'^\sigma_{2n+1}}{\mathfrak{p}'^\sigma_{2n+1}} \right)^{-\nu_{2n+1}} \left(\frac{\pi'^\sigma_{2m+1}, \pi'^\sigma_{2t}}{\mathfrak{p}'^\sigma_{2t}} \right)^{-w_{2n+1}\nu_{2n+1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-w_{2n+1}\nu_{2n+1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}} \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-w_{2n+1}\nu_{2n+2}} \end{aligned} \tag{3.1}$$

We also have

$$\omega^{ra_{2m+2,2n+2}} = \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_{2n+2}\nu_{2n+2}} \quad (3.2)$$

and

$$\omega^{ra_{2m+2,2t-1}} = \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_{2t-1}\nu_{2t-1}} \quad (3.3)$$

Now we take powers of the elements in equations 3.2 and 3.3 and find that it equals a power of the result of 3.1.

We use the assumption that $w_{2t-1} = 1$ (Lemma 3.10). By Lemma 3.9,

$$\begin{aligned} & \omega^{r\nu_{2t-1}a_{2m+2,2n+2}} \omega^{rw_{2n+1}\nu_{2n+2}a_{2m+2,2t-1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_{2n+2}\nu_{2n+2}\nu_{2t-1}} \\ & \quad \times \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-w_{2n+1}\nu_{2n+2}\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_{2n+1}\nu_{2n+2}\nu_{2t-1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-w_{2n+2}\nu_{2n+2}\nu_{2t-1}} \\ & \quad \times \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-w_{2n+1}\nu_{2n+2}\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{w_{2n+2}\nu_{2n+2}\nu_{2t-1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-w_{2n+1}\nu_{2n+2}\nu_{2t-1}} \end{aligned}$$

We also have

$$\begin{aligned} & \omega^{r\nu_{2t-1}a_{2m+1,2n+1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2n+2}}{\mathfrak{p}'_{2n+2}} \right)^{-\nu_{2n+2}\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-w_{2n+1}\nu_{2n+2}\nu_{2t-1}}. \end{aligned}$$

Therefore

$$\omega^{r\nu_{2t-1}a_{2m+2,2n+2}} \omega^{rw_{2n+1}\nu_{2n+2}a_{2m+2,2t-1}} = \omega^{r\nu_{2t-1}a_{2m+1,2n+1}}$$

and so for $0 \leq m \leq t-1$ and $t_1 \leq n < t-1$,

$$\nu_{2t-1}a_{2m+1,2n+1} = \nu_{2t-1}a_{2m+2,2n+2} + w_{2n+1}\nu_{2n+2}a_{2m+2,2t-1}.$$

Multiplying both sides by ν_{2t-1} , we have

$$a_{2m+1,2n+1} = a_{2m+2,2n+2} + \nu_{2t-1}w_{2n+1}\nu_{2n+2}a_{2m+2,2t-1}$$

By a very similar argument,

$$a_{2m+2,2n+1} = a_{2m+1,2n+2} + \nu_{2t-1}w_{2n+1}\nu_{2n+2}a_{2m+1,2t-1}.$$

This gives us relations as follows:

$$a_{11} = a_{22} + \nu_{2t-1} w_1 \nu_2 a_{2,2t-1}$$

$$a_{21} = a_{12} + \nu_{2t-1} w_1 \nu_2 a_{1,2t-1}$$

$$a_{31} = a_{42} + \nu_{2t-1} w_1 \nu_2 a_{4,2t-1}$$

$$a_{41} = a_{32} + \nu_{2t-1} w_1 \nu_2 a_{3,2t-1}$$

\vdots

But we can add a multiple of a column to another column in a matrix without changing its rank. For example, we could add

$$\nu_{2t-1} w_1 \nu_2$$

times the $2t - 1$ column of the matrix to column 2, and then in our new matrix we'd have the relations

$$a_{11} = a_{22}$$

$$a_{21} = a_{12}$$

$$a_{31} = a_{42}$$

$$a_{41} = a_{32}$$

\vdots

In general, we can add

$$\nu_{2t-1} w_{2n+1} \nu_{2n+2}$$

times the the $2t - 1$ column of the matrix to column $2n + 2$ to get a new matrix with the relations

$$a_{2m+1,2n+1} = a_{2m+2,2n+2}, \quad a_{2m+2,2n+1} = a_{2m+1,2n+2}.$$

Therefore we know that this portion of the matrix is equivalent to one composed of blocks of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

Recall that we had a slightly different construction for the last row. However, ultimately the matrix structure is independent of which prime is considered the ‘special prime’. We chose the last prime, and created Kummer extensions in which \mathfrak{p}_i and \mathfrak{p}_{2t} ramified for $i < 2t$ and \mathfrak{p}_i a type 2 prime. However, we could just as easily have chosen \mathfrak{p}_{2t-1} to be the extra prime, and that choice would not alter the structure of the matrix.

Therefore the symmetric block structure should be present in all columns corresponding to type 2 primes except for the last column, since we have an odd number of columns.

However, we do have a symmetry present in the last column of the matrix as

well. Since

$$\begin{aligned}\sigma(\omega^{ra_{2m+1,2t-1}}) &= \omega^{ra_{2m+1,2t-1}} = \left(\frac{\pi'_{2m+1}{}^\sigma, \pi'_{2t-1}{}^\sigma}{\mathfrak{p}'_{2t-1}{}^\sigma} \right)^{-\nu_{2t-1}} \left(\frac{\pi'_{2m+1}{}^\sigma, \pi'_{2t}{}^\sigma}{\mathfrak{p}'_{2t}{}^\sigma} \right)^{-\nu_{2t-1}} \\ &= \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-\nu_{2t-1}}\end{aligned}$$

and

$$\omega^{ra_{2m+2,2t-1}} = \left(\frac{\pi'_{2m+2}, \pi'_{2t-1}}{\mathfrak{p}'_{2t-1}} \right)^{-\nu_{2t-1}} \left(\frac{\pi'_{2m+2}, \pi'_{2t}}{\mathfrak{p}'_{2t}} \right)^{-\nu_{2t-1}},$$

we have

$$a_{2m+1,2t-1} = a_{2m+2,2t-1}.$$

3.3.3 Row corresponding to the extra generator

In the case where there is an ambiguous ideal class which is not strongly ambiguous, we have an additional generator \mathfrak{P}'_0 , which corresponds to an additional row at the top of the matrix. However, because only one additional generator is required, and not a pair of Galois conjugates, there are no symmetries present in this row (although we still have the condition that the coefficients of the row sum to zero mod 3).

3.3.4 Matrix structure

Therefore if $t = t_1$ and we require an additional generator for the ambiguous ideal classes,

$$M = \left(\begin{array}{c} M_1 \\ \hline M_2 \end{array} \right)$$

where M_1 is a $1 \times 2t$ matrix with no symmetries and M_2 is a $2t \times 2t$ matrix of blocks of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}.$$

If $t = t_1$ and we don't need an additional generator, then

$$M = M_2.$$

Otherwise, for $t_2 > 0$, which means the unit of K_1 is not the norm of an element, we do not require an additional generator (we don't need to worry about the strong/weak distinction). Therefore we can perform elementary row operations to obtain

$$M = \left(M_1 \mid M_2 \right)$$

where M_1 is a $2t \times (2t - 2)$ matrix of blocks of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

and M_2 is a $2t \times 1$ matrix of blocks of the form

$$\begin{pmatrix} c \\ c \end{pmatrix}.$$

3.4 An example

Let L be a cyclic cubic extension of $K = \mathbb{Q}(\zeta_8)$ such that only primes above 31 and 1447 ramify. Both primes are inert in $\mathbb{Q}(i)/\mathbb{Q}$ and split in $\mathbb{Q}(\zeta_8)/\mathbb{Q}(i)$.

Primes above 31 are type 2 and primes above 1447 are type 1. Since not all primes are type 1, $e = 1$ and we do not need to worry about finding an additional generator for A^Δ , since all ambiguous classes are strongly ambiguous.

We lift to L'/K' where $K' = K(\omega)$ so that we can compute Hilbert symbols using the equation for tamely ramified symbols.

There are two primes in K lying over 31, \mathfrak{p}_{31} and $\bar{\mathfrak{p}}_{31}$, and two primes in K lying over 1447, \mathfrak{p}_{1447} and $\bar{\mathfrak{p}}_{1447}$.

We can decompose α as

$$\alpha = \alpha_{1447} \bar{\alpha}_{1447} \alpha_{31}^{\nu_{31}}$$

where $K'(\sqrt[3]{\alpha_{1447}})$ is the extension in which only \mathfrak{p}_{1447} ramifies, $K'(\sqrt[3]{\bar{\alpha}_{1447}})$ is the extension in which only $\bar{\mathfrak{p}}_{1447}$ ramifies, and $K'(\sqrt[3]{\alpha_{31}})$ is the extension in which \mathfrak{p}_{31} and $\bar{\mathfrak{p}}_{31}$ both ramify. We can assume $\nu_{1447} = \bar{\nu}_{1447} = 1$. For ease of notation, let

$\nu = \nu_{13}$. Then the matrix as described above is

$$M = \begin{pmatrix} -1 - \nu & 1 & \nu \\ 1 & -1 - \nu & \nu \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Since $\nu \in \{1, 2\}$, we have two possible matrices, one of rank 1 and one of rank 2:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Since $e = 1$, the class groups of the fields have 3-rank

$$4 - \text{rank } M,$$

and so the matrices above correspond to 3-rank 3 and 2 respectively.

By looking for subfields of composite fields (as in §2.3), we can find two cyclic cubic extensions L/K in which primes above 31 and 1447 ramify:

$$f_1 = x^3 - 2956x^2 + 2852836x - 903305544$$

$$f_2 = x^3 - 2956x^2 + 2852836x - 893975288.$$

The field corresponding to f_1 has 3-class group $(\mathbb{Z}/3\mathbb{Z})^3$ and the one corresponding to f_2 has 3-class group $(\mathbb{Z}/3\mathbb{Z})^2$.

We can also find Kummer generators explicitly.

$$\alpha_{1447} = ((237i/4 + 237/4)\sqrt{2} - 93i - 93)\sqrt{-3} + (-283i/4 - 283/4)\sqrt{2} + 166i + 166$$

$$\bar{\alpha}_{1447} = ((237i/4 + 237/4)\sqrt{2} + 93i + 93)\sqrt{-3} + (-283i/4 - 283/4)\sqrt{2} - 166i - 166$$

$$\alpha_{31} = 93\sqrt{3} + 62i$$

Then the field given by f_1 has Kummer generator

$$\alpha = \alpha_{1447}\bar{\alpha}_{1447}\alpha_{31}.$$

The field given by f_2 has Kummer generator

$$\alpha = \alpha_{1447}\bar{\alpha}_{1447}\alpha_{31}^2.$$

f_1 corresponds to the first matrix and f_2 to the second.

Chapter 4: Galois structure of units

4.1 Units of K_1 and L_1

In this section, we present some results concerning the units in $K_1 = \mathbb{Q}(\zeta_8)$. We let L_1/K_1 be a cyclic field of degree p . We first prove that if all of the ramified primes lie over rational primes that are congruent to 3 mod 8, then the fundamental unit of K_1 , $\sqrt{2}+1$, is the norm of a unit in L_1 . We then consider the Galois structure of the units in L_1 . Specifically, we determine that there are two possible structures for the units mod p^{th} powers. Then, we prove that this structure determines if the unit in K_1 is the norm of a unit in L_1 .

4.1.1 Units as norms of units

We start with the following proposition.

Proposition 4.1. *Let $K_1 = \mathbb{Q}(\zeta_8)$ and let L_1 be a cyclic degree p extension such that $\text{Gal}(L_1/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}^2 \times \mathbb{Z}/p\mathbb{Z}$. Let p_1, \dots, p_t be the rational primes below the primes that ramify in L_1/K_1 . If $p_i \equiv 3 \pmod{8}$ for all i , then the fundamental unit of K_1 is the norm of a unit in L_1 .*

Proof. Let $P = p_1 \dots p_t$. Then since L_1 is the lift of an abelian degree p number field,

$L_1 \subseteq \mathbb{Q}(\zeta_{8P})$. Then $1 - \zeta_{8P}$ is a unit in $\mathbb{Q}(\zeta_{8P})$, and therefore $N_{\mathbb{Q}(\zeta_{8P})/L_1}(1 - \zeta_{8P})$ is a unit in L_1 . We will now show that $N_{L_1/\mathbb{Q}(\zeta_8)}N_{\mathbb{Q}(\zeta_{8P})/L_1}(1 - \zeta_{8P})$ is the fundamental unit of K_1 . First, note that

$$N_{L/\mathbb{Q}(\zeta_8)}N_{\mathbb{Q}(\zeta_{8P})/L_1}(1 - \zeta_{8P}) = N_{\mathbb{Q}(\zeta_{8P})/\mathbb{Q}(\zeta_8)}(1 - \zeta_{8P}) = \prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b).$$

We also know that

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8}}} (1 - \zeta_{8P}^b) = 1 - \zeta_8.$$

Therefore we can evaluate the norm by letting b run over all numbers which are $1 \pmod{8}$, then dividing by the terms which are divisible by each p_i , and then modifying the numerator and denominator as needed to remove the values which were over-counted.

For example, if only two primes ramify, so $P = p_1 p_2$, we could evaluate the norm as

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b) = \frac{\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8}}} (1 - \zeta_{8P}^b) \prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8}}} (1 - \zeta_{8P}^b)}{\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ p_1 | b}} (1 - \zeta_{8P}^b) \prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ p_2 | b}} (1 - \zeta_{8P}^b)}$$

The values of b in the numerator are divisible by an even number of the p_i and the values of b in the denominator are divisible by an odd number of the p_i .

Consider the case where we want to evaluate one of the products above, where

exactly n primes divide b : call them p_1, \dots, p_n . If n is odd, then since $p_i \equiv 3 \pmod{8}$ for all i , $p_1 \dots p_n \equiv 3 \pmod{8}$. Write

$$b = kp_1 \dots p_n.$$

Since $p_1 \dots p_n \equiv 3 \pmod{8}$, we must have $k \equiv 3 \pmod{8}$ to ensure that $b \equiv 1 \pmod{8}$.

Therefore

$$\begin{aligned} \prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ p_1 \dots p_n | b}} (1 - \zeta_{8P}^b) &= \prod_{j=0}^{P/(p_1 \dots p_n) - 1} (1 - \zeta_{8P}^{(8j+3)p_1 \dots p_n}) \\ &= \prod_{j=0}^{P/(p_1 \dots p_n) - 1} (1 - \zeta_{P/(p_1 \dots p_n)}^j \zeta_{8P/(p_1 \dots p_n)}^3) \\ &= 1 - \zeta_8^3 \end{aligned}$$

On the other hand, if n is even, then $p_1 \dots p_n \equiv 1 \pmod{8}$. If we again write

$$b = kp_1 \dots p_n,$$

then we must have $k \equiv 1 \pmod{8}$. Therefore we have

$$\begin{aligned}
\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ p_1 \dots p_n | b}} (1 - \zeta_{8P}^b) &= \prod_{j=0}^{P/(p_1 \dots p_n) - 1} (1 - \zeta_{8P}^{(8j+1)p_1 \dots p_n}) \\
&= \prod_{j=0}^{P/(p_1 \dots p_n) - 1} (1 - \zeta_{P/(p_1 \dots p_n)}^j \zeta_{8P/(p_1 \dots p_n)}) \\
&= 1 - \zeta_8
\end{aligned}$$

Let $G_n = \{b | 1 \leq b < 8P, b \equiv 1 \pmod{8}, \text{ exactly } n \text{ primes } p_i \text{ divide } b\}$. Then

since

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8}}} (1 - \zeta_{8P}^b) = 1 - \zeta_8,$$

we have, if t is even,

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b) = \frac{(1 - \zeta_8) (\prod_{b \in G_2} 1 - \zeta_{8P}^b) (\prod_{b \in G_4} 1 - \zeta_{8P}^b) \dots (\prod_{b \in G_t} 1 - \zeta_{8P}^b)}{(\prod_{b \in G_1} 1 - \zeta_{8P}^b) (\prod_{b \in G_3} 1 - \zeta_{8P}^b) \dots (\prod_{b \in G_{t-1}} 1 - \zeta_{8P}^b)}$$

and if t is odd,

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b) = \frac{(1 - \zeta_8) (\prod_{b \in G_2} 1 - \zeta_{8P}^b) (\prod_{b \in G_4} 1 - \zeta_{8P}^b) \dots (\prod_{b \in G_{t-1}} 1 - \zeta_{8P}^b)}{(\prod_{b \in G_1} 1 - \zeta_{8P}^b) (\prod_{b \in G_3} 1 - \zeta_{8P}^b) \dots (\prod_{b \in G_t} 1 - \zeta_{8P}^b)}.$$

Consider one of the products above:

$$\prod_{b \in G_n} (1 - \zeta_{8P}^b).$$

Here, exactly n of the primes p_1, \dots, p_t divide b . There are $\binom{t}{n}$ ways to choose the n primes. The value of the product does not depend on which primes are chosen, so

$$\prod_{b \in G_n} (1 - \zeta_{8P}^b) = \left(\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ p_1 \dots p_n | b}} (1 - \zeta_{8P}^b) \right)^{\binom{t}{n}}$$

All products in the numerator have even n and all products in the denominator have odd n , and above we've shown that

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ p_1 \dots p_n | b}} (1 - \zeta_{8P}^b) = \begin{cases} 1 - \zeta_8^3 & \text{if } n \text{ is odd} \\ 1 - \zeta_8 & \text{if } n \text{ is even} \end{cases}.$$

So if t is even, we have

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b) = \frac{(1 - \zeta_8)(1 - \zeta_8)^{\binom{t}{2}}(1 - \zeta_8)^{\binom{t}{4}} \dots (1 - \zeta_8)^{\binom{t}{t}}}{(1 - \zeta_8^3)^{\binom{t}{1}}(1 - \zeta_8^3)^{\binom{t}{3}} \dots (1 - \zeta_8^3)^{\binom{t}{t-1}}}$$

and if t is odd,

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b) = \frac{(1 - \zeta_8)(1 - \zeta_8)^{\binom{t}{2}}(1 - \zeta_8)^{\binom{t}{4}} \dots (1 - \zeta_8)^{\binom{t}{t-1}}}{(1 - \zeta_8^3)^{\binom{t}{1}}(1 - \zeta_8^3)^{\binom{t}{3}} \dots (1 - \zeta_8^3)^{\binom{t}{t}}}$$

Now we need two binomial identities:

$$\sum_{i=0}^t (-1)^i \binom{t}{i} = 0,$$

$$\sum_{i=0}^t \binom{t}{i} = 2^t$$

Therefore

$$\sum_{i=0}^{t/2} \binom{t}{2i} = \sum_{i=0}^{t/2} \binom{t}{2i+1} = 2^{t-1}.$$

Therefore (regardless if t is even or odd) we have

$$\prod_{\substack{1 \leq b < 8P \\ b \equiv 1 \pmod{8} \\ (b, P) = 1}} (1 - \zeta_{8P}^b) = \frac{(1 - \zeta_8)^{2^{t-1}}}{(1 - \zeta_8^3)^{2^{t-1}}}.$$

Since $\frac{(1-\zeta_8)}{(1-\zeta_8^3)} = \zeta_8^{-1}(\sqrt{2} - 1)$, then

$$N_{\mathbb{Q}(\zeta_{8P})/\mathbb{Q}(\zeta_8)}(1 - \zeta_{8P}) = (\zeta_8^{-1}(\sqrt{2} - 1))^{2^{t-1}}$$

and therefore

$$N_{\mathbb{Q}(\zeta_{8P})/\mathbb{Q}(\zeta_8)}(1 - \zeta_{8P})^{-1} = (\zeta_8(\sqrt{2} + 1))^{2^{t-1}}.$$

Since L_1/K_1 is a degree $p \neq 2$ extension, this implies that $\sqrt{2} + 1$ is the norm of a unit in L_1 .

□

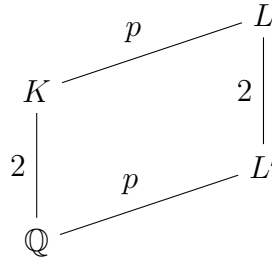
4.1.2 Galois module structure

Recall that the fundamental unit of K_1 is $\sqrt{2} + 1$. Therefore, up to roots of unity, the unit group of $K_1 = \mathbb{Q}(\zeta_8)$ equals the unit group of its maximal real subfield, $K = \mathbb{Q}(\sqrt{2})$. If we want to determine the structure of the units and

determine if the fundamental unit is the norm of a unit in L_1/K_1 , we can in fact consider L/K instead, the totally real cyclic degree p extension. We use the notation

$$\text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle.$$

Since $p \neq 2$, we are content to determine the units up to index 2. Therefore let E_L be the unit group of L modulo $\{\pm 1\}$ and let $E_K < E_L$ be the subgroup of units coming from K modulo $\{\pm 1\}$. L has $2p - 1$ fundamental units, one of which comes from K and $p - 1$ of which come from its real degree p subfield. Call the real degree p field L' and let $E_{L'} < E_L$ be the subgroup of units which come from L' modulo $\{\pm 1\}$. Finally, let U_K, U_L , and $U_{L'}$ be the units of K, L and L' , respectively, modulo p^{th} powers and $\{\pm 1\}$.



We let

$$G = \text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle.$$

Our goal is to prove a theorem about the structure of U_L . First, however, we need a few lemmas.

Lemma 4.2. $E_K E_{L'} = \ker((1 + \sigma)(1 + \sigma + \dots + \sigma^{p-1}))$.

Proof. First, note that clearly

$$E_K E_{L'} \subseteq \ker((1 + \sigma)(1 + \sigma + \dots + \sigma^{p-1}))$$

since $N_{K/\mathbb{Q}} = (1 + \sigma)$ and $N_{L'/\mathbb{Q}} = (1 + \sigma + \dots + \sigma^{p-1})$.

Now we tensor with \mathbb{C} . Since by [27, Lemma 5.27] we have a Minkowski unit that generates a subgroup of finite index, the dimension over \mathbb{C} will be the \mathbb{Z} -rank.

We have

$$\mathbb{C}[\sigma] \simeq \bigoplus_{\chi} \varepsilon_{\chi} \mathbb{C}[\sigma]$$

where $\{\chi\}$ are the characters and ε_{χ} are the idempotents. Then σ acts as $\chi(\sigma)$ on $\varepsilon_{\chi} \mathbb{C}[\sigma]$.

Therefore

$$(1 + \sigma)(1 + \sigma + \dots + \sigma^{p-1})$$

acts as

$$(1 + \chi(\sigma))(1 + \chi(\sigma) + \dots + \chi(\sigma)^{p-1}).$$

The possible values for $\chi(\sigma)$ are 1 (whose idempotent is essentially the norm and so is not present here), -1 , the $p - 1$ primitive p^{th} roots of unity, and the $p - 1$ primitive $(2p)^{\text{th}}$ roots of unity.

If $\chi(\sigma) = -1$, then

$$(1 + \chi(\sigma))(1 + \chi(\sigma) + \dots + \chi(\sigma)^{p-1}) = 0.$$

If $\chi(\sigma) = \zeta_p$, then again

$$(1 + \chi(\sigma))(1 + \chi(\sigma) + \dots + \chi(\sigma)^{p-1}) = 0.$$

If $\chi(\sigma) = \zeta_{2p}$, then since $\zeta_{2p} = -\zeta_p$,

$$(1 + \chi(\sigma))(1 + \chi(\sigma) + \dots + \chi(\sigma)^{p-1}) = (1 - \zeta_p)(1 - \zeta_p + \zeta_p^2 + \dots - \zeta_p^{p-1}) \neq 0.$$

Therefore the character values $\{-1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$ give the kernel. So the dimension of the kernel over \mathbb{C} is p and therefore the \mathbb{Z} -rank of the kernel is p .

Therefore $E_K E_{L'}$ is of a subgroup of finite index of the kernel. We now just need to show that the index is 1 and they are in fact equal.

Suppose ℓ is a prime dividing the index and suppose $e_K e_{L'} = \pm e^\ell$ for some

$$e \in \ker((1 + \sigma)(1 + \sigma + \dots + \sigma^{p-1})),$$

$e_K \in E_K$ and $e_{L'} \in E_{L'}$.

Now apply $1 + \sigma + \dots + \sigma^{p-1}$. Then

$$(1 + \sigma + \dots + \sigma^{p-1})e_K = e_K \cdot (\sigma + \sigma^2)e_K \cdot \dots \cdot (\sigma^{p-2} + \sigma^{p-1})e_K = \pm e_K$$

and

$$(1 + \sigma + \dots + \sigma^{p-1})e_{L'} = \pm 1.$$

So

$$e_K = \pm((1 + \sigma + \dots + \sigma^{p-1})e)^\ell.$$

If ℓ is odd, we don't need to worry about the ' \pm ' part. Consider the polynomial $x^\ell - e_K$. If e_K is not an ℓ^{th} power in K , then $x^\ell - e_K$ is irreducible and so there are no solutions in L (since L does not contain ℓ^{th} roots of unity). Therefore e_K is an ℓ^{th} power in K . If ℓ is odd, then $e_{L'}$ must also be an ℓ^{th} power in L (since $e_K e_{L'} = e^\ell$), which is only possible if $e_{L'}$ is an ℓ^{th} power in L' . Therefore

$$e_K e_{L'} \in (E_K E_{L'})^\ell$$

and therefore $e = e_K e_{L'}$.

If $\ell = 2$, let

$$\hat{e}_K = \pm e_K = ((1 + \sigma + \dots + \sigma^{p-1})e)^2.$$

If \hat{e}_K is not a square in K , then $x^2 - \hat{e}_K$ is irreducible which is impossible. Therefore \hat{e}_K is a square in K . Assume $\pm e_{L'}$ is a square in L but not in L' . Since $K = \mathbb{Q}(\sqrt{2})$,

$$L = L'(\sqrt{\pm e_{L'}}) = L'(\sqrt{2}).$$

Therefore $\pm e_{L'} = 2s^2$ for some $s \in L'$. Take a prime of L' that divides 2. Then the valuation of $e_{L'}$ at the prime must be trivial since it is a unit, but the valuation of $2s^2$ at the prime is odd (since the valuation of 2 must be either 1 or p). This is impossible.

Therefore not only are the ranks equal, but we have equality.

□

Let $R = (\mathbb{Z}/p\mathbb{Z})[G]$. Let Φ_n be the n^{th} cyclotomic polynomial.

Lemma 4.3. $U_K U_{L'} \simeq R/\Phi_2(\sigma)R \oplus R/\Phi_p(\sigma)R$.

Proof. We know

$$E_K \simeq \mathbb{Z}[\sigma]/(\sigma + 1)\mathbb{Z}[\sigma] = \mathbb{Z}[\sigma]/\Phi_2(\sigma)\mathbb{Z}[\sigma].$$

Then consider U_K , which is E_K modulo p^{th} powers. Then

$$U_K \simeq R/\Phi_2(\sigma)R.$$

Now we want to determine the structure of $U_{L'}$. First, note that

$$\mathbb{Z}[\sigma]/(\sigma^{p-1} + \dots + \sigma + 1)\mathbb{Z}[\sigma] = \mathbb{Z}[\sigma]/\Phi_p[\sigma]\mathbb{Z}[\sigma] \simeq \mathbb{Z}[\zeta_p]$$

acts on $E_{L'}$, and therefore by the structure theorem of finitely generated modules over Dedekind domains, $E_{L'}$ is isomorphic to an ideal I which is determined up to ideal class. Since the prime above p is principal, we may assume that I has index prime to p in $\mathbb{Z}[\zeta_p]$. Therefore

$$U_{L'} = E_{L'}/(p^{\text{th}} \text{ powers}) \simeq I/pI \simeq \mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p] \simeq R/\Phi_p(\sigma)R.$$

Then since $U_K U_{L'}$ is the direct sum of U_K and $U_{L'}$, we have

$$U_K U_{L'} \simeq R/\Phi_2(\sigma)R \oplus R/\Phi_p(\sigma)R.$$

□

Lemma 4.4. $U_L/U_K U_{L'} \simeq R/\Phi_{2p}(\sigma)R.$

Proof. First, note that the norm from L to \mathbb{Q} is

$$1 + \sigma + \dots + \sigma^{2p-1} = \Phi_2(\sigma)\Phi_p(\sigma)\Phi_{2p}(\sigma).$$

Therefore Φ_{2p} maps E_L into $\ker(\Phi_2(\sigma)\Phi_p(\sigma)) = E_K E_{L'}$ by Lemma 4.2. So

$$\mathbb{Z}[\sigma]/\Phi_{2p}[\sigma]\mathbb{Z}[\sigma] \simeq \mathbb{Z}[\zeta_p]$$

acts on $E_L/E_K E_{L'}$, and therefore again by the structure theorem of finitely generated modules over Dedekind domains, $E_L/E_K E_{L'}$ is isomorphic to an ideal I which is determined up to ideal class. The prime above p is principal, and therefore we may assume that I has index prime to p in $\mathbb{Z}[\zeta_p]$. Therefore

$$U_L/U_K U_{L'} \simeq I/pI \simeq \mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p] \simeq R/\Phi_{2p}(\sigma)R.$$

□

We're now ready to prove a theorem which gives us the structure of U_L as an

R -module.

Theorem 4.5. *Let $G = \text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$. Let $R = (\mathbb{Z}/p\mathbb{Z})[G]$. U_L has one of two possible structures over R :*

$$U_L \simeq \begin{cases} (R/(\sigma - 1)^{p-1}R) \oplus (R/(\sigma + 1)R) \oplus (R/(\sigma + 1)^{p-1}R) \text{ or} \\ (R/(\sigma - 1)^{p-1}R) \oplus (R/(\sigma + 1)^pR) \end{cases}$$

Proof. Over R , we have

$$\Phi_p(\sigma) \equiv (\sigma - 1)^{p-1}$$

$$\Phi_{2p}(\sigma) \equiv (\sigma + 1)^{p-1}$$

Therefore by Lemma 4.3,

$$U_K U_{L'} \simeq R/(\sigma + 1)R \oplus R/(\sigma - 1)^{p-1}R$$

and by Lemma 4.4,

$$U_L/U_K U_{L'} \simeq R/(\sigma + 1)^{p-1}R.$$

We have an exact sequence of the unit groups as

$$0 \rightarrow U_K U_{L'} \rightarrow U_L \rightarrow U_L/U_K U_{L'} \rightarrow 1.$$

This gives us the exact sequence

$$0 \rightarrow (R/(\sigma + 1)R) \oplus (R/(\sigma - 1)^{p-1}R) \rightarrow U_L \rightarrow (R/(\sigma + 1)^{p-1}R) \rightarrow 1.$$

We know that the norm

$$\Phi_2(\sigma)\Phi_p(\sigma)\Phi_{2p}(\sigma) = (\sigma - 1)^{p-1}(\sigma + 1)^p$$

annihilates U_L and so by looking at the characteristic polynomials, we can see that there are only two possibilities for U_L as an R -module. Either we have a split exact sequence

$$U_L \simeq U_K U_{L'} \oplus U_L / U_K U_{L'} \simeq R/(\sigma - 1)^{p-1}R \oplus R/(\sigma + 1)R \oplus R/(\sigma + 1)^{p-1}R$$

or we have

$$U_L \simeq R/(\sigma - 1)^{p-1}R \oplus R/(\sigma + 1)^pR.$$

□

When we develop a heuristic model in Chapter 6, we will also want the following result.

Proposition 4.6. *Let $G = \text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$. and let $R = (\mathbb{Z}/p\mathbb{Z})[G]$. Then $\text{Ext}_R^1(R/(\sigma + 1)R \oplus R/(\sigma - 1)^{p-1}R, R/(\sigma + 1)^{p-1}R) \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. We will treat the two summands in $R/(\sigma + 1)R \oplus R/(\sigma - 1)^{p-1}R$ separately.

We start with an exact sequence

$$0 \rightarrow R \xrightarrow{(\sigma+1)^{p-1}} R \rightarrow R/(\sigma+1)^{p-1}R \rightarrow 0.$$

Then we can use the exact sequence of Hom and Ext functors (see [15, Proposition 3F.11]):

$$\begin{aligned} \text{Hom}_R(R, R/(\sigma+1)R) &\xrightarrow{((\sigma+1)^{p-1})^*} \text{Hom}_R(R, R/(\sigma+1)R) \\ &\rightarrow \text{Ext}_R^1(R/(\sigma+1)^{p-1}, R/(\sigma+1)R) \rightarrow \text{Ext}_R^1(R, R/(\sigma+1)R). \end{aligned}$$

Since R is free, $\text{Ext}_R^1(R, R/(\sigma+1)R)$ is trivial. We also have

$$\text{Hom}_R(R, R/(\sigma+1)R) \simeq R/(\sigma+1)R,$$

and therefore we have the exact sequence

$$R/(\sigma+1)R \xrightarrow{((\sigma+1)^{p-1})^*} R/(\sigma+1)R \rightarrow \text{Ext}_R^1(R/(\sigma+1)^{p-1}, R/(\sigma+1)R) \rightarrow 0.$$

The image of $((\sigma+1)^{p-1})^*$ is trivial and therefore

$$\text{Ext}_R^1(R/(\sigma+1)^{p-1}, R/(\sigma+1)R) \simeq R/(\sigma+1)R \simeq \mathbb{Z}/p\mathbb{Z}.$$

Similarly, we can use the sequence induced by $\text{Hom}(-, R/(\sigma - 1)^{p-1}R)$.

$$R/(\sigma - 1)^{p-1}R \xrightarrow{((\sigma + 1)^{p-1})^*} R/(\sigma - 1)^{p-1}R \rightarrow \text{Ext}_R^1(R/(\sigma + 1)^{p-1}, R/(\sigma - 1)^{p-1}R) \rightarrow 0.$$

Then the map $((\sigma + 1)^{p-1})^*$ acts surjectively, and so we have

$$\text{Ext}_R^1(R/(\sigma + 1)^{p-1}, R/(\sigma - 1)^{p-1}R) = 0.$$

Therefore

$$\begin{aligned} & \text{Ext}_R^1(R/(\sigma + 1)R \oplus R/(\sigma - 1)^{p-1}R, R/(\sigma + 1)^{p-1}R) \\ &= \text{Ext}_R^1(R/(\sigma + 1)^{p-1}R, R/(\sigma + 1)R) \\ & \quad \oplus \text{Ext}_R^1(R/(\sigma + 1)^{p-1}R, R/(\sigma - 1)^{p-1}R) \\ &\simeq R/(\sigma + 1)R \\ &\simeq \mathbb{Z}/p\mathbb{Z}. \end{aligned}$$

□

Finally, we have the following result telling us if the unit is the norm of a unit.

Proposition 4.7. *Let L/K be as described preceding Theorem 4.5. Let $G = \text{Gal}(L/\mathbb{Q})$ and let $R = (\mathbb{Z}/p\mathbb{Z})[G]$. Then the fundamental unit of K is the norm of a unit in L if and only if U_L , the units of L modulo p^{th} powers and $\{\pm 1\}$, has the structure*

$$U_L \simeq R/(\sigma - 1)^{p-1}R \oplus R/(\sigma + 1)^pR.$$

Proof. The norm from L to K mod p^{th} powers is

$$\sigma^{2p-2} + \sigma^{2p-4} + \dots + \sigma^2 + 1 = (\sigma + 1)^{p-1}(\sigma - 1)^{p-1}.$$

Therefore the norm is non-trivial when

$$U_L \simeq R/(\sigma - 1)^{p-1}R \oplus R/(\sigma + 1)^pR$$

and trivial when

$$U_L \simeq R/(\sigma - 1)^{p-1}R \oplus R/(\sigma + 1)R \oplus R/(\sigma + 1)^{p-1}R.$$

□

4.2 Units of L_n/K_n

Let K_n be the n^{th} layer in the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$. Let L_n be a cyclic cubic extension of K_n , a lift of a cyclic cubic number field. In this section, we determine the Galois structure of the units of K_n . We use the structure to prove that a relative unit in K_n is the norm of an element in L_n modulo cubes if and only if all of the relative units in K_n are norms of elements in L_n modulo cubes. This result will be key to heuristics developed in Chapter 6.

4.2.1 Preliminaries

We first need some fundamental results.

Definition 4.8. *A skew circulant matrix is defined to be an $n \times n$ matrix of the form*

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ -a_{n-2} & -a_{n-1} & \dots & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -a_2 & -a_3 & \dots & a_0 & a_1 \\ -a_1 & -a_2 & \dots & -a_{n-1} & a_0 \end{pmatrix}.$$

The associated polynomial to a skew circulant matrix is

$$g(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}.$$

Then each row of the matrix is given by $x^i g(x) \pmod{x^n + 1}$ for $0 \leq i \leq n - 1$.

Proposition 4.9. *Let ζ be a solution to $x^n + 1 = 0$ (ζ is a $(2n)^{\text{th}}$ root of unity).*

Each ζ gives an eigenvector of a skew circulant matrix

$$(1, \zeta, \zeta^2, \dots, \zeta^{n-1})$$

and the eigenvalues are $g(\zeta)$ where g is the associated polynomial.

Proof. Write an $n \times n$ matrix which is skew circulant as

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -a_1 & -a_2 & \dots & -a_{n-1} & a_0 \end{pmatrix}.$$

Then

$$\begin{aligned} & \begin{pmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -a_1 & -a_2 & \dots & -a_{n-1} & a_0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta^{n-1} \end{pmatrix} \\ &= \begin{pmatrix} a_0 + a_1\zeta + \dots + a_{n-2}\zeta^{n-2} + a_{n-1}\zeta^{n-1} \\ -a_{n-1} + a_0\zeta + \dots + a_{n-3}\zeta^{n-2} + a_{n-2}\zeta^{n-1} \\ \vdots \\ -a_1 - a_2\zeta - \dots - a_{n-1}\zeta^{n-2} + a_0\zeta^{n-1} \end{pmatrix} \\ &= (a_0 + a_1\zeta + \dots + a_{n-2}\zeta^{n-2} + a_{n-1}\zeta^{n-1}) \begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta^{n-1} \end{pmatrix} \end{aligned}$$

Each eigenvector has the associated eigenvalue

$$a_0 + a_1\zeta + \dots + a_{n-2}\zeta^{n-2} + a_{n-1}\zeta^{n-1}.$$

□

4.2.2 Units as norms

Let K_n be the n^{th} layer of the anti-cyclotomic \mathbb{Z}_2 -extension of $K_0 = \mathbb{Q}(i)$ where $n \geq 1$. K_n is a totally imaginary field of degree 2^{n+1} over \mathbb{Q} and therefore has no real embeddings ($r_1 = 0$) and 2^n pairs of complex embeddings ($r_2 = 2^n$). By Dirichlet's unit theorem, K_n has $r_1 + r_2 - 1 = 2^n - 1$ fundamental units.

Let E_n be the unit group of K_n and let U_n be the units of K_n modulo cubes.

We also have $\text{Gal}(K_n/\mathbb{Q}) \simeq D_n$. Let σ and τ be generators of the Galois group where σ has order 2^n and τ has order 2. Let τ be complex conjugation under some embedding $\tau \hookrightarrow \mathbb{C}$. We have the following relation, since $\text{Gal}(K_n/\mathbb{Q}) \simeq D_n$:

$$\tau\sigma^i = \sigma^{-i}\tau.$$

Let F_n be the fixed field of τ . This field is of degree 2^n over \mathbb{Q} . Consider the embeddings σ^i applied to F_n . Since τ fixes F_n , we now determine which if any of the Galois elements stabilize F_n , since these will be the real embeddings. Since

$$\tau\sigma^i(F_n) = \sigma^{-i}\tau(F_n) = \sigma^{-i}(F_n),$$

it's sufficient to consider just the elements of the form σ^i . Let $x \in F_n$. Say σ^i stabilizes F_n and therefore $\tau\sigma^i(x) = \sigma^i(x)$. Then

$$\sigma^i(x) = \tau\sigma^i(x) = \sigma^{-i}\tau(x) = \sigma^{-i}(x) \implies \sigma^{2i}(x) = x.$$

Therefore $\sigma^{2i} \in \text{Gal}(K_n/F_n)$. Since $\sigma^{2i} \neq \tau$, we have $i = 0$ or $i = 2^{n-1}$ and so there are exactly two real embeddings. Therefore there are $2^{n-1} - 1$ pairs of complex embeddings and so F_n has

$$r_1 + r_2 - 1 = 2 + 2^{n-1} - 1 - 1 = 2^{n-1}$$

fundamental units.

The units of K_{n-1} are embedded into the units of K_n , and similarly the units of F_n are also embedded into the units of K_n . Since F_n has 2^{n-1} independent units and K_{n-1} has $2^{n-1} - 1$ independent units, this means that at least one unit of K_n which is not a unit in K_{n-1} is fixed by τ .

We now need to understand the structure of the relative units of K_n modulo cubes, which we define as

$$U_n^{rel} = \ker (N_{K_n/K_{n-1}} : U_n \rightarrow U_{n-1}).$$

Lemma 4.10. *There exists $u \in U_n$ such that the relative units mod cubes, U_n^{rel} , are spanned by*

$$\{u, \sigma u, \sigma^2 u, \dots, \sigma^{2^{n-1}-1} u\}$$

and furthermore

$$\sigma^{2^n-1} u \equiv u^{-1} \pmod{\text{cubes}}.$$

Proof. We have $\text{Gal}(K_n/\mathbb{Q})$ with generators σ and τ , where τ is complex conjugation under some embedding. Then $(\sigma^j, \tau\sigma^j)$ are the pairs of complex conjugate embeddings of K_n into \mathbb{C} for $0 \leq j < 2^n$. By [27, Lemma 5.27], there exists a unit $\varepsilon \in E_n$ such that

$$\{\varepsilon, \sigma\varepsilon, \sigma^2\varepsilon, \dots, \sigma^{2^n-2}\varepsilon\}$$

generate a subgroup H of finite index in E_n . Therefore, since

$$\varepsilon^{1+\sigma+\dots+\sigma^{2^n-1}} \in \{\pm 1, \pm i\},$$

we have

$$E_n \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}[\langle\sigma\rangle]/(1 + \sigma + \dots + \sigma^{2^n-1}).$$

The units mod cubes are

$$U_n = E_n/E_n^3 \simeq E_n \otimes_{\mathbb{Z}} \mathbb{F}_3.$$

Let $g \in \langle\sigma\rangle$. Since H is g -stable, we can calculate the characteristic polynomial of g , $f_g(x)$, using H . Since H is a \mathbb{Z} -module, $f_g(x) \in \mathbb{Z}[x]$. We can also compute $f_g(x)$ using a basis for E_n modulo torsion, and since H and E_n span $E_n \otimes \mathbb{Q}$, they yield the same characteristic polynomials. We can reduce $f_g(x)$ mod 3 to get the characteristic polynomial of g on U_n and on $H \otimes_{\mathbb{Z}} \mathbb{F}_3$.

The Brauer-Nesbitt Theorem says that the semi-simplification is determined by the characteristic polynomials of $g \in \langle \sigma \rangle$. Since $|\langle \sigma \rangle| = 2^n$ is relatively prime to 3, the characteristic of \mathbb{F}_3 , the representations of $\langle \sigma \rangle$ on U_n and on $H \otimes_{\mathbb{Z}} \mathbb{F}_3$ are already semi-simple and so these representations are isomorphic:

$$U_n \simeq H \otimes_{\mathbb{Z}} \mathbb{F}_3 \simeq \mathbb{F}_3[\langle \sigma \rangle] / (1 + \sigma + \dots + \sigma^{2^n-1}). \quad (4.1)$$

Since $N_{K_n/K_{n-1}} = 1 + \sigma^{2^{n-1}}$, we have

$$\begin{aligned} U_n^{rel} &= \ker \left((1 + \sigma^{2^{n-1}}) : U_n \rightarrow U_{n-1} \right) \\ &\simeq \left\{ \sum_{i=0}^{2^n-1} a_i \sigma^i \in \mathbb{F}_3[\langle \sigma \rangle] \mid (1 + \sigma^{2^{n-1}}) \sum_{i=0}^{2^n-1} a_i \sigma^i \equiv 0 \pmod{(1 + \sigma + \dots + \sigma^{2^n-1})} \right\} \\ &= \left\{ \sum_{i=0}^{2^n-1} a_i \sigma^i \mid (1 + \sigma^{2^{n-1}}) \sum_{i=0}^{2^{n-1}-1} (a_i + a_{2^{n-1}+i}) \sigma^i \equiv 0 \pmod{(1 + \sigma + \dots + \sigma^{2^n-1})} \right\} \\ &= \left\{ \sum_{i=0}^{2^n-1} a_i \sigma^i \mid a_i + a_{2^{n-1}+i} \equiv c \pmod{3} \text{ for } 0 \leq i \leq 2^{n-1} - 1 \right\} \end{aligned}$$

for some constant c . So U_n^{rel} is generated over $\mathbb{F}_3[\langle \sigma \rangle]$ by $\sigma^{2^{n-1}} - 1$. This corresponds to an element $u \in U_n$ by the isomorphism in Equation 4.1. Therefore U_n is spanned by

$$\{u, \sigma u, \sigma^2 u, \dots, \sigma^{2^{n-1}-1} u\}$$

and

$$\sigma^{2^{n-1}} u \equiv u^{-1} \pmod{\text{cubes.}}$$

□

Let u be a unit which is fixed by τ : $\tau u = u$. Then

$$\tau \sigma^i u = \sigma^{-i} \tau u = \sigma^{-i} u.$$

Note that then

$$\tau \sigma^{2^n-1} u = \sigma^{2^n-2^{n-1}} \tau u = \sigma^{2^n-1} u.$$

Proposition 4.11. *Let $\mathfrak{p}, \sigma \mathfrak{p}, \dots, \sigma^{2^n-1} \mathfrak{p}$ be primes in K_n lying over $p \equiv 3 \pmod{4}$.*

Let $\tau \mathfrak{p} = \sigma^k \mathfrak{p}$. Then k is even if and only if there is at least one prime lying over p which is fixed by τ .

Proof. Since the primes all lie over rational primes which are $3 \pmod{4}$, the primes are inert in K_0 and totally split in K_n/K_0 (Proposition 3.1).

First, assume k is even: $k = 2k'$. Then

$$\tau \sigma^{k'} \mathfrak{p} = \sigma^{-k'} \tau \mathfrak{p} = \sigma^{-k'+2k'} \mathfrak{p} = \sigma^{k'} \mathfrak{p}$$

and therefore $\sigma^{k'} \mathfrak{p}$ is fixed by τ .

Now assume k is odd: $k = 2k' + 1$. Then let $\sigma^j \mathfrak{p}$ be fixed by τ : $\tau \sigma^j \mathfrak{p} = \sigma^j \mathfrak{p}$.

But

$$\sigma^j \mathfrak{p} = \tau \sigma^j \mathfrak{p} = \sigma^{-j} \tau \mathfrak{p} = \sigma^{-j+2k'+1} \mathfrak{p}$$

which implies $j \equiv -j + 2k' + 1 \pmod{2^n} \implies 2k' + 1 \equiv 2j \pmod{2^n}$ which is a contradiction. \square

Without loss of generality, since it only changes the ordering of the primes, we

can let $\tau\mathfrak{p} = \mathfrak{p}$ if there is a prime fixed by τ , and $\tau\mathfrak{p} = \sigma\mathfrak{p}$ if there is not.

Let L_n/K_n be a cyclic cubic extension. Recall that by the Hasse Norm Theorem, a unit $u \in K_n$ is the norm of an element in L_n if and only if it is a local norm at all primes that ramify in L_n/K_n . We also have the following proposition which tells us that we only need to worry about the ‘new units’ at each stage.

Proposition 4.12. *For $n \geq 1, m \geq 1$, let u be a unit in K_n regarded as a unit in K_{n+m} . Then u is the norm of an element in L_{n+m} if and only if it is the norm of an element in L_n .*

Proof. Suppose $u \in K_{n+m}$ is the norm of an element $a \in L_{n+m}$: $N_{L_{n+m}/K_{n+m}}(a) = u$.

Then

$$N_{L_{n+m}/K_n}(a) = N_{K_{n+m}/K_n} N_{L_{n+m}/K_{n+m}}(a) = u^{2^m}.$$

Since 2^m is prime to 3 and we have a cubic extension, this implies u is a norm.

Therefore u is the norm of an element in L_n . The converse is trivial. \square

We can determine if the units of K_n are norms from L_n by constructing a matrix of norm residue symbols where the $(i, j)^{th}$ entry of the matrix is the symbol $\left(\frac{u_j}{\mathfrak{p}_i}\right)$. There are 2^n relative units mod cubes in K_n and $2^n t$ primes that ramify in L_n/K_n . Write the units as

$$u, \sigma u, \dots, \sigma^{2^{n-1}-1} u.$$

These are the units in K_n which have norm 1 in K_{n-1} mod cubes. By Proposition 4.12, these are the only units we need to consider as we already know if units from fields lower in the towers are norms. For each set of primes that ramify in L_n/K_n

and lie over the same rational prime, write the primes of K_n as

$$\mathfrak{p}, \sigma\mathfrak{p}, \dots, \sigma^{2^n-1}\mathfrak{p}.$$

We're now ready to prove the following theorem.

Theorem 4.13. *Let $n \geq 2$. Let U_n^{rel} be the units in K_n that have norm 1 in K_{n-1} mod cubes. Then either all of these units are norms of elements in L_n or none of the units are norms of elements in L_n (or more precisely, the only elements which are norms are cubes).*

Proof. A unit $u \in K_n$ is the norm of an element in L_n if and only if its norm residue symbols modulo each prime that ramifies in L_n/K_n are trivial. As above, let u be a unit fixed by τ and let $u_j = \sigma^j u$. Note that this implies

$$\tau u_j = \tau \sigma^j u = \sigma^{-j} \tau u = \sigma^{2^n-j} u = (\sigma^{2^{n-1}-j} u)^{-1} = u_{2^{n-1}-j}^{-1}$$

since $\sigma^{2^{n-1}} u = u^{-1}$.

We can consider each set of conjugate primes separately, so we'll first look only at primes which all lie over the same rational prime. Write these primes as

$$\mathfrak{p}_0 = \mathfrak{p}, \mathfrak{p}_1 = \sigma\mathfrak{p}, \dots, \mathfrak{p}_{2^n-1} = \sigma^{2^n-1}\mathfrak{p}.$$

We'll address two cases separately: the case where at least one of the primes is fixed by τ , and the case where no primes are fixed by τ .

Fixed prime. First, the case where a prime is fixed. Without loss of generality, let \mathfrak{p} be that prime: $\tau\mathfrak{p} = \mathfrak{p}$. Then

$$\tau\sigma^j\mathfrak{p} = \sigma^{-j}\tau\mathfrak{p} = \sigma^{-j}\mathfrak{p}.$$

Construct a matrix (a_{ij}) using the norm residue symbols:

$$\left(\frac{u_j}{\mathfrak{p}_i}\right) \equiv u_j^{(N\mathfrak{p}_i-1)/3} \equiv \omega^{a_{ij}} \pmod{\mathfrak{p}_i}$$

where ω is a fixed primitive cube root of unity. We extend τ and σ such that ω is fixed by both. Since each \mathfrak{p}_i is inert in K_0/\mathbb{Q} and totally split in K_n/K_0 , $N\mathfrak{p}_i = p^2$. The entries in the matrix are the powers of cube roots of unity, and so the matrix is over \mathbb{F}_3 .

First consider $\mathfrak{p}_0 = \mathfrak{p}$. Write

$$\left(\frac{u_j}{\mathfrak{p}}\right) = \omega^{a_j}.$$

For $0 \leq j \leq 2^{n-1} - 1$, apply τ , using $\tau u_j = u_{2^{n-1}-j}^{-1}$ and the assumption that $\tau\mathfrak{p} = \mathfrak{p}$:

$$\omega^{a_j} = \left(\frac{u_j}{\mathfrak{p}}\right) = \tau \left(\frac{u_j}{\mathfrak{p}}\right) = \left(\frac{u_{2^{n-1}-j}^{-1}}{\mathfrak{p}}\right) = \omega^{-a_{2^{n-1}-j}} \implies a_j = -a_{2^{n-1}-j}.$$

This gives us some relations between the symbols. We want to pay special attention

to what happens when $j = 2^{n-1} - j$, or $j = 2^{n-2}$. Then

$$a_{2^{n-2}} = -a_{2^{n-2}} \implies a_{2^{n-2}} = 0.$$

We can use the above relations to write the first row of the matrix a_{ij} in terms of a_j , $0 \leq j < 2^{n-2}$:

$$\left(a_0 \quad a_1 \quad \dots \quad a_{2^{n-2}-1} \quad 0 \quad -a_{2^{n-2}-1} \quad \dots \quad -a_1 \right).$$

To get the next row, we can apply σ . Then

$$\omega^{a_j} = \sigma \left(\frac{u_j}{\mathfrak{p}} \right) = \left(\frac{u_{j+1}}{\sigma \mathfrak{p}} \right)$$

for $0 \leq j < 2^{n-1} - 1$ and

$$\omega^{a_1} = \left(\frac{u_{2^{n-1}-1}^{-1}}{\mathfrak{p}} \right) = \sigma \left(\frac{u_{2^{n-1}-1}^{-1}}{\mathfrak{p}} \right) = \left(\frac{u_0}{\sigma \mathfrak{p}} \right).$$

If we continue in this manner, we can construct a $2^n \times 2^{n-1}$ skew circulant

matrix:

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{2^{n-2}-1} & 0 & -a_{2^{n-2}-1} & \dots & -a_1 \\ a_1 & a_0 & \dots & a_{2^{n-2}-2} & a_{2^{n-2}-1} & 0 & \dots & -a_2 \\ a_2 & a_1 & \dots & a_{2^{n-2}-3} & a_{2^{n-2}-2} & a_{2^{n-2}-1} & \dots & -a_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & 0 & a_{2^{n-2}-1} & a_{2^{n-2}-2} & \dots & a_0 \\ -a_0 & -a_1 & \dots & -a_{2^{n-2}-1} & 0 & a_{2^{n-2}-1} & \dots & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & -a_{2^{n-2}-1} & -a_{2^{n-2}-2} & -a_{2^{n-2}-3} & \dots & -a_1 \\ a_1 & a_2 & \dots & 0 & -a_{2^{n-2}-1} & -a_{2^{n-2}-2} & \dots & -a_0 \end{pmatrix}$$

If $n = 2$, we have the matrix

$$\begin{pmatrix} a_0 & 0 \\ 0 & a_0 \\ -a_0 & 0 \\ 0 & -a_0 \end{pmatrix}$$

which has rank 0 if $a_0 = 0$ and rank 2 if $a_0 \neq 0$ over \mathbb{F}_3 . This means that either both units are norms modulo all four primes or neither of them are.

By Proposition 4.9, the top half of the matrix has eigenvectors

$$(1, \zeta, \dots, \zeta^{2^{n-1}-1})$$

where ζ is one of the 2^{n-1} distinct solutions to $x^{2^{n-1}} + 1 = 0$. The corresponding eigenvalue is

$$\begin{aligned} & a_0 + a_1\zeta + \dots + a_{2^{n-2}-1}\zeta^{2^{n-2}-1} - a_{2^{n-2}-1}\zeta^{2^{n-2}+1} - \dots - a_1\zeta^{2^{n-1}-1} \\ &= \sum_{j=0}^{2^{n-2}-1} a_j\zeta^j - \sum_{j=1}^{2^{n-2}-1} a_{2^{n-2}-j}\zeta^{2^{n-2}+j}. \end{aligned}$$

We want to show that the eigenvalues are all non-zero unless the matrix is the zero matrix.

We've already handled the $n = 2$ case. For $n > 2$, we can factor $x^{2^{n-1}} + 1$ as

$$(x^{2^{n-2}} + x^{2^{n-3}} - 1)(x^{2^{n-2}} - x^{2^{n-3}} - 1) \pmod{3}.$$

Therefore $\zeta^{2^{n-2}} \equiv \pm\zeta^{2^{n-3}} + 1$. Furthermore,

$$\zeta^{2^{n-2}+2^{n-3}} \equiv \pm\zeta^{2^{n-2}} + \zeta^{2^{n-3}} \equiv -\zeta^{2^{n-3}} \pm 1$$

over \mathbb{F}_3 .

We can use this to reduce the eigenvalue to lower terms.

$$\begin{aligned}
& \sum_{j=0}^{2^{n-2}-1} a_j \zeta^j - \sum_{j=1}^{2^{n-2}-1} a_{2^{n-2}-j} \zeta^{2^{n-2}+j} \\
&= a_0 + a_{2^{n-3}} \zeta^{2^{n-3}} + \sum_{j=1}^{2^{n-3}-1} (a_j \zeta^j + a_{2^{n-3}+j} \zeta^{2^{n-3}+j}) \\
&\quad - a_{2^{n-3}} \zeta^{2^{n-2}+2^{n-3}} - \sum_{j=1}^{2^{n-3}-1} (a_{2^{n-2}-j} \zeta^{2^{n-2}+j} + a_{2^{n-3}-j} \zeta^{2^{n-2}+2^{n-3}+j}) \\
&\equiv a_0 \mp a_{2^{n-3}} - a_{2^{n-3}} \zeta^{2^{n-3}} \\
&\quad + \sum_{j=1}^{2^{n-3}-1} (a_j - a_{2^{n-2}-j} \mp a_{2^{n-3}-j}) \zeta^j + (a_{2^{n-3}+j} \mp a_{2^{n-2}-j} + a_{2^{n-3}-j}) \zeta^{2^{n-3}+j}
\end{aligned}$$

Let I_k be the $k \times k$ identity matrix and let J_k be the $k \times k$ anti-identity matrix.

Note that our eigenvalue is a polynomial in ζ of degree $2^{n-2} - 1$. Therefore the eigenvalue equals zero only if each coefficient is zero. We can think of the eigenvalue as a vector, where

$$p_0 + p_1 \zeta + \dots + p_{2^{n-2}-1} \zeta^{2^{n-2}-1} \mapsto (p_0, p_1, \dots, p_{2^{n-2}-1}).$$

Then we can write the eigenvalue as a $2^{n-2} \times 2^{n-2}$ matrix, which we'll call B , times the column vector $(a_0, a_1, \dots, a_{2^{n-2}-1})$.

Then

$$B = \left(\begin{array}{c|c|c|c}
1 & & -1 & \\
\hline
& I \mp J & & -J \\
\hline
0 & & -1 & \\
\hline
& J & & I \mp J
\end{array} \right)$$

where the I and J matrices are both of size $(2^{n-3} - 1) \times (2^{n-3} - 1)$.

Considering just the blocks containing I and/or J , we have the following chain of row operations:

$$\begin{aligned}
\left(\begin{array}{c|c} I \mp J & -J \\ \hline J & I \mp J \end{array} \right) &\rightarrow \left(\begin{array}{c|c} I \mp J & -J \\ \hline \pm J & \pm I - J \end{array} \right) && \text{(multiply 2nd row by } \pm I \text{)} \\
&\rightarrow \left(\begin{array}{c|c} I & \pm I + J \\ \hline J & I \mp J \end{array} \right) && \text{(1st row} + \text{ 2nd row, } -2 \equiv 1 \text{)} \\
&\rightarrow \left(\begin{array}{c|c} I & \pm I + J \\ \hline I & J \mp I \end{array} \right) && \text{(multiply 2nd row by } J \text{)} \\
&\rightarrow \left(\begin{array}{c|c} I & \pm I + J \\ \hline 0 & \pm I \end{array} \right) && \text{(2nd row} - \text{ 1st row)}
\end{aligned}$$

This matrix has determinant ± 1 , and therefore B also has determinant ± 1 . Then B has full rank, and therefore there is no non-trivial solution to

$$B \cdot (a_0, \dots, a_{2^{n-2}-1}) = (0, \dots, 0).$$

Therefore the only way for the eigenvalue to equal zero is for $a_j = 0$ for all j .

No fixed prime. Now, the case where a prime is not fixed. Let $\tau \mathbf{p} = \sigma \mathbf{p}$. Then

$$\tau \sigma^j \mathbf{p} = \sigma^{-j} \tau \mathbf{p} = \sigma^{-j+1} \mathbf{p}.$$

Again construct a matrix a_{ij} over \mathbb{F}_3 using the norm residue symbols:

$$\left(\frac{u_j}{\mathfrak{p}_i}\right) \equiv u_j^{(p^2-1)/3} \equiv \omega^{a_{ij}} \pmod{\mathfrak{p}_i}$$

where ω is a fixed primitive cube root of unity.

We'll again start by considering $\mathfrak{p}_0 = \mathfrak{p}$. Write

$$\left(\frac{u_j}{\mathfrak{p}}\right) = \omega^{a_j}.$$

Then using $\tau u_j = u_{2^{n-1}-j}^{-1}$ and the assumption that $\tau \mathfrak{p} = \sigma \mathfrak{p}$, for $0 \leq j < 2^{n-2}$,

$$\omega^{a_j} = \left(\frac{u_j}{\mathfrak{p}}\right) = \sigma \left(\frac{u_j}{\mathfrak{p}}\right) = \left(\frac{u_{2^{n-1}-j}}{\sigma \mathfrak{p}}\right).$$

Apply σ^{2^n-1} :

$$\omega^{a_j} = \sigma^{2^n-1}(\omega^{a_j}) = \left(\frac{u_{2^{n-1}-j-1}^{-1}}{\mathfrak{p}}\right) = \omega^{-a_{2^{n-1}-j-1}}.$$

Therefore the first row of the matrix is

$$\left(a_0 \quad a_1 \quad \dots \quad a_{2^{n-2}-1} \quad -a_{2^{n-2}-1} \quad \dots \quad -a_0\right).$$

We can again apply σ to get the full matrix:

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{2^{n-2}-1} & -a_{2^{n-2}-1} & \dots & -a_0 \\ a_0 & a_0 & \dots & a_{2^{n-2}-2} & a_{2^{n-2}-1} & \dots & -a_1 \\ a_1 & a_0 & \dots & a_{2^{n-2}-3} & a_{2^{n-2}-2} & \dots & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & -a_{2^{n-2}-2} & -a_{2^{n-2}-3} & \dots & -a_1 \\ a_1 & a_2 & \dots & -a_{2^{n-2}-1} & -a_{2^{n-2}-2} & \dots & -a_0 \end{pmatrix}$$

If $n = 2$, we have the matrix

$$\begin{pmatrix} a_0 & -a_0 \\ a_0 & a_0 \\ -a_0 & a_0 \\ -a_0 & -a_0 \end{pmatrix}$$

which has rank 0 if $a_0 = 0$ and rank 2 if $a_0 \neq 0$ over \mathbb{F}_3 . This again means that either both units are norms modulo all four primes or neither of them are.

By Proposition 4.9, the top half of the matrix has eigenvectors

$$(1, \zeta, \dots, \zeta^{2^{n-1}-1})$$

where ζ is one of the 2^{n-1} distinct solutions to $x^{2^{n-1}} + 1 = 0$. The corresponding

eigenvalue is

$$\begin{aligned}
& a_0 + a_1\zeta + \dots + a_{2^{n-2}-1}\zeta^{2^{n-2}-1} - a_{2^{n-2}-1}\zeta^{2^{n-2}-1} - \dots - a_0\zeta^{2^{n-1}-1} \\
&= \sum_{j=0}^{2^{n-2}-1} a_j\zeta^j - \sum_{j=0}^{2^{n-2}-1} a_{2^{n-2}-1-j}\zeta^{2^{n-2}+j}.
\end{aligned}$$

For $n > 2$, we again have

$$\begin{aligned}
x^{2^{n-1}} + 1 &\equiv (x^{2^{n-2}} + x^{2^{n-3}} - 1)(x^{2^{n-2}} - x^{2^{n-3}} - 1), \\
\zeta^{2^{n-2}} &\equiv \pm\zeta^{2^{n-3}} + 1, \\
\zeta^{2^{n-2}+2^{n-3}} &\equiv -\zeta^{2^{n-3}} \pm 1.
\end{aligned}$$

We can use this to reduce the eigenvalue to lower terms.

$$\begin{aligned}
& \sum_{j=0}^{2^{n-2}-1} a_j\zeta^j - \sum_{j=0}^{2^{n-2}-1} a_{2^{n-2}-1-j}\zeta^{2^{n-2}+j} \\
&= \sum_{j=0}^{2^{n-3}-1} a_j\zeta^j + a_{2^{n-3}+j}\zeta^{2^{n-3}+j} - a_{2^{n-2}-1-j}\zeta^{2^{n-2}+j} - a_{2^{n-3}-1-j}\zeta^{2^{n-2}+2^{n-3}+j} \\
&= \sum_{j=0}^{2^{n-3}-1} a_j\zeta^j + a_{2^{n-3}+j}\zeta^{2^{n-3}+j} \mp a_{2^{n-2}-1-j}(\zeta^{2^{n-3}+j} \pm \zeta^j) + a_{2^{n-3}-1-j}(\zeta^{2^{n-3}+j} \mp \zeta^j) \\
&= \sum_{j=0}^{2^{n-3}-1} (a_j - a_{2^{n-2}-1-j} \mp a_{2^{n-3}-1-j})\zeta^j + (a_{2^{n-3}+j} \mp a_{2^{n-2}-1-j} + a_{2^{n-3}-1-j})\zeta^{2^{n-3}+j}
\end{aligned}$$

Writing the matrix B as in the previous case, we get

$$B = \left(\begin{array}{c|c} I \mp J & -J \\ \hline J & I \mp J \end{array} \right)$$

where the I and J matrices are both of size $(2^{n-3}) \times (2^{n-3})$. Just as before, this matrix can be row-reduced to

$$\left(\begin{array}{c|c} I & \pm I + J \\ \hline 0 & \mp I \end{array} \right)$$

and so here again the matrix has determinant ± 1 .

So again, the matrix has full rank and so there are no non-trivial solutions for the $\{a_j\}$ which yield a zero eigenvalue.

So in both cases, the eigenvalues are all non-zero unless the matrix is identically zero. Therefore the original matrix of norm residue symbols is all zero or it has full rank.

If primes over more than one rational prime ramify, we can construct matrices for each set of conjugate primes separately. Then each matrix is either full rank or rank zero, and therefore the units are either all local norms or none of them are. If the units are all local norms modulo all of the primes, the units are global norms. Otherwise, none of the units are global norms. \square

Proposition 4.14. *Let $K_0 = \mathbb{Q}(i)$. Let K_n/K_0 be the anti-cyclotomic \mathbb{Z}_2 -extension.*

Let

$$\text{Gal}(K_n/\mathbb{Q}) \simeq D_n = \langle \sigma, \tau \rangle$$

where σ has order 2^n and τ has order 2 and restricts to the generator of $\text{Gal}(K_0/\mathbb{Q})$.

If $p \equiv 7 \pmod{8}$, then at least one of the primes above p in K_n is fixed by τ . If

$p \equiv 3 \pmod{8}$, then none of the primes above p in K_n are fixed by τ .

Proof. Recall that $K_1 = \mathbb{Q}(\zeta_8)$. Let F_n be the fixed field of τ .

We have the following diagram of fields:

$$\begin{array}{ccc}
 & & K_n \\
 & \swarrow & | \\
 F_n & & \\
 | & & \\
 & \swarrow & K_1 \\
 F_1 & & \\
 | & & \\
 & \swarrow & K_0 \\
 \mathbb{Q} & &
 \end{array}$$

Take $F_1 = \mathbb{Q}(\sqrt{2})$. By Proposition 3.1, primes which are inert in K_0 split completely in K_n/K_0 . Primes which are $19 \pmod{24}$ are inert in F_1/\mathbb{Q} and therefore must split completely in K_n/F_1 . This means there can be no primes in K_n which are fixed by τ .

Primes which are $p \equiv 7 \pmod{24}$ split in F_1 and are inert in K_0 , and therefore are inert in K_1/F_1 . Let $\mathfrak{p} \in K_n$ be a prime ideal lying over $p \in \mathbb{Q}$, $p \equiv 7 \pmod{24}$. Then

$$N_{K_n/K_1} \mathfrak{p} = \mathfrak{p}^{1+\sigma^2+\sigma^4+\dots+\sigma^{2^n-2}} := \mathfrak{q}.$$

Since $\tau \mathfrak{q} = \mathfrak{q}$, $\tau \mathfrak{p}$ must be one of the primes of K_n over \mathfrak{q} . So

$$\tau \mathfrak{p} = \sigma^{2j} \mathfrak{p}$$

for some j . But then if we apply τ to $\sigma^j \mathfrak{p}$, we get

$$\tau \sigma^j \mathfrak{p} = \sigma^{-j} \tau \mathfrak{p} = \sigma^j \mathfrak{p}$$

and so $\sigma^j \mathfrak{p}$ is fixed by τ . Therefore there must be a prime in F_n lying over p which is inert in K_n/F_n .

□

We can now apply Theorem 4.13, where the two cases here correspond to the two cases in the theorem. Either all of the relative units in K_n are norms of elements in L_n modulo cubes or none of them are.

Furthermore, the proof of Theorem 4.13 shows that for $n \geq 2$, the matrix which tells us if the units of K_n are norms has 2^{n-2} independent parameters.

We'll make use of this theorem in Chapter 6 when we develop heuristics for the behavior of the class group as we move up the tower.

Chapter 5: Data

This chapter contains the data we obtained by computing the class groups of cyclic cubic extensions of the first few layers in the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$. We also have some computations for quintic extensions. The computations were all done with Sage [7] and assume the Generalized Riemann Hypothesis.

5.1 The anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$

By Proposition 5 from [16] and personal correspondence with Broker [2], we have explicit polynomials giving the first layers of the anti-cyclotomic \mathbb{Z}_2 -extension of $K_0 = \mathbb{Q}(i)$. The polynomials below give K_n/K_0 for $1 \leq n \leq 4$.

$$K_1 \quad x^2 + 2$$

$$K_2 \quad x^4 + 2$$

$$K_3 \quad x^8 + 2$$

$$K_4 \quad x^{16} - 8x^8 - 2$$

We have also explicitly computed the units in each of the above fields. We get 2^{n-1} new units in K_n . Here, we give the generator of the relative units mod cubes. Acting on the generator by σ gives the full set of generators.

$$K_1 \quad \sqrt{2} + 1$$

$$K_2 \quad (-i - 1)\sqrt[4]{-2^3} + 2i\sqrt{-2} + (-2i + 2)\sqrt[4]{-2} - 3$$

$$K_3 \quad (-i + 2)\sqrt[8]{-2^7} + (i - 1)\sqrt[8]{-2^6} - 2i\sqrt[8]{-2^4} \\ + (3i + 1)\sqrt[8]{-2^3} + (-2i - 2)\sqrt[8]{-2^2} + 3$$

$$K_4 \quad -116/3(4 - 3\sqrt[8]{2})^{15} + 68/3(4 - 3\sqrt[8]{2})^{14} + 38/3(4 - 3\sqrt[8]{2})^{13} - 24(4 - 3\sqrt[8]{2})^{12} \\ + 20/3(4 - 3\sqrt[8]{2})^{11} + 38/3(4 - 3\sqrt[8]{2})^{10} - 38/3(4 - 3\sqrt[8]{2})^9 - 2/3(4 - 3\sqrt[8]{2})^8 \\ + 956/3(4 - 3\sqrt[8]{2})^7 - 560/3(4 - 3\sqrt[8]{2})^6 - 314/3(4 - 3\sqrt[8]{2})^5 + 198(4 - 3\sqrt[8]{2})^4 \\ - 164/3(4 - 3\sqrt[8]{2})^3 - 314/3(4 - 3\sqrt[8]{2})^2 + 314/3(4 - 3\sqrt[8]{2}) + 17/3$$

5.2 L_0/K_0

We first computed the class group in extensions of $\mathbb{Q}(i)$ in which only primes over one rational prime ramify in L_0/K_0 and in which the rational prime is inert in $\mathbb{Q}(i)$ (i.e. it is congruent to 3 mod 4). Recall that we defined t_i to be the number of rational primes which are inert in $\mathbb{Q}(i)$ and t_s to be the number of rational primes which split in $\mathbb{Q}(i)$.

All of the 311 such fields where the rational prime is less than 10,000 had trivial class group, as proven in Chapter 2.

We then considered the case where only primes over one rational prime ramify in L_0/K_0 , but now that prime splits in $K_0 = \mathbb{Q}(i)$ (i.e. it is congruent to 1 mod 4). Of the 300 such fields in which the rational prime is less than 10,000, two hundred of the fields had class group with rank 1 and 100 of the fields had class group with rank 2.

	Rank 1	Rank 2	Total
Number	200	100	300
Proportion	0.6667	0.3333	1.0000

Table 5.1: Class Group Rank Statistics for $t_i = 0, t_s = 1$.

In §6.1, we give a heuristic argument that predicts that these proportions are $2/3$ and $1/3$.

Next we consider extensions in which primes over two rational primes ramify. For the cases $t_s = 2$ and $t_i = 2$, we considered fields in which both rational primes were less than 1000. For $t_s = t_i = 1$, we consider fields in which both primes were less than 300.

	Rank 1	Rank 2	Total
Number	1696	196	1892
Proportion	0.8964	0.1036	1.0000

Table 5.2: Class Group Rank Statistics for $t_i = 2, t_s = 0$.

In §6.1, we give a heuristic argument that predicts that these proportions are $8/9$ and $1/9$.

	Rank 2	Rank 3	Rank 4	Total
Number	227	147	10	384
Proportion	0.5911	0.3828	0.0260	1.0000

Table 5.3: Class Group Rank Statistics for $t_i = 1, t_s = 1$.

In §6.1, we give a heuristic argument that predicts that these three proportions are

$$\frac{16}{27} = \left(\frac{2}{3} \times \frac{8}{9}\right), \quad \frac{10}{27}, \quad \text{and} \quad \frac{1}{27}.$$

	Rank 3	Rank 4	Rank 5	Rank 6	Total
Number	669	540	49	2	1260
Proportion	0.5310	0.4286	0.0389	0.0016	1.0000

Table 5.4: Class Group Rank Statistics for $t_i = 0$, $t_s = 2$.

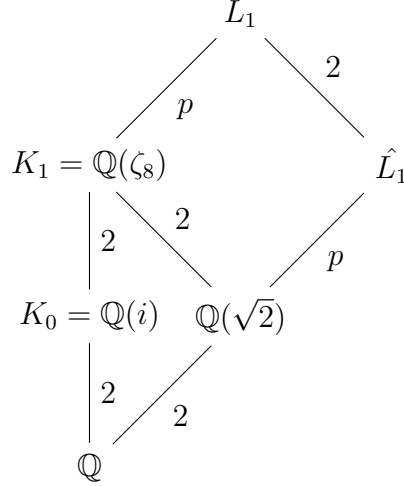
In §6.1, we give a heuristic argument that predicts that these three proportions are

$$\frac{384}{729}, \quad \frac{304}{729}, \quad \frac{40}{729}, \quad \text{and} \quad \frac{1}{729}.$$

5.3 L_1/K_1

Let $K_1 = \mathbb{Q}(\zeta_8)$ which is the next layer in both the cyclotomic and anti-cyclotomic \mathbb{Z}_2 -extensions of $\mathbb{Q}(i)$. Let L_1/K_1 be a cyclic degree p extension which is the lift of a cyclic degree p number field. Most of the computations were done for $p = 3$ but we also include a small number of quintic extensions. We only considered extensions in which all ramified primes were inert in $\mathbb{Q}(i)$ (and therefore congruent to $3 \pmod{4}$). Since we're only considering abelian extensions, this means the ramified primes must also be congruent to $1 \pmod{p}$.

Let \hat{L}_1 be the real subfield of L_1 . Then $L_1/\mathbb{Q}(\zeta_8)$ is the lift of the extension $\hat{L}_1/\mathbb{Q}(\sqrt{2})$ and we have the following diagram of fields:



Primes which are congruent to 7 mod 8 split in $\mathbb{Q}(\sqrt{2})$. When all ramified primes are 7 mod 8, this fact will allow us to compute the class group of L_1 by instead computing the class group of \hat{L}_1 .

Proposition 5.1. *Let $\hat{L}_1/\mathbb{Q}(\sqrt{2})$ be a cyclic degree p extension in which only primes that are congruent to 7 mod 8 ramify. Let L_1/K_1 be the lift of the extension. Let $A(L_1)$ be the p -class group of L_1 and let $A(\hat{L}_1)$ be the p -class group of \hat{L}_1 . Then*

$$A(\hat{L}_1) \simeq A(L_1).$$

Proof. Let $\Delta = \text{Gal}(L_1/K_1)$ and let $\hat{\Delta} = \text{Gal}(\hat{L}_1/\mathbb{Q}(\sqrt{2}))$. By Chevalley's formula for $\hat{L}_1/\mathbb{Q}(\sqrt{2})$,

$$|A(\hat{L}_1)^\Delta| = p^{t-1-\hat{e}}$$

and similarly for $L_1/\mathbb{Q}(\zeta_8)$,

$$|A(L_1)^{\hat{\Delta}}| = p^{t-1-e}.$$

Since there is only one fundamental unit in $\mathbb{Q}(\zeta_8)$ and it is $\sqrt{2} + 1$, and since $\sqrt{2} + 1$

is a norm from L_1 if and only if it is a norm from \hat{L}_1 , we have $e = \hat{e}$. Therefore $|A(\hat{L}_1)^{\hat{\Delta}}| = |A(L_1)^{\Delta}|$. Since these are both elementary groups, because $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\zeta_8)$ both have class number 1, they must be isomorphic.

Using the same notation as Washington [27, §10.2], let

$$\text{Gal}(L_1/\hat{L}_1) = \{1, J\}$$

where J is complex conjugation and let

$$A(L_1)^{\pm} = \frac{1 \pm J}{2} A(L_1).$$

Then

$$A(L_1) = A(L_1)^+ \oplus A(L_1)^-.$$

Then since $A(\hat{L}_1)$ injects into $A(L_1)^+$, we have the following sequence of embeddings:

$$A(\hat{L}_1)^{\hat{\Delta}} \hookrightarrow (A(L_1)^+)^{\Delta} \hookrightarrow A(L_1)^{\Delta} \simeq A(\hat{L}_1)^{\hat{\Delta}}$$

and therefore we must have equality. Therefore

$$(A(L_1)^+)^{\Delta} \simeq A(L_1)^{\Delta}$$

and so $(A(L_1)^-)^{\Delta}$ must be trivial. Then by Nakayama's lemma, $A(L_1)^-$ must also

be trivial. Additionally,

$$A(L_1)^+ = N_{L_1/\hat{L}_1} A(L_1) \hookrightarrow A(\hat{L}_1) \hookrightarrow A(L_1)^+$$

and therefore

$$A(L_1) \simeq A(L_1)^+ \simeq A(\hat{L}_1).$$

□

On the other hand, primes that are congruent to 3 mod 8 are inert in $\mathbb{Q}(\sqrt{2})$. Consider the case where there is only one ramified prime, congruent to 3 mod 8. Then by Chevalley's formula,

$$|A(\hat{L}_1)| = p^{t-1-\hat{e}} = p^{-\hat{e}}$$

and therefore we must have $\hat{e} = 0$ for $\hat{L}_1/\mathbb{Q}(\sqrt{2})$ and $|A(\hat{L}_1)| = 1$. If the fixed part is trivial, the entire group must be trivial and so the p -class number of \hat{L} is 1. Applying Chevalley to L_1/K_1 , we have

$$|A(\hat{L}_1)| = p^{t-1-e} = p^{1-e}$$

and so if $e = 0$,

$$|A(\hat{L}_1)| = p.$$

In fact, as shown in §6.2, e will always be 0 in these extensions.

Finally, consider the case where r of the ramified primes are congruent to $3 \pmod{8}$ and s primes are congruent to $7 \pmod{8}$. Then $r + 2s$ primes ramify in $\hat{L}_1/\mathbb{Q}(\sqrt{2})$. By Chevalley's formula,

$$|A(\hat{L}_1)| = p^{r+2s-1-e}$$

and

$$|A(L_1)| = p^{2r+2s-1-e}$$

and so

$$A(\hat{L}_1) \not\cong A(L_1)$$

unless $r = 0$.

We will divide computations according to the following conventions. We call a field 'type 1' if the unit of K_1 , $\sqrt{2} + 1$, is the norm of an element in L_1 , and we call a field 'strong' if it is type 1 and additionally the unit of K_1 is the norm of a unit in L_1 . In a strong field, all ambiguous ideals are strongly ambiguous. We call the field 'weak' if it is type 1 and the unit of K_1 is not the norm of a unit in L_1 . In a weak field, there are ambiguous ideals that are not strongly ambiguous.

5.3.1 Cubic extensions

For L_1/K_1 and $t = 1$, we computed the rank of the class group, dividing the results by type (1 or 2), and for type 1, by classification as strong or weak. This data is for primes up to 3327607 that are $7 \pmod{24}$ except for 31 primes which took

too long to compute. For extensions in which all primes are congruent to 7 mod 24, the class groups were computed for $\hat{L}_1/\mathbb{Q}(\sqrt{2})$.

Recall that t is the number of rational primes that ramify in L_1/K_1 . We denote these primes

$$p_1, \dots, p_t.$$

Category	Rank 0	Rank 1	Rank 2	Total
Type 1 Strong	0	6612	851	7463
Type 1 Weak	0	2209	285	2494
Type 2	19899	0	0	19899

Table 5.5: Class Group Rank Statistics for L_1 , $p = 3$, $t = 1$, $p_1 \equiv 7 \pmod{24}$

Of the type 1 primes, 74.95% were found to be strong. In §6.2.1, we give a heuristic argument that predicts that this proportion should be 3/4. Of the strong, 88.60% had rank 1 and of the weak, 88.22% had rank 1. In §6.2, we give a heuristic argument that predicts that for both cases of the type 1 fields, 8/9 should have rank 1. All type 2 primes had trivial 3-class group as predicted by Chevalley's formula.

We also collected data on the actual structure of the class group. We use the notation '9 3', for example, to represent the group $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

3-Class Group	Type 1 Strong	Type 1 Weak
3	6612	2209
3 3	751	252
9 3	87	30
9 9	10	3
27 9	3	0

Table 5.6: Class Group Statistics for L_1 , $p = 3$, $t = 1$, $p_1 \equiv 7 \pmod{24}$

The class group structure seems to be independent of the strong versus weak distinction.

For primes $19 \pmod{24}$, we computed the same information for primes up to 72043. All extensions were type 1 and strong.

Category	Rank 1	Rank 2	Total
Type 1 Strong	589	284	873

Table 5.7: Class Group Rank Statistics for L_1 , $p = 3$, $t = 1$, $p_1 \equiv 19 \pmod{24}$

In this case, 67.47% had rank 1 and 32.53% had rank 2. Because we couldn't use the real subfield, these computations took significantly more time and so fewer fields were computed. In §6.2, we give a heuristic argument that predicts that these proportions should be $2/3$ and $1/3$.

3-Class Group	Type 1 Strong
3	589
3 3	181
9 3	72
9 9	20
27 9	7
27 27	3
81 27	1

Table 5.8: Class Group Statistics for L_1 , $p = 3$, $t = 1$, $p_1 \equiv 19 \pmod{24}$

We also computed the rank of the class group when two primes, both $7 \pmod{24}$ and both type 1, ramify. We were able to compute all but 10 of the fields where the primes were less than 15,000.

Category	Rank 3	Rank 4	Rank 5	Total
Type 1 Strong	2791	785	70	3646
Type 1 Weak	1208	376	16	1600

Table 5.9: Class Group Rank Statistics for L_1 , $p = 3$, $t = 2$, $p_i \equiv 7 \pmod{24}$

Here 69.57% of the type 1 were strong. Our heuristics predict that this proportion should be $3/4$. We might need to modify our heuristics or it could be slow convergence, a well-known phenomenon for class group heuristics. Of the strong, 76.55% have rank 3, 21.53% have rank 4 and 1.92% have rank 5. Of the weak, 75.5% have rank 3, 23.5% have rank 4 and 1% have rank 5.

For $t = 2$, both primes $19 \pmod{24}$, there were 110 fields where both primes were less than 500. All fields were type 1 and strong.

Category	Rank 3	Rank 4	Rank 5	Total
Type 1 Strong	61	48	1	110

Table 5.10: Class Group Rank Statistics for L_1 , $p = 3$, $t = 2$, $p_i \equiv 19 \pmod{24}$

3-Class Group	Type 1 Strong
3 3 3	61
3 3 3 3	35
9 3 3 3	10
9 9 3 3	3
3 3 3 3 3	1

Table 5.11: Class Group Statistics for L_1 , $p = 3$, $t = 2$, $p_i \equiv 19 \pmod{24}$

For $t = 2$, one prime $7 \pmod{24}$ and one prime $19 \pmod{24}$, we computed the class groups for the 573 fields where both primes are less than 750.

Category	Rank 2	Rank 3	Rank 4	Rank 5	Total
Type 1 Strong	0	63	59	11	133
Type 1 Weak	0	28	17	1	46
Type 2	232	152	10	0	394

Table 5.12: Class Group Rank Statistics for L_1 , $p = 3$, $t = 2$, $p_1 \equiv 7 \pmod{24}$, $p_2 \equiv 19 \pmod{24}$.

Finally, for $t = 3$, we were able to compute 1623 fields where all primes are $7 \pmod{24}$ and type 1.

Category	Rank 5	Rank 6	Rank 7	Rank 8	Total
Type 1 Strong	768	270	21	1	1060
Type 1 Weak	415	135	13	0	563

Table 5.13: Class Group Rank Statistics for L_1 , $p = 3$, $t = 3$, $p_i \equiv 7 \pmod{24}$.

5.3.2 Quintic extensions

First, we only considered extensions in which only one rational prime congruent to $7 \pmod{8}$ ramifies. Then we were able to find the class group by taking extensions of the real subfield, $\mathbb{Q}(\sqrt{2})$. We computed the class group of the 4084 extensions in which one prime less than 814,000 ramifies.

Category	Rank 0	Rank 1	Rank 2	Rank 3	Total
Type 1 Strong	0	654	24	2	680
Type 1 Weak	0	135	7	0	142
Type 2	3262	0	0	0	3262

Table 5.14: Class Group Rank Statistics for L_1 , $p = 5$, $t = 1$, $p_1 \equiv 31 \pmod{40}$.

Note that 20.13% of the fields were type 1. Of the type 1, 82.73% were strong: all ambiguous ideals were strongly ambiguous. In §6.2.1, our heuristics predict that 1/5 of the fields should be type 1 and 5/6 of type 1 fields should be strongly ambiguous.

We were also able to compute the class groups for extensions in which only one prime congruent to 3 mod 8 ramifies, where the prime was less than 4,500. The extensions were all type 1 and strong.

Category	Rank 1	Rank 2	Rank 3	Rank 4	Total
Type 1 Strong	31	7	2	1	41

Table 5.15: Class Group Rank Statistics for L_1 , $p = 5$, $t = 1$, $p_1 \equiv 11 \pmod{40}$.

5.4 L_2/K_2

We were able to do some computations in the next layer of the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$. Recall that $K_2 = \mathbb{Q}(i, \sqrt[4]{-2})$. Cubic extensions of K_2 are degree 24 fields and so computations are slow.

Rank 0	Rank 1	Rank 2	Rank 3	Total
11	4	9	1	

Table 5.16: Class Group Rank Statistics for L_2 , $p = 3$, $t = 1$, $p_1 \equiv 7 \pmod{24}$

Rank 1	Rank 2	Rank 3	Rank 4	Total
10	5	2	3	

Table 5.17: Class Group Rank Statistics for L_2 , $p = 3$, $t = 1$, $p_1 \equiv 19 \pmod{24}$

We also include the exact results for the unit indices and for the class group for primes less than 500.

p	$\log_3[E_{K_2} : E_{K_2} \cap N_{L_2/K_2}L_2]$	$\log_3[E_{K_2} : N_{L_2/K_2}E_{L_2}]$	Chevalley Rank	A_{L_2}
7	3	3	0	0
31	3	3	0	0
79	2	3	1	1
103	2	3	1	1
127	3	3	0	0
151	1	1	2	2
199	1	1	2	2
223	2	3	1	1
271	3	3	0	0
367	1	3	2	2
439	1	1	2	2
463	3	3	0	0
487	2	2	1	1

Table 5.18: Class Group Rank Statistics for L_2 , $p = 3$, $t = 1$, $p_1 \equiv 7 \pmod{24}$

p	$\log_3[E_{K_2} : E_{K_2} \cap N_{L_2/K_2}L_2]$	$\log_3[E_{K_2} : N_{L_2/K_2}E_{L_2}]$	Chevalley Rank	A_{L_2}
19	2	2	1	1
43	2	2	1	1
67	0	0	3	4
139	2	2	1	1
163	0	2	3	3
211	0	0	3	3
283	2	2	1	1
307	2	2	1	2
331	2	2	1	1
379	2	2	1	1
499	2	2	1	1

Table 5.19: Class Group Rank Statistics for L_2 , $p = 3$, $t = 1$, $p_1 \equiv 19 \pmod{24}$

Chapter 6: Heuristics

In this chapter, we will present heuristics and predictions for the ranks and structure of the class group in the cyclic extensions of fields in the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$. We will take the results proven in Chapters 2 through 4 and use the data computed in Chapter 5 to develop a model for the behavior of the class group in the cyclic extensions.

6.1 L_0/K_0

In this section, we consider cyclic degree p extensions L_0 of $K_0 = \mathbb{Q}(\sqrt{-D})$ such that

$$\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Let p_1, \dots, p_t be the primes of \mathbb{Q} which ramify in L_0/K_0 . Additionally, assume $p_i \neq p$ and if a prime ramifies in K_0/\mathbb{Q} it does not ramify in L_0/K_0 . We let t_s be the number of ramified primes which split in K_0/\mathbb{Q} and t_i be the number of ramified primes which are inert in K_0/\mathbb{Q} : $t_i + 2t_s = t$.

$$\begin{array}{c}
L \\
| \\
p \\
K = \mathbb{Q}(\sqrt{-D}) \\
| \\
2 \\
\mathbb{Q}
\end{array}$$

Recall from §2.1 that the $(\sigma - 1)^2$ -rank of the class group of L_0 is

$$2t - 2 - \text{rank } M$$

where M is the $(2t_s + t_i) \times (2t_s + t_i)$ matrix of Hilbert symbols described in Proposition 2.2. We also know that M has the structure

$$M = \left(\begin{array}{c|c} M_1 & M_2 \\ \hline M_3 & M_4 \end{array} \right)$$

where M_1 is a $2t_s \times 2t_s$ matrix of blocks of the form $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, M_2 is a $2t_s \times t_i$ matrix of blocks of the form $\begin{pmatrix} a \\ a \end{pmatrix}$, M_3 is a $t_i \times 2t_s$ matrix of blocks of the form $\begin{pmatrix} a & a \end{pmatrix}$ and M_4 is a $t_i \times t_i$ matrix with no particular structure. By Hilbert reciprocity, each column of the matrix must sum to zero.

Let

$$D = \begin{pmatrix} I_{t_s} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & 0 \\ 0 & I_{t_i} \end{pmatrix} \\ = \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 1 & -1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & -1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

where I_k is the $k \times k$ identity matrix and \otimes is the Kronecker product and let

$M' = D^{-1}MD$. Then

$$M' = \left(\begin{array}{c|c} M'_1 & M'_2 \\ \hline M'_3 & M'_4 \end{array} \right)$$

Now M'_1 consists of blocks of the form $\begin{pmatrix} a+b & 0 \\ 0 & a-b \end{pmatrix}$, the blocks of M'_2 are of the form $\begin{pmatrix} a \\ 0 \end{pmatrix}$, the blocks of M'_3 become $\begin{pmatrix} -a & 0 \end{pmatrix}$, and $M'_4 = M_4$.

Then note that by rearranging rows and columns, we can decompose M' into a two block-diagonal matrix. One block has dimension $(t_s + t_i) \times (t_s + t_i)$ and the

other has dimension $t_s \times t_s$. See M' below.

As an example, consider a matrix M in the case where there are two primes of \mathbb{Q} that split in K_0 ($t_s = 2$) and two primes that are inert ($t_i = 2$), and so six primes in total ramify in the cubic extension. Order the primes as split followed by inert.

Then we have

$$M = \left(\begin{array}{cc|cc|c|c} m_1 & m_2 & m_3 & m_4 & m_5 & m_6 \\ m_2 & m_1 & m_4 & m_3 & m_5 & m_6 \\ \hline m_7 & m_8 & m_9 & m_{10} & m_{11} & m_{12} \\ m_8 & m_7 & m_{10} & m_9 & m_{11} & m_{12} \\ \hline m_{13} & m_{13} & m_{14} & m_{14} & m_{15} & m_{16} \\ \hline m_{17} & m_{17} & m_{18} & m_{18} & m_{19} & m_{20} \end{array} \right),$$

$$M' = \left(\begin{array}{cc|cc|c|c}
m_1 + m_2 & 0 & m_3 + m_4 & 0 & m_5 & m_6 \\
0 & m_1 - m_2 & 0 & m_3 - m_4 & 0 & 0 \\
\hline
m_7 + m_8 & 0 & m_9 + m_{10} & 0 & m_{11} & m_{12} \\
0 & m_7 - m_8 & 0 & m_9 - m_{10} & 0 & 0 \\
\hline
-m_{13} & 0 & -m_{14} & 0 & m_{15} & m_{16} \\
\hline
-m_{17} & 0 & -m_{18} & 0 & m_{19} & m_{20}
\end{array} \right)$$

$$\sim \left(\begin{array}{cccc|cc}
m_1 + m_2 & m_3 + m_4 & m_5 & m_6 & 0 & 0 \\
m_7 + m_8 & m_9 + m_{10} & m_{11} & m_{12} & 0 & 0 \\
-m_{13} & -m_{14} & m_{15} & m_{16} & 0 & 0 \\
-m_{17} & -m_{18} & m_{19} & m_{20} & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & m_1 - m_2 & m_3 - m_4 \\
0 & 0 & 0 & 0 & m_7 - m_8 & m_9 - m_{10}
\end{array} \right)$$

Therefore since M and M' have the same rank, we can model the probability of M having a given rank as the probability that a matrix of the same form as M' has that rank.

Recall also that by Hilbert reciprocity, each column of M sums to zero. Note that the columns of the upper left block, after multiplying some rows by -1 , are the same as the original column sums of M . Therefore to determine the rank of M we can think of M as being decomposed into two independent matrices, one of dimension $(t_s + t_i - 1) \times (t_s + t_i)$ and one of dimension $t_s \times t_s$.

We therefore know the structure of the matrices that determine the rank of the p -class groups. Now we can determine the probability that a matrix has a given

rank under the assumption that independent Hilbert symbols are equidistributed.

First, consider a random $m \times n$ matrix over \mathbb{F}_p .

Proposition 6.1 (Gerth [10, Theorem 2]). *Let $k, m, n \in \mathbb{N}$ with $k \leq \min\{m, n\}$.*

Let $q = 1/p$ and $(q)_r = \prod_{j=1}^r (1 - q^j)$. Then the number of matrices in $\mathbb{F}_p^{m \times n}$ of rank k is

$$p^{(n+m-k)k} \frac{(q)_n (q)_m}{(q)_{n-k} (q)_{m-k} (q)_k}.$$

Corollary 6.2. *If the entries of the matrices are equidistributed, the probability that an $m \times n$ matrix over \mathbb{F}_p has rank k is*

$$p^{(n+m-k)k - nm} \frac{(q)_n (q)_m}{(q)_{n-k} (q)_{m-k} (q)_k}.$$

We will use the notation $P(X)$ to denote the probability that an event X occurs.

We have the following proposition on the equidistribution of Artin symbols at primes in a particular extension.

Proposition 6.3 ([6, Corollary 8.18]). *Let L be an abelian extension of K , and let \mathfrak{m} be a modulus divisible by all primes that ramify in L . Then, given any element $\sigma \in \text{Gal}(L/K)$, the set of primes \mathfrak{p} not dividing \mathfrak{m} such that $\left(\frac{L/K}{\mathfrak{p}}\right) = \sigma$ has density $1/[L : K]$ and hence is infinite.*

We expect that the Artin symbols we use (and hence the tamely ramified Hilbert symbols) are equidistributed. We cannot apply Proposition 6.3 since we are varying the field as well as the primes at which we're computing the Artin symbol,

but it is still reasonable to assume that the symbols are equidistributed (see [9] and [23]).

Then we have the following proposition due to Wittmann. Note that having only inert primes ramify means that there is no additional structure on the matrix M , and so we can consider it as an arbitrary $(t_i - 1) \times t_i$ matrix.

Define the symbol $\begin{bmatrix} a \\ b \end{bmatrix}_q$ to be the q -binomial coefficient:

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \frac{(q)_a}{(q)_b (q)_{a-b}}$$

where $(q)_k = \prod_{j=1}^k (1 - q^j)$.

Wittmann proves the following result giving the probability that the dimension of $A^{\sigma-1}/A^{(\sigma-1)^2}$ is r when all ramified primes in L_0/K_0 are inert in K_0 . This result in turn gives the probability that the p -rank of A is $t - 1 + r$.

Proposition 6.4 (Wittmann [29, Theorem 4.3]). *Assume $t_i > 0$ and $t_s = 0$. Then for $0 \leq r \leq t_i - 1$, the probability that $\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = r$ is*

$$P\left(\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = r\right) = q^{r^2+r} \begin{bmatrix} t_i - 1 \\ r \end{bmatrix}_q \begin{bmatrix} t_i \\ r + 1 \end{bmatrix}_q (q)_{t_i-1-r}.$$

Now we consider that case where not all of the ramified primes are inert. We determine the probability that a matrix of the form M' has rank $t - 1 - r$, which then gives us the probability that

$$\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = r.$$

M' is equivalent to a block diagonal matrix where each non-zero entry is independent, and there are two blocks: one of dimension $(t_s + t_i - 1) \times (t_s + t_i)$ and one of dimension $t_s \times t_s$.

Therefore to determine the probability that the rank of M' is $t - 1 - r$, we can determine the probability that the rank of a random $(t_s + t_i - 1) \times (t_s + t_i)$ matrix plus the rank of a random $t_s \times t_s$ matrix is $t - 1 - r$.

Proposition 6.5. *Assume $0 \leq r \leq 2t_s + t_i - 1$ and $t_s > 0$. Then*

$$P\left(\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = r\right) = \frac{(q)_{t_s+t_i}(q)_{t_s}}{(q)_{r+1}} \mathcal{S}$$

where \mathcal{S} depends on t_s , t_i and r .

If $r \geq t_s$ and $r \geq t_s + t_i - 1$, then

$$\mathcal{S} = \sum_{k=0}^{2t_s+t_i-1-r} q^\gamma \begin{bmatrix} t_s + t_i - 1 \\ k \end{bmatrix}_q \begin{bmatrix} t_s \\ 2t_s + t_i - 1 - r - k \end{bmatrix}_q \begin{bmatrix} r + 1 \\ t_s + t_i - k \end{bmatrix}_q$$

where $\gamma = 2t_i^2 - 4t_i k - 2t_i r + 4t_i t_s - 3t_i + 2k^2 + 2kr - 4kt_s + 3k - 2rt_s - 3t_s + 1 + 2t_s^2 + r^2 + 2r$.

Otherwise,

$$\mathcal{S} = \sum_{k=0}^{\min\{r, t_s\}} q^{2k^2 - 2kr - k + r^2 + r} \begin{bmatrix} t_s + t_i - 1 \\ r - k \end{bmatrix}_q \begin{bmatrix} t_s \\ k \end{bmatrix}_q \begin{bmatrix} r + 1 \\ k \end{bmatrix}_q.$$

Proof. First, recall that

$$P(\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = r) = P(\text{rank } M = 2t_s + t_i - 1 - r),$$

and because M is equivalent to a $(t_s + t_i - 1) \times (t_s + t_i)$ matrix M_1 and a $t_s \times t_s$ matrix M_2 , we have

$$\begin{aligned} & P(\text{rank } M = 2t_s + t_i - 1 - r) \\ &= \sum_{k=0}^{2t_s+t_i-1-r} P(\text{rank } M_1 = k)P(\text{rank } M_2 = 2t_s + t_i - 1 - r - k). \end{aligned}$$

The probability that an arbitrary $m \times n$ matrix over \mathbb{F}_p has rank k is given by Corollary 6.2. When $k > \min\{m, n\}$, the probability is zero. Therefore

$$k > t_s + t_i - 1 \implies P(\text{rank } M_1 = k) = 0$$

and since

$$2t_s + t_i - 1 - r - k > t_s \iff k < t_s + t_i - 1 - r$$

we have

$$k < t_s + t_i - 1 - r \implies P(\text{rank } M_2 = 2t_s + t_i - 1 - r - k) = 0.$$

Therefore when we're computing the probability

$$P(\text{rank } M = 2t_s + t_i - 1 - r),$$

we should adjust the bounds of the sum, since the formula from Corollary 6.2 is only valid when the rank $r \leq \min(m, n)$. Therefore we need to adjust the upper bound

when

$$t_s + t_i - 1 < 2t_s + t_i - 1 - r \iff r < t_s$$

and we need to adjust the lower bound when

$$2t_s + t_i - 1 - r > t_s \iff r < t_s + t_i - 1.$$

Therefore we will have four cases which we will address separately:

$$r \geq t_s, r \geq t_s + t_i - 1,$$

$$r \geq t_s, r < t_s + t_i - 1,$$

$$r < t_s, r \geq t_s + t_i - 1,$$

$$r < t_s, r < t_s + t_i - 1.$$

Case 1: $r \geq t_s, r \geq t_s + t_i - 1$. In this case, we don't need to adjust either the lower or upper bounds of the sum. Therefore we have

$$\begin{aligned}
& P(\text{rank } M = 2t_s + t_i - 1 - r) \\
&= \sum_{k=0}^{2t_s+t_i-1-r} P(\text{rank } M_1 = k)P(\text{rank } M_2 = 2t_s + t_i - 1 - r - k) \\
&= \sum_{k=0}^{2t_s+t_i-1-r} \frac{q^{(t_s+t_i-1)(t_s+t_i)}}{q^{(2t_s+2t_i-1-k)k}} \frac{(q)_{t_s+t_i-1}(q)_{t_s+t_i}}{(q)_{t_s+t_i-1-k}(q)_{t_s+t_i-k}(q)_k} \\
&\quad \times \frac{q^{t_s^2}}{q^{(r+k+1-t_i)(2t_s+t_i-1-r-k)}} \frac{(q)_{t_s}^2}{(q)_{r+k+1-t_i-t_s}^2 (q)_{2t_s+t_i-1-r-k}} \\
&= \sum_{k=0}^{2t_s+t_i-1-r} q^{\gamma'} \begin{bmatrix} t_s + t_i - 1 \\ k \end{bmatrix}_q \begin{bmatrix} t_s \\ 2t_s + t_i - 1 - r - k \end{bmatrix}_q \frac{(q)_{t_s+t_i}}{(q)_{t_s+t_i-k}} \frac{(q)_{t_s}}{(q)_{r+k+1-t_i-t_s}} \\
&= \frac{(q)_{t_s+t_i}(q)_{t_s}}{(q)_{r+1}} \sum_{k=0}^{2t_s+t_i-1-r} q^{\gamma'} \begin{bmatrix} t_s + t_i - 1 \\ k \end{bmatrix}_q \begin{bmatrix} t_s \\ 2t_s + t_i - 1 - r - k \end{bmatrix}_q \begin{bmatrix} r + 1 \\ t_s + t_i - k \end{bmatrix}_q
\end{aligned}$$

where $\gamma' = 2t_i^2 - 4t_i k - 2t_i r + 4t_i t_s - 3t_i + 2k^2 + 2kr - 4kt_s + 3k - 2rt_s - 3t_s + 1 + 2t_s^2 + r^2 + 2r$.

Assuming fixed values for t_s, t_i and r this gives us a polynomial in q .

Case 2: $r \geq t_s$, $r < t_s + t_i - 1$. Note that this case can only occur only if $t_i > 1$.

Here, we need to adjust the lower bound since $P(\text{rank } M_2 = k) = 0$ for $k < t_s + t_i - 1$.

$$\begin{aligned}
& P(\text{rank } M = 2t_s + t_i - 1 - r) \\
&= \sum_{k=t_s+t_i-1-r}^{2t_s+t_i-1-r} P(\text{rank } M_1 = k)P(\text{rank } M_2 = 2t_s + t_i - 1 - r - k) \\
&= \sum_{k=0}^{t_s} P(\text{rank } M_1 = t_s + t_i - 1 - r + k)P(\text{rank } M_2 = t_s - k) \\
&= \sum_{k=0}^{t_s} \frac{q^{(t_s+t_i-1)(t_s+t_i)}}{q^{(t_s+t_i+r-k)(t_s+t_i-1-r+k)}} \frac{(q)_{t_s+t_i-1}(q)_{t_s+t_i}}{(q)_{r-k}(q)_{r+1-k}(q)_{t_s+t_i-1-r+k}} \frac{q^{t_s^2}}{q^{(t_s+k)(t_s-k)}} \frac{(q)_{t_s}^2}{(q)_k^2 (q)_{t_s-k}} \\
&= \frac{(q)_{t_s+t_i}(q)_{t_s}}{(q)_{r+1}} \sum_{k=0}^{t_s} q^{2k^2-2kr-k+r^2+r} \begin{bmatrix} t_s + t_i - 1 \\ r - k \end{bmatrix}_q \begin{bmatrix} t_s \\ k \end{bmatrix}_q \begin{bmatrix} r + 1 \\ k \end{bmatrix}_q
\end{aligned}$$

Case 3: $r < t_s$, $r \geq t_s + t_i - 1$. This case occurs only if $t_i = 0$ and $r = t_s - 1$.

Therefore

$$2t_s + t_i - 1 - r = t_s.$$

In this case we need to adjust the upper bound.

$$\begin{aligned}
& P(\text{rank } M = 2t_s + t_i - 1 - r) = P(\text{rank } M = t_s) \\
&= \sum_{k=0}^{t_s-1} P(\text{rank } M_1 = k)P(\text{rank } M_2 = t_s - k) \\
&= \sum_{k=0}^{t_s-1} \frac{q^{(t_s-1)(t_s)}}{q^{(2t_s-1-k)k}} \frac{(q)_{t_s-1}(q)_{t_s}}{(q)_{t_s-1-k}(q)_{t_s-k}(q)_k} \frac{q^{t_s^2}}{q^{(t_s+k)(t_s-k)}} \frac{(q)_{t_s}^2}{(q)_k^2 (q)_{t_s-k}} \\
&= (q)_{t_s} \sum_{k=0}^{t_s-1} q^{t_s^2-t_s-2t_s k+k+2k^2} \begin{bmatrix} t_s - 1 \\ k \end{bmatrix}_q \begin{bmatrix} t_s \\ k \end{bmatrix}_q^2
\end{aligned}$$

Plugging in $r = t_s - 1$ and $t_i = 0$ into the equation in the statement of the proposition matches this result.

Case 4: $r < t_s$, $r < t_s + t_i - 1$. Here both bounds need to be adjusted:

$$\begin{aligned}
& P(\text{rank } M = 2t_s + t_i - 1 - r) \\
&= \sum_{k=t_s+t_i-1-r}^{t_s+t_i-1} P(\text{rank } M_1 = k)P(\text{rank } M_2 = 2t_s + t_i - 1 - r - k) \\
&= \sum_{k=0}^r P(\text{rank } M_1 = t_s + t_i - 1 - r + k)P(\text{rank } M_2 = t_s - k) \\
&= \sum_{k=0}^r \frac{q^{t_s^2 - t_s + 2t_s t_i + t_i^2 - t_i}}{q^{(t_s+t_i+r-k)(t_s+t_i-1-r+k)}} \frac{(q)_{t_s+t_i-1}(q)_{t_s+t_i}}{(q)_{r-k}(q)_{r+1-k}(q)_{t_s+t_i-1-r+k}} \frac{q^{t_s^2}}{q^{(t_s+k)(t_s-k)}} \frac{(q)_{t_s}^2}{(q)_k^2 (q)_{t_s-k}} \\
&= \sum_{k=0}^r \frac{q^{2t_s^2 - t_s + 2t_s t_i + t_i^2 - t_i}}{q^{2t_s^2 - t_s + 2t_s t_i + t_i^2 - k^2 + 2kr + k - r^2 - r - k^2}} \begin{bmatrix} t_s + t_i - 1 \\ r - k \end{bmatrix}_q \begin{bmatrix} t_s \\ k \end{bmatrix}_q \frac{(q)_{t_s+t_i}(q)_{t_s}}{(q)_{r+1-k}(q)_k} \\
&= \frac{(q)_{t_s+t_i}(q)_{t_s}}{(q)_{r+1}} \sum_{k=0}^r q^{2k^2 - 2kr - k + r^2 + r} \begin{bmatrix} t_s + t_i - 1 \\ r - k \end{bmatrix}_q \begin{bmatrix} t_s \\ k \end{bmatrix}_q \begin{bmatrix} r + 1 \\ k \end{bmatrix}_q
\end{aligned}$$

□

Given the above proposition, we can determine the probability that the rank is r as $t_s \rightarrow \infty$.

Corollary 6.6. *For $r \geq 0$,*

$$\begin{aligned}
& \lim_{t_s \rightarrow \infty} P\left(\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = r\right) \\
&= \frac{(q)_\infty^2}{(q)_r (q)_{r+1}} \sum_{k=0}^r q^{2k^2 - 2rk - k + r^2 + r} \begin{bmatrix} r \\ k \end{bmatrix}_q \begin{bmatrix} r + 1 \\ k \end{bmatrix}_q.
\end{aligned}$$

In particular,

$$\lim_{t_s \rightarrow \infty} P\left(\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = 0\right) = \frac{(q)_{\infty}^2}{(q)_1}.$$

Corollary 6.7. For $p = 3$,

$$\lim_{t_s \rightarrow \infty} P\left(\dim_{\mathbb{F}_p}(A^{\sigma-1}/A^{(\sigma-1)^2}) = 0\right) \approx 0.4706.$$

We also compute the expected probabilities for the 3-rank of the class group for some cases. See Tables 6.1, 6.2, and 6.3.

$t_s \backslash t_i$	0	1	2	3	4	$\rightarrow \infty$
0	0	1	0.8889	0.8560	0.8454	0.8402
1	0.6667	0.5926	0.5706	0.5636	0.5613	0.5601
2	0.5267	0.5072	0.5010	0.4989	0.4982	0.4979
3	0.4885	0.4824	0.4804	0.4798	0.4796	0.4794
4	0.4765	0.4745	0.4739	0.4736	0.4736	0.4735

Table 6.1: $P(3\text{-rank} = 2t_s + t_i - 1)$

$t_s \backslash t_i$	0	1	2	3	4	$\rightarrow \infty$
0	0	0	0.1111	0.1427	0.1526	0.1575
1	0.3333	0.3704	0.3804	0.3836	0.3846	0.3851
2	0.4170	0.4227	0.4244	0.4250	0.4252	0.4253
3	0.4342	0.4355	0.4360	0.4361	0.4361	0.4362
4	0.4390	0.4394	0.4395	0.4395	0.4395	0.4396

Table 6.2: $P(3\text{-rank} = 2t_s + t_i)$

$t_s \backslash t_i$	0	1	2	3	4	$\rightarrow \infty$
0	0	0	0	0.0014	0.0020	0.0023
1	0	0.0370	0.0485	0.0522	0.0534	0.0540
2	0.0549	0.0677	0.0719	0.0733	0.0737	0.0740
3	0.0743	0.0785	0.0799	0.0804	0.0806	0.0806
4	0.0808	0.0822	0.0826	0.0828	0.0829	0.0829

Table 6.3: $P(3\text{-rank} = 2t_s + t_i + 1)$

6.2 L_1/K_1

In the previous section we presented heuristics for the behavior of the p -class group in cyclic degree p extensions of $K_0 = \mathbb{Q}(i)$. Here, we'll go up a layer in the anti-cyclotomic \mathbb{Z}_2 -extension. We will restrict to the case where all primes which ramify in L_1/K_1 are inert in K_0/\mathbb{Q} . This is because of Proposition 3.1: if a prime is inert in K_0/\mathbb{Q} then it splits completely in the anti-cyclotomic extension of K_0 , which will induce growth in the p -ranks of the class groups. We will present some heuristics for the behavior of the p -class group of L_1/K_1 , where $K_1 = \mathbb{Q}(\zeta_8)$ and L_1 is a cyclic degree p extension such that $\text{Gal}(L_1/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}^2 \times \mathbb{Z}/p\mathbb{Z}$. Note that this is the first step in the cyclotomic extension of $\mathbb{Q}(i)$ as well as the first step in the anti-cyclotomic extension of $\mathbb{Q}(i)$.

We will let p_1, \dots, p_t be the rational primes which ramify in L_1/K_1 . Since L_1/K_1 is the lift of an abelian number field, all primes which ramify are congruent to 1 mod p , and since we're only considering primes that are inert in $\mathbb{Q}(i)/\mathbb{Q}$, they must also be congruent to 3 mod 4. However, we will actually have two distinct cases: primes that are 3 mod 8 and primes that are 7 mod 8.

By Proposition 4.1, if all primes that ramify in L_1/K_1 are over primes congruent to $3 \pmod{8}$, we have $e = 0$ and all ambiguous ideals are strongly ambiguous. There is no similar result for primes $7 \pmod{8}$. In this case we will need a separate result to determine if, when the unit is the norm of an element of L_1 , it is in fact the norm of a unit.

Note that Proposition 4.1 also implies that the local norm residue symbols at primes congruent to $3 \pmod{8}$ are trivial. Therefore, when trying to determine if the unit is a global norm, we only need to compute the norm residue symbols at primes which are $7 \pmod{8}$.

6.2.1 Strongly ambiguous ideals

There is one remaining piece to the heuristic model: we need to understand when the ambiguous ideals are all strongly ambiguous. If they are not, then we require an additional generator, as discussed in Chapter 3. Recall that $K_1 = \mathbb{Q}(\zeta_8)$. We will address the general case, where L_1/K_1 is a cyclic degree $p \neq 2$ extension.

By Proposition 4.1, if a ramified prime is congruent to $3 \pmod{8}$, we know already that the unit of K_1 is the norm of a unit in L_1 and therefore all ambiguous ideals are strongly ambiguous.

Here, we present a theory for when there is no local obstruction to the unit being the norm of a unit. In other words, we assume that the unit is the norm of an element in L_1 (which means the local norm residue symbols are all trivial), and then look to see if the unit is the norm of a unit.

By Theorem 4.5, the difference between the structure of the units in the two cases depends on how the module decomposes into submodules. In particular, let $G = \text{Gal}(L/\mathbb{Q}) = \langle \sigma \rangle$ and let $R = (\mathbb{Z}/p\mathbb{Z})[G]$. Then

$$U_L \simeq \begin{cases} (R/(\sigma - 1)^{p-1}R) \oplus (R/(\sigma + 1)R) \oplus (R/(\sigma + 1)^{p-1}R) \text{ or} \\ (R/(\sigma - 1)^{p-1}R) \oplus (R/(\sigma + 1)^pR) \end{cases}$$

We can consider $U_L/U_{L'}$, i.e. we can ignore the $R/(\sigma - 1)^{p-1}R$ term since it does not affect the norm to K .

If $U_L/U_{L'} \simeq R/(\sigma + 1)^pR$, then we can represent it as a $p \times p$ matrix whose Jordan form is

$$J = \begin{pmatrix} -1 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & 1 \\ 0 & 0 & 0 & \dots & 0 & -1 \end{pmatrix}.$$

Lemma 6.8. *The number of matrices with Jordan form J is*

$$\frac{|GL_p(\mathbb{F}_p)|}{(p-1)p^{p-1}}.$$

Proof. To count how many possible matrices have this Jordan form, we find the

matrices Q such that

$$QJQ^{-1} = J.$$

By solving the system $QJ = JQ$, we find that Q must have the form

$$\begin{pmatrix} q_1 & q_2 & q_3 & \cdots & q_{p-1} & q_p \\ 0 & q_1 & q_2 & \cdots & q_{p-2} & q_{p-1} \\ 0 & 0 & q_1 & \cdots & q_{p-3} & q_{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q_1 & q_2 \\ 0 & 0 & 0 & \cdots & 0 & q_1 \end{pmatrix}.$$

Therefore, since Q must have non-zero determinant, $q_1 \in \mathbb{F}_p^\times$. For $i > 1$, $q_i \in \mathbb{F}_p$, so there are $(p-1)p^{p-1}$ such matrices. This is the size of the stabilizer, and therefore there are $\frac{|GL_p(\mathbb{F}_p)|}{(p-1)p^{p-1}}$ matrices with this Jordan form. \square

On the other hand, if $U_L/U_{L'} \simeq R/(\sigma+1)R \oplus R/(\sigma+1)^{p-1}R$, then its Jordan

form should be a $p \times p$ matrix

$$J' = \begin{pmatrix} -1 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & -1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & -1 \end{pmatrix}.$$

Lemma 6.9. *The number of matrices with Jordan form J' is*

$$\frac{|GL_p(\mathbb{F}_p)|}{(p-1)^2 p^p}.$$

Proof. Solving the system

$$Q' J' = J' Q',$$

we find that Q' must have the form

$$\begin{pmatrix} q'_1 & q'_2 & q'_3 & \dots & q'_{p-1} & q'_p \\ 0 & q'_1 & q'_2 & \dots & q'_{p-2} & 0 \\ 0 & 0 & q'_1 & \dots & q'_{p-3} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & q'_1 & 0 \\ 0 & 0 & 0 & \dots & q'_{p+1} & q'_{p+2} \end{pmatrix}.$$

Here $q'_1, q'_{p+2} \in \mathbb{F}_p^\times$ and for $i \neq 1, p+2$, $q'_i \in \mathbb{F}_p$. □

Now, we make a heuristic guess. It's clear from the data for the cubic and quintic extensions (see §5.3), that the ratio of strong type 1 fields to weak type 1 fields should be $p : 1$. The explanation above using the module structure gives us a ratio of $p(p-1) : 1$. However, the matrices above correspond to all $p-1$ non-split extensions. By Proposition 4.6 and Theorem 4.5, we know there are $p-1$ non-split extensions and therefore we propose that we have over-counted by a factor of $p-1$, which gives us $\frac{|GL_p(\mathbb{F}_p)|}{(p-1)p^p}$ matrices per extension. This gives us a ratio of $p : 1$ and therefore we expect the unit to be the norm of a unit with probability

$$\frac{p}{p+1}.$$

6.2.2 One rational prime ramifies

Let's consider the case where only primes above one rational prime ramify ($t = 1$). We consider only primes which are inert in K_0 and therefore split in K_1/K_0 . These primes will either both be type 1 ($e = 0$) or both be type 2 ($e = 1$). For the type 1 primes, we will also need to consider if the ambiguous ideal classes are all strongly ambiguous. If not, we need to find an extra generator for A^Δ .

$\mathfrak{p}_1 \equiv 3 \pmod{8}$. If the ramified prime is congruent to 3 mod 8, then we know that the unit is always the norm of a unit by Proposition 4.1. Therefore in this case, the prime is type 1 ($e = 0$) and so all ambiguous ideals are strongly ambiguous.

Therefore all our Artin symbol matrices (a_{ij}) from Chapter 3 are of the form

$$\begin{pmatrix} a & -a \\ -a & a \end{pmatrix}.$$

Under the assumption that the Artin symbols are equidistributed (see §6.1), we expect the matrix to be all zero with probability $1/p$ and to otherwise have rank 1.

Now consider the $p = 3$ case, so the ramified prime p_1 is congruent to 19 mod 24.

Recall that by Theorem 3.5, the 3-rank is given by

$$2(2t - 1 - e) - \text{rank } M = 2 - \text{rank } M.$$

Therefore we expect $1/3$ of fields to have rank 2 and the remainder to have rank 1.

Rank 1	Rank 2
$2/3$	$1/3$

Table 6.4: Expected Rank Probabilities for $t = 1, p_1 \equiv 3 \pmod{8}$

$p_1 \equiv 7 \pmod{8}$. Now let's go back to the general p case and consider fields where the ramified prime is congruent to 7 mod 8, and so we cannot apply Proposition 4.1.

First, consider the case where the prime is type 1. Then \mathfrak{P}_1 and \mathfrak{P}_2 generate the ambiguous ideal class group.

If we're in the strong case, then all ambiguous ideals are strongly ambiguous, and the ramified primes generate A^Δ . Therefore the matrix as developed in Theorem

3.5 has the form

$$\begin{pmatrix} a & -a \\ -a & a \end{pmatrix}$$

since we know that each row must sum to zero by Hilbert reciprocity.

If these ideals are not all strongly ambiguous, then we require an additional generator for A^Δ which we call \mathfrak{P}_0 .

However, in the case where $e = 0$, we have $|A^\Delta| = 3^{2t-1} = 3$. Since $\mathfrak{P}_1, \mathfrak{P}_2 \in A^\Delta$, if they do not generate A^Δ , they must both be trivial. So for $t = 1$, we have the special case where if we require an extra generator \mathfrak{P}_0 , that means both \mathfrak{P}_1 and \mathfrak{P}_2 generate the trivial class. Furthermore, if the ideal class generated by \mathfrak{P}_i is trivial, then the Artin map will send it to the trivial Galois element in $\text{Gal}(\tilde{L}/L)$, which means the row in the matrix M is all zeros (see Theorem 3.5). Therefore we have a matrix of the form

$$\begin{pmatrix} a & -a \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

since again, each row of the matrix must sum to zero.

We now want to consider 3×2 matrices where the bottom two rows correspond to the ramified primes and the top row corresponds to an additional prime ideal class. We do this so we can treat the strong and weak cases uniformly.

In the weak case, the top row corresponds to the generator of A^Δ since the ramified primes don't generate. In the strong case, the top row is just a random prime ideal class. In the strong case, since one of the bottom two rows corresponds

to the generator, the top row must be a linear combination of the bottom two rows.

Let's assume we have a matrix of symbols of the form

$$\begin{pmatrix} a & -a \\ b & -b \\ -b & b \end{pmatrix}.$$

For the case where all ambiguous ideals are strong, possible matrices are

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

In the weak case, where we require an additional generator, the possible matrices are

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Let X be the event that the matrix is

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

We again make the assumption that the Artin symbols are equidistributed.

Ignoring the strong/weak distinction, we should have $P(X) = 1/9$ since we have

two independent parameters and so 9 possible matrices. We use this to determine the probabilities for the matrix rank in the strong and weak cases. First, note that

$$P(X) = P(X|\text{strong})P(\text{strong}) + P(X|\text{not strong})P(\text{not strong}).$$

From §6.2.1, we have $P(\text{strong}) = 3/4$ and $P(\text{not strong}) = 1/4$. We also know $P(X|\text{strong}) = 0$, since the top row is not a linear combination of the other two rows. Therefore we have

$$1/9 = P(X|\text{not strong})(1/4) \implies P(X|\text{not strong}) = 4/9.$$

By the same argument, we get the same probability for the matrix

$$\begin{pmatrix} 2 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Now let Y be the event that the matrix is

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

This is the only remaining matrix possible in the ‘not strong’ case and since the

previous cases had probabilities adding up to $8/9$, we must have

$$P(Y|\text{not strong}) = 1/9.$$

Then

$$P(Y) = P(Y|\text{strong})P(\text{strong}) + P(Y|\text{not strong})P(\text{not strong})$$

$$1/9 = P(Y|\text{strong})(3/4) + (1/9)(1/4)$$

Therefore $P(Y|\text{strong}) = 1/9$.

So in both cases, we have probability $1/9$ that the matrix is all zero. The all-zero matrix means the 3-rank of A is

$$2t - 1 + 2t - 1 - \text{rank } M = 2 - 1 + 2 - 1 - 0 = 2.$$

The only other choice is to have a matrix with rank 1, which means the 3-rank is 1. Therefore for a type 1 prime, we expect $1/9$ of fields to have rank 2 and $8/9$ of fields to have rank 1.

This intuitively makes sense. The strong/not strong distinction changes how we find the generators of the ambiguous class group but does not actually change the structure of the class group. It is reasonable to expect that the probability that the class group has a particular rank should be independent of whether or not the

ramified primes generate the entire ambiguous class group.

On the other hand, if we have just one type 2 prime ($e = 1$), the matrix M is a 2×1 matrix. We also have the condition that each row sums to zero, and so there is only one possible matrix:

$$M = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Therefore all fields have 3-rank

$$2t - 2 + 2t - 2 - \text{rank } M = 0.$$

	Rank 0	Rank 1	Rank 2
Type 1 Strong	0	8/9	1/9
Type 1 Weak	0	8/9	1/9
Type 2	1	0	0

Table 6.5: Expected Rank Probabilities for $t = 1$, $p_1 \equiv 7 \pmod{8}$

6.2.3 At least one type 2 prime

The presence of an additional generator in the case where the ambiguous ideals are not all strongly ambiguous makes general heuristics more difficult, since the matrix lacks symmetry. However, for a given t , we could use the general format of the matrix to predict the rank.

But as t increases, it becomes increasingly likely that the unit is not the norm

of an element in L_1 , since that would require that the local norm residue symbol at each ramified prime be trivial. If t rational primes ramify in L/K , we expect all of the local norm residue symbols to be trivial with probability

$$1/3^t.$$

Therefore the dominant case will be Case 2, in which $e = 1$. As described in §3.2, in this case we expect the matrix to have the form

$$M = \left(M_1 \mid M_2 \right)$$

where M_1 is a $2t \times (2t - 2)$ matrix of blocks of the form

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

and M_2 is a $2t \times 1$ matrix of blocks of the form

$$\begin{pmatrix} c \\ c \end{pmatrix}.$$

To understand the structure of this matrix better, append a column of zeros to the matrix so it becomes a square $2t \times 2t$ matrix.

Let

$$D = \left(I_t \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right).$$

Then

$$M' = D^{-1}MD = \left(M'_1 \middle| M'_2 \right)$$

where M'_1 consists of blocks $\begin{pmatrix} a+b & 0 \\ 0 & a-b \end{pmatrix}$ and the blocks of M'_2 are of the form $\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix}$.

The two columns of M'_2 are equal. Since we also have the condition that the rows of M sum to zero, by Hilbert reciprocity, the rows which contain the $a + b$ terms in M'_1 sum to zero. Therefore we can decompose M' into two independent matrices, just as in §6.1, so that we have two $t \times (t - 1)$ independent matrices.

Proposition 6.10. *Let $t_2 > 0$. Define $\gamma = 2t^2 + 2k^2 - 4tk + 4k + 2 + 3r + 2rk - 2tr + r^2 - 4t$. Then*

$$P(\text{rank } A_1 = 2t - 2 + r) = \begin{cases} \frac{(q)_t(q)_{t-1}}{(q)_{r+1}} \sum_{k=0}^{2t-2-r} q^\gamma \begin{bmatrix} t \\ k \end{bmatrix}_q \begin{bmatrix} t-1 \\ 2t-2-r-k \end{bmatrix}_q \begin{bmatrix} r+1 \\ t-1-k \end{bmatrix}_q & \text{if } r \geq t - 1 \\ \frac{(q)_t(q)_{t-1}}{(q)_{r+1}} \sum_{k=0}^r q^{2k^2+r^2+r} \begin{bmatrix} t-1 \\ r-k \end{bmatrix}_q \begin{bmatrix} t \\ k+1 \end{bmatrix}_q \begin{bmatrix} r+1 \\ k \end{bmatrix}_q & \text{if } r < t - 1. \end{cases}$$

Proof. The rank of A_1 , when $t_2 > 0$, is $2t - 2 + 2t - 2 - \text{rank } M$. Therefore we wish to consider the probability that $\text{rank } M = 2t - 2 - r$.

As before, we can decompose M into two submatrices, which we call \hat{M}_1 and \hat{M}_2 , which can each have rank $0 \leq r \leq t - 1$.

First, consider the case where $r \geq t - 1 \implies 2t - 2 - r \leq t - 1$. Then

$$\begin{aligned}
& P(\text{rank } M = 2t - 2 - r) \\
&= \sum_{k=0}^{2t-2-r} P(\text{rank } \hat{M}_1 = k)P(\text{rank } \hat{M}_2 = 2t - 2 - r - k) \\
&= \sum_{k=0}^{2t-2-r} q^\gamma \frac{(q)_t^2 (q)_{t-1}^2}{(q)_{t-k} (q)_{t-1-k} (q)_k (q)_{t-(2t-2-r-k)} (q)_{t-1-(2t-2-r-k)} (q)_{2t-2-r-k}} \\
&= \frac{(q)_t (q)_{t-1}}{(q)_{r+1}} \sum_{k=0}^{2t-2-r} q^\gamma \begin{bmatrix} t \\ k \end{bmatrix}_q \begin{bmatrix} t-1 \\ 2t-2-r-k \end{bmatrix}_q \begin{bmatrix} r+1 \\ t-1-k \end{bmatrix}_q.
\end{aligned}$$

Now, consider $r < t - 1 \implies 2t - 2 - r > t - 1$. Then

$$\begin{aligned}
& P(\text{rank } M = 2t - 2 - r) \\
&= \sum_{k=t-1-r}^{t-1} P(\text{rank } \hat{M}_1 = k)P(\text{rank } \hat{M}_2 = 2t - 2 - r - k) \\
&= \sum_{k=0}^r P(\text{rank } \hat{M}_1 = t - 1 - r + k)P(\text{rank } \hat{M}_1 = t - 1 - k) \\
&= \sum_{k=0}^r q^{2k^2+r^2+r} \frac{(q)_t^2 (q)_{t-1}^2}{(q)_{1+r-k} (q)_{r-k} (q)_{t-1-r+k} (q)_{1+k} (q)_k (q)_{t-1-k}} \\
&= \frac{(q)_t (q)_{t-1}}{(q)_{r+1}} \sum_{k=0}^r q^{2k^2+r^2+r} \begin{bmatrix} t-1 \\ r-k \end{bmatrix}_q \begin{bmatrix} t \\ k+1 \end{bmatrix}_q \begin{bmatrix} r+1 \\ k \end{bmatrix}_q.
\end{aligned}$$

□

Recall that the 3-rank of the class group of L_1 when $t_2 > 0$ is

$$2t - 2 + 2t - 2 - \text{rank } M.$$

Therefore

$$P(\text{rank } A = 2t - 2 + r) = P(\text{rank } M = 2t - 2 - r).$$

For $t = 2$, we have

$$P(\text{rank } A = 2) = P(r = 0) = 1 - 2q^2 + q^4$$

$$P(\text{rank } A = 3) = P(r = 1) = 2q^2 - 2q^4$$

$$P(\text{rank } A = 4) = P(r = 2) = q^4$$

For $p = 3$,

$$P(\text{rank } A = 2) = 64/81 \approx 0.7901$$

$$P(\text{rank } A = 3) = 16/81 \approx 0.1975$$

$$P(\text{rank } A = 4) = 1/81. \approx 0.0123$$

When $t = 2$, with both primes type 1 ($t_2 = 0$) and congruent to 7 mod 8, we will just address the probability that the matrix is full rank, since this is the most likely outcome. The 7 mod 8 condition means that we expect the unit to be the norm of a unit with probability

$$P(\text{strong}) = 3/4.$$

We use much of the same reasoning as in §6.2.2. In this case, we can think of the matrix as having the form

$$\begin{pmatrix} a & b & c & -a - b - c \\ -d - e - f & d & e & f \\ d & -d - e - f & f & e \\ g & h & -g - h - j & j \\ h & g & j & -g - h - j \end{pmatrix}.$$

where the first row corresponds to the extra generator in the not strong (i.e. weak) case, and is a linear combination of the other rows in the strong case. Each variable in $\{a, \dots, j\}$ should be uniformly distributed if we assume the equidistribution of the Artin symbols. Recall that in the strong case, the ramified primes generate the entire ambiguous ideal class, and in the weak case, we require an extra generator. Consider matrices where the submatrix consisting of the bottom four rows has rank 3 (which is its maximal possible rank). This can only occur in the strong case; otherwise, the ramified primes would generate the ambiguous class group.

Over $\mathbb{Z}/3\mathbb{Z}$, there are 384 possible 4×4 matrices of the form of the bottom submatrix which have rank 3. There are 3^3 possibilities for the top row. Let X be the event that the matrix has this structure. Therefore, assuming equidistribution,

$$P(X) = \frac{3^3 \times 384}{3^9} = \frac{384}{729}.$$

Now this probability is for all matrices, regardless of if they correspond to the strong

or not strong case. Recall that this matrix only occurs in the strong case. Then

$$P(X) = P(X|\text{strong})P(\text{strong})$$

and since $P(\text{strong}) = 3/4$,

$$P(X|\text{strong}) = \frac{1536}{2187} \approx 0.7023.$$

Now, just as in §6.2.2, the probability that the class group is a certain rank should be independent of the strong/weak condition, since that condition only tells us if the ramified primes generate the ambiguous ideals. The condition should not affect the rank of the class group. Therefore we expect

$$P(X|\text{not strong}) = \frac{1536}{2187} \approx 0.7023.$$

The 3-rank when $t_2 = 0$ is given by

$$2t - 1 + 2t - 1 - \text{rank } M = 6 - \text{rank } M.$$

Therefore when the matrix has rank 3, the 3-rank of the class group is 3. Therefore when $t_2 = 0$ we expect 70.23% of the fields to have rank 3.

On the other hand, if two primes ramify and are both congruent to 3 mod 8,

then we know the unit is always the norm of a unit:

$$P(\text{strong}) = 1.$$

Therefore since

$$P(X) = P(X|\text{strong})P(\text{strong}),$$

and we know

$$P(X) = \frac{384}{729},$$

we have

$$P(X|\text{strong}) = \frac{384}{729} \approx 0.5267.$$

Finally, in the case where one prime is $3 \pmod 8$ and one is $7 \pmod 8$, we have

$$P(\text{strong}) = 3/4$$

since we do not have local conditions forcing the unit to always be the norm of a unit. Therefore we again have

$$P(X) = \frac{1536}{2187} \approx 0.7023.$$

This last probability doesn't match the obtained data very well (see Table [5.3.1](#)), so perhaps a modification to our heuristic model is required here.

6.3 L_n/K_n

Let K_n be the n^{th} layer in the anti-cyclotomic \mathbb{Z}_2 -extension of $K_0 = \mathbb{Q}(i)$. Let L_n/K_n be a cyclic cubic extension, and let p_1, \dots, p_t be the primes dividing the relative discriminant of L_n/K_n . Our goal here is to develop a model for how often we should expect the units in K_n to be the norms of element in L_n . We expect that the norm residue symbols should be equidistributed, and therefore we can use the matrix structure developed in Chapter 4 to derive probabilities that the units are norms. Recall also that by Theorem 4.13 the matrices of norm residue symbols for the relative units mod p^{th} powers either had full rank or were rank zero, which means that either all of the units are norms or none of them are.

We begin by reviewing our results for L_0/K_0 and L_1/K_1 and then move on to the general case of L_n/K_n .

There are no fundamental units in K_0 .

There is one fundamental unit in K_1 . To determine if it is the norm of an element in L_1 , we compute norm residue symbols. We know the norm residue symbols are trivial at primes that are $19 \pmod{24}$. Let $0 \leq s \leq t$ be the number of rational primes below the ramified primes in L_1/K_1 that are congruent to $7 \pmod{24}$. There are then s independent symbols, all of which must be trivial in order for the fundamental unit to be a global norm.

More generally, there are 2^{n-1} units added in K_n , the relative units mod cubes. By Theorem 4.13, for $n \geq 2$, either all of the relative units in K_n are norms of elements in L_n modulo cubes or none of them are, and there are 2^{n-2} independent

norm residue symbols which determine if the units are norms.

Under the assumption that norm residue symbols are equidistributed, we can compute the probabilities that the relative units mod cubes are norms. Write X_n for the event that the relative units in K_n are all norms of element in L_n .

$$\begin{aligned} K_1: & P(X_1) = 1/3^s \\ K_2: & P(X_2) = 1/3^t \\ K_3: & P(X_3) = 1/3^{2t} \\ K_4: & P(X_4) = 1/3^{4t} \\ K_n: & P(X_n) = 1/3^{2^{n-2}t} \end{aligned}$$

The probability that none of the units are norms in K_n is the product of the probabilities that none of the relative units are norms in K_j for $1 \leq j \leq n$.

By Chevalley, we have

$$\text{rank } A_n^\Delta = 2^n t - 1 - e_n$$

where e_n is given by the rank of the matrix of norm residue symbols for the units. This assumes that 3 does not divide $h(K_n)$ (which is quite possibly true), and in fact, our heuristics are developed under that assumption. If 3 does divide $h(K_n)$, then these heuristics apply to the class group of L_n excluding the contribution from K_n .

For K_n , we expect that the matrix corresponding to the relative units is zero with probability $1/3^{2^{n-2}t}$ for $n \geq 2$ and probability $1/3^s$ for $n = 1$. On the other hand, we expect that the matrix is full rank (i.e. rank 2^{n-1}) with probability $1 - 1/3^{2^{n-2}t}$ for $n \geq 2$ and probability $1 - 1/3^s$ for $n = 1$.

Now note that the probability that the matrix is full rank at each step (which means e_n is maximal) is

$$(1 - 1/3^s) \prod_{j=1}^n (1 - 1/3^{2^j t}).$$

We can compute the probabilities in the limit as $n \rightarrow \infty$.

When $s = t$, we have

$$t = 1: \quad \lim_{n \rightarrow \infty} (1 - 1/3) \prod_{j=1}^n (1 - 1/3^{2^j}) \approx 0.390125.$$

$$t = 2: \quad \lim_{n \rightarrow \infty} (1 - 1/3^2) \prod_{j=1}^n (1 - 1/3^{2 \times 2^j}) \approx 0.780250.$$

$$t = 3: \quad \lim_{n \rightarrow \infty} (1 - 1/3^3) \prod_{j=1}^n (1 - 1/3^{3 \times 2^j}) \approx 0.926024.$$

$$t = 4: \quad \lim_{n \rightarrow \infty} (1 - 1/3^4) \prod_{j=1}^n (1 - 1/3^{4 \times 2^j}) \approx 0.949768.$$

When e_n is maximal, i.e. $e_n = 2^n - 1$, we have

$$\text{rank } A_n^\Delta = 2^n t - 2^n.$$

For $t = s = 1$, this gives $\text{rank } A_n^\Delta = 0$ which means we expect in the limit that 39% of fields will have trivial class group up the tower.

When $s = 0$, we know the unit of K_1 is always the norm of a unit in L_1 . Then we have

$$t = 1: \quad \lim_{n \rightarrow \infty} \prod_{j=1}^n (1 - 1/3^{2^j}) \approx 0.585187.$$

$$t = 2: \quad \lim_{n \rightarrow \infty} \prod_{j=1}^n (1 - 1/3^{2 \times 2^j}) \approx 0.877781.$$

$$t = 3: \quad \lim_{n \rightarrow \infty} \prod_{j=1}^n (1 - 1/3^{3 \times 2^j}) \approx 0.961640.$$

$$t = 4: \quad \lim_{n \rightarrow \infty} \prod_{j=1}^n (1 - 1/3^{4 \times 2^j}) \approx 0.987504.$$

Now, e_n is at most $2^n - 2$ since the unit of K_1 is always the norm of a unit. Therefore we have $\text{rank } A_n^\Delta = 2^n t - 2^n + 1$. Therefore for $t = 1$, we expect in the limit that 59% of fields will have class group $\mathbb{Z}/3\mathbb{Z}$ up the tower.

We can explicitly compute the probability that $e_n = b$ for $0 \leq b \leq 2^n - 1$ by writing b in binary: $b = b_k b_{k-1} \dots b_1 b_0$. Then each b_j in the binary representation corresponds to contribution of the units in K_{j+1} .

For example, say $t = s = 1$ and $n = 3$ and we wish to compute the probability that $e_3 = 5$. Since each set of relative units are either all norms or none of them are, e_3 can only equal 5 if the unit in K_1 is a norm and the four units in K_3 are norms:

$$P = (1 - 1/3)(1/3)(1 - 1/9) = 16/81.$$

We now consider what this tells us about the rank of A^Δ . By Lemma 4.12, we have an increasing sequence

$$\dots \subseteq N_{L_n/K_n} L_n^\times \cap E_{K_n} \subseteq N_{L_{n+1}/K_{n+1}} L_{n+1}^\times \cap E_{K_{n+1}} \subseteq \dots$$

For $n \geq 2$, the probability that there is a strict increase from step n to step $n + 1$ is

$$1/3^{2^{n-1}t}.$$

Therefore the probability that there is a strict increase infinitely often is bounded

above by

$$\sum_{j=N}^{\infty} 1/3^{2^j-1t}$$

for every N , which converges to zero quickly. In other words, the order of

$$N_{L_n/K_n} L_n \cap E_{K_n}$$

stabilizes with probability 1. Therefore by Chevalley's formula we expect that there exists an N_0 such that the 3-rank of A^Δ is

$$A \cdot 2^n + B$$

for $n \geq N_0$.

6.3.1 A conjecture

We now want to address the question: how often is the 3-class group in fact equal to the ambiguous 3-class group? In other words, how often does Chevalley's formula (Theorem 1.4) give the actual 3-rank of the class group?

We will consider here the case where two primes ramify and they are both congruent to 7 mod 24. We will again assume that 3 does not divide $h(K_n)$; if it does, then the conjectures in this section apply to the 3-class group of L_n excluding the contribution from K_n .

From the previous section, we expect the probability that the unit index is

maximal in L_n/K_n in this case to be

$$(1 - 1/3^2) \prod_{j=1}^n (1 - 1/3^{2 \times 2^{j-1}}).$$

Then we have

$$\text{rank } A_n^\Delta = 2^n.$$

We can also use the same theory as in §4.2.2 to develop an idea of what the rank matrices should look like. We assume that the unit index is maximal. In L_1/K_1 , that means we have a matrix of the form

$$\begin{pmatrix} a & b & c \\ b & a & c \\ d & e & f \\ e & d & f \end{pmatrix}$$

where $a + b + c = 0$ and $d + e + f = 0$. To find its rank, we could equivalently consider the matrix

$$\begin{pmatrix} a & b \\ b & a \\ d & e \\ e & d \end{pmatrix}.$$

Assuming equidistribution, this matrix has full rank with probability

$$64/81 = (1 - q^2)^2$$

where $q = 1/3$.

In general, for L_n/K_n , we expect to have a $(2^{n+1}) \times (2^n + 1)$ matrix whose rows sum to zero. We can equivalently then consider a $2^{n+1} \times 2^n$ matrix without the ‘sum to zero’ condition. Using the analysis of §4.2.2, and the theory developed for L_0/K_0 and L_1/K_1 , we can predict the structure of this matrix.

Let

$$\text{Gal}(K_n/\mathbb{Q}) \simeq D_n = \langle \sigma, \tau \rangle$$

where σ has order 2^n and τ has order 2. If we consider primes of K_n lying over a rational prime congruent to 7 mod 8, then by Proposition 4.14, at least one of the primes of K_n is fixed by τ . This gives us relations between the Artin symbols, just as in §4.2.2.

We predict the matrix to have the form

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{2^{n-1}-1} & a_{2^{n-1}} & a_{2^{n-1}-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_{2^{n-1}-2} & a_{2^{n-1}-1} & a_{2^{n-1}} & \dots & a_2 \\ a_2 & a_1 & \dots & a_{2^{n-1}-3} & a_{2^{n-1}-2} & a_{2^{n-1}-1} & \dots & a_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & a_{2^{n-1}-1} & a_{2^{n-1}-2} & a_{2^{n-1}-3} & \dots & a_1 \\ a_1 & a_2 & \dots & a_{2^{n-1}} & a_{2^{n-1}-1} & a_{2^{n-1}-2} & \dots & a_0 \\ b_0 & b_1 & \dots & b_{2^{n-1}-1} & b_{2^{n-1}} & b_{2^{n-1}-1} & \dots & b_1 \\ b_1 & b_0 & \dots & b_{2^{n-1}-2} & b_{2^{n-1}-1} & b_{2^{n-1}} & \dots & b_2 \\ b_2 & b_1 & \dots & b_{2^{n-1}-3} & b_{2^{n-1}-2} & b_{2^{n-1}-1} & \dots & b_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_2 & b_3 & \dots & b_{2^{n-1}-1} & b_{2^{n-1}-2} & b_{2^{n-1}-3} & \dots & b_1 \\ b_1 & b_2 & \dots & b_{2^{n-1}} & b_{2^{n-1}-1} & b_{2^{n-1}-2} & \dots & b_0 \end{pmatrix}.$$

When $n = 2$, we have a 8×4 matrix of the form

$$\begin{pmatrix} a & b & c & b \\ b & a & b & c \\ c & b & a & b \\ b & c & b & a \\ d & e & f & e \\ e & d & e & f \\ f & e & d & e \\ e & f & e & d \end{pmatrix}.$$

This matrix has full rank with probability

$$512/729 = (1 - q^2)^3.$$

For $n = 3$, the matrix has full rank with probability

$$40960/59049 = (1 - q^2)^3(1 - q^4).$$

In general we make the conjecture that the matrix has full rank with probability

$$(1 - q^2)^2 \prod_{j=1}^{n-1} (1 - q^{2^j}).$$

Since the 3-rank is

$$2(\text{rank } A_n^\Delta) - \text{rank } M = 2^{n+1} - \text{rank } M,$$

if M has maximal rank then the 3-rank is 2^n and is exactly the 3-rank of the ambiguous class group.

If we assume that in the case where the unit index is not maximal, the matrix is never full rank, then

$$\begin{aligned} P(\text{M max rank}) &= P(\text{M max rank} | E(L_n/K_n) \text{ max}) P(E(L_n/K_n) \text{ max}) \\ &\quad + P(\text{M max rank} | E(L_n/K_n) \text{ not max}) P(E(L_n/K_n) \text{ not max}) \\ &= (1 - q^2)^2 \prod_{j=1}^{n-1} (1 - q^{2^j}) \cdot (1 - q^2) \prod_{j=1}^n (1 - q^{2^j}) + 0 \\ &= (1 - q^2)^3 (1 - q^{2^n}) \prod_{j=1}^{n-1} (1 - q^{2^j})^2. \end{aligned}$$

Then

$$\lim_{n \rightarrow \infty} (1 - q^2)^3 (1 - q^{2^n}) \prod_{j=1}^{n-1} (1 - q^{2^j})^2 \approx 0.54115.$$

On the other hand, if we assume that in the case where the unit index is not maximal,

the matrix is always full rank, then

$$\begin{aligned}
P(\text{M max rank}) &= P(\text{M max rank} | E(L_n/K_n) \text{ max}) P(E(L_n/K_n) \text{ max}) \\
&\quad + P(\text{M max rank} | E(L_n/K_n) \text{ not max}) P(E(L_n/K_n) \text{ not max}) \\
&= (1 - q^2)^3 (1 - q^{2^n}) \prod_{j=1}^{n-1} (1 - q^{2^j})^2 + 1 - \left((1 - q^2) \prod_{j=1}^n (1 - q^{2^j}) \right)
\end{aligned}$$

Then

$$\lim_{n \rightarrow \infty} (1 - q^2)^3 (1 - q^{2^n}) \prod_{j=1}^{n-1} (1 - q^{2^j})^2 + 1 - \left((1 - q^2) \prod_{j=1}^n (1 - q^{2^j}) \right) \approx 0.76089.$$

In fact, this limit converges quickly. For $n = 5$, we have lower bound 0.54115 and upper bound 0.76090.

Conjecture 6.11. *Let L_n/K_n be a cubic cyclic extension of K_n , the n^{th} step in the anti-cyclotomic \mathbb{Z}_2 -extension of $\mathbb{Q}(i)$. Let A_n be the 3-class group of L_n and let \mathcal{P}_n be the probability that $\text{rank } A_n = \text{rank } A_n^\Delta$. Then for $n \geq 5$,*

$$0.5411 < \mathcal{P}_n < 0.7609.$$

For prime cyclic extensions of degree greater than 3, we expect that a larger percentage of the fields will have $\text{rank } A = \text{rank } A^\Delta$.

6.4 Group structure

Let A be the p -class group of a cyclic degree p extension L/K where $p \nmid h_K$. The previous sections presented heuristics for the rank of the class group. Here, we want to investigate the actual group structure using the methods of Cohen and Lenstra (see [5]).

First, we need a few results from Gras [12].

Proposition 6.12 (Gras [12, Proposition 4.1]). *Let*

$$A_n = \{a \in A \mid a^{(\sigma-1)^n} = 1\} \text{ and } A^{(n)} = \{a \in A \mid a^{p^n} = 1\}$$

for all $n \geq 0$. Then

1. We have $A_j \subseteq A_{j+1}$ and $A_j = A_{j+1}$ if and only if $A_j = A$ for $j \geq 0$.
2. The orders of the groups A_{j+1}/A_j are decreasing.
3. For every $n \geq 0$ we have the relation

$$A^{(n)} = A_{n(p-1)}.$$

Proposition 6.13 (Gras [12, Proposition 4.2]). *Let R_q be the p^q -rank of A (i.e. the dimension over F_p of the vector space $A^{p^{q-1}}/A^{p^q}$); then R_q is equal to the dimension over \mathbb{F}_p of $A^{(q)}/A^{(q-1)}$.*

Additionally, we have the relation

$$p^{R_q} = \prod_{i=(q-1)(t-1)}^{q(p-1)-1} |A_{i+1}/A_i| = |A_{q(p-1)}/A_{(q-1)(p-1)}|$$

Corollary 6.14. *If $R_q < p - 1$ for some q , then $R_{q+1} = 0$ (and consequently $R_j = 0$ for $j > q$).*

Proof. We have a sequence of inclusions

$$A_{(q-1)(p-1)} \subseteq A_{(q-1)(p-1)+1} \subseteq \cdots \subseteq A_{q(p-1)}.$$

First, let's assume $A_{q(p-1)} \neq A$. Then by Proposition 6.12, the inclusions must all be proper, and since these are all p -groups, $|A_{q(p-1)}| \geq p^{p-1}|A_{(q-1)(p-1)}|$. Therefore

$$p^{R_q} = |A_{q(p-1)}/A_{(q-1)(p-1)}| \geq p^{p-1}$$

and so $R_q \geq p - 1$.

Therefore if $R_q < p - 1$, then $A_{q(p-1)} = A$, and so $R_{q+1} = 0$. \square

The following classical result (see [19, Proposition 15]) follows from Corollary 6.14.

Corollary 6.15. *Let p be an odd prime, and suppose that L/K is a cyclic extension of degree p , where $p \nmid h_K$. If A is cyclic, then A is trivial or $\simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. Assume A is not trivial. Then, since A is cyclic, $R_1 = 1$. But $1 < p - 1$ for all odd primes, which means $R_j = 0$ for $j \geq 2$ and $A \simeq \mathbb{Z}/p\mathbb{Z}$. \square

Proposition 6.16. *If the $(\sigma - 1)^2$ rank of A is 0, then A is an elementary p -group.*

Proof. The $(\sigma - 1)^2$ -rank is the rank of $A^{(\sigma-1)}/A^{(\sigma-1)^2}$. If the $(\sigma - 1)^2$ rank of A is 0, then $A^{(\sigma-1)} = A^{(\sigma-1)^2}$ and therefore $A_1 = A_2$. Therefore $A = A_1$ by Proposition 6.12, and since A_1 is killed by the norm, it is an elementary p -group. \square

For $p = 3$, we have

$$\begin{aligned} \text{rank } A &= \sum_{j=1}^{p-1} \text{rank} (A^{(\sigma-1)^{j-1}}/A^{(\sigma-1)^j}) \\ &= \text{rank} (A/A^{(\sigma-1)}) + \text{rank} (A^{(\sigma-1)}/A^{(\sigma-1)^2}) \end{aligned}$$

We therefore know the group structure when the $(\sigma - 1)^2$ -rank is trivial. When it is non-trivial, we can apply Cohen-Lenstra heuristics (see [21], [5]). Given a fixed rank, we want to obtain conjectural probabilities for how likely a given group of rank r is to be the 3-ideal class group. The idea of the Cohen-Lenstra heuristics is that a group should appear inversely proportional to the size of its automorphism group.

In order to apply Cohen-Lenstra's heuristics, we need the following result giving the order of the automorphism group.

Theorem 6.17 ([21, Theorem 1.2.10]). *Let $G = \prod_{i=1}^k (\mathbb{Z}/p^{e_i})^{r_i}$ be a finite abelian p -group in standard form, i.e., $k \geq 0$, $e_1 > \dots > e_k > 0$, $r_i > 0$. The size of the automorphism group of G is*

$$|Aut(G)| = \left(\prod_{i=1}^k \left(\prod_{s=1}^{r_i} (1 - p^{-s}) \right) \right) \left(\prod_{1 \leq i, j \leq k} p^{\min(e_i, e_j) r_i r_j} \right).$$

However, not all groups are obtainable as the 3-class group. For example, if $r = 1$, then by Proposition 6.15, the only possibility is $A \simeq \mathbb{Z}/3\mathbb{Z}$.

For $r = 2$, groups are of the form $(\mathbb{Z}/p^e\mathbb{Z})^2$ or $(\mathbb{Z}/p^{e+1}\mathbb{Z}) \times \mathbb{Z}/p^e\mathbb{Z}$. To see this, assume $A = (\mathbb{Z}/p^{e+e'}\mathbb{Z}) \times (\mathbb{Z}/p^e\mathbb{Z})$ for $e' > 1$. Then $R_{e+e'} = 1$. We also know that $R_e = 2$ and $R_{e+1} = 1$. However, by Corollary 6.14 this implies that $R_{e+e'} = 0$ and so we have a contradiction.

Let's apply Cohen-Lenstra to the $r = 2$ case. First, we need to determine the weight of all groups of ranks 2. Let \mathcal{A}_r be the weight of all groups A of rank r that are admissible as A . By Theorem 6.17,

$$\begin{aligned} |\text{Aut}((\mathbb{Z}/p^e\mathbb{Z})^2)| &= (1 - p^{-1})(1 - p^{-2})p^{4e} \\ |\text{Aut}(\mathbb{Z}/p^{e+1}\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z})| &= (1 - p^{-1})^2 p^{4e+1}. \end{aligned}$$

Therefore, letting $q = p^{-1}$ as usual,

$$\begin{aligned} \mathcal{A}_2 &= \sum_{\text{rank } A=2} \frac{1}{|\text{Aut}(A)|} \\ &= \sum_{e=1}^{\infty} \frac{1}{(1 - p^{-1})(1 - p^{-2})} p^{-4e} + \sum_{e=1}^{\infty} \frac{1}{(1 - p^{-1})^2} p^{-4e-1} \\ &= \frac{1}{(1 - q)(1 - q^2)} \sum_{e=1}^{\infty} q^{4e} + \frac{q}{(1 - q)^2} \sum_{e=1}^{\infty} q^{4e} \\ &= \frac{q^4}{(1 - q)(1 - q^2)(1 - q^4)} + \frac{q^5}{(1 - q)^2(1 - q^4)} \\ &= \frac{q^4(1 + q + q^2)}{(1 - q)(1 - q^2)(1 - q^4)} \end{aligned}$$

When $p = 3$,

$$\mathcal{A}_2 = \frac{39}{1280}.$$

Now we can evaluate the predicted occurrence of particular groups for $p = 3$:

$$P(A \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} | \text{rank } A = 2) = \frac{80}{117} \approx .6838$$

$$P(A \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} | \text{rank } A = 2) = \frac{320}{1053} \approx .3039$$

$$P(A \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} | \text{rank } A = 2) = \frac{80}{9477} \approx .0084$$

$$P(A \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} | \text{rank } A = 2) = \frac{320}{85293} \approx .0038$$

$$P(A \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} | \text{rank } A = 2) = \frac{80}{314928} \approx .0001$$

Note that these predictions seem to match the structure of the class group in L_1 when one prime ramifies and it is congruent to 19 mod 24 (see Table 5.3.1) but not when the prime is congruent to 7 mod 24 (see Table 5.3.1). In the second case, the $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ appears more often than the Cohen-Lenstra style heuristics predict.

Recall that the 3-rank when only one type 1 prime ramifies is

$$2 - \text{rank } M$$

where M has only one independent parameter. Intuitively, one might expect that each independent parameter is equally likely, so that M has rank 0 with probability

$1/3$. But as shown in §6.2.2, in fact M has rank 0 with probability $1/9$. It is likely that something similar occurs when one constructs matrices which give the 9-rank of the class group. In other words, there may be local obstructions to applying Cohen-Lenstra style heuristics to the 3-class groups in these extensions.

Chapter 7: The structure theorem

After completing some of the computations in Chapter 5, it became clear that there were fundamental differences in the behavior of the p -class group in \mathbb{Z}_ℓ -extensions when $\ell \neq p$ when compared to the case where $\ell = p$. In this chapter, we present a particular field extension that demonstrates this difference.

First, we review the structure theorem for the ℓ -class group in \mathbb{Z}_ℓ -extensions.

Theorem 7.1 ([27, Theorem 13.13]). *Let L_∞/L be a \mathbb{Z}_ℓ -extension. Let ℓ^{e_n} be the exact power of ℓ dividing the class number of L_n . Then there exist integers $\lambda \geq 0$, $\mu \geq 0$, and ν , all independent of n , and an integer n_0 such that for all $n \geq n_0$,*

$$e_n = \mu\ell^n + \lambda n + \nu.$$

Let K_0 be an imaginary quadratic field and let L_0/K_0 be an extension of degree ℓ . Let K_∞/K_0 be the anti-cyclotomic \mathbb{Z}_ℓ -extension and therefore L_∞/L_0 is its lift.

Furthermore, let

$$\Lambda = \mathbb{Z}_\ell[[T]]$$

and

$$\nu_n = (1+T)^{\ell^n-1} + (1+T)^{\ell^n-2} + \dots + (1+T) + 1.$$

Then an elementary Λ -module E is defined to be one of the form

$$E = \bigoplus_i \Lambda/(\ell^{\mu_i}) \oplus \bigoplus_j \Lambda/(f_j)$$

where $\mu_i > 0$ is an integer and f_j is a distinguished polynomial, which means it is monic and ℓ divides each coefficient (except the leading monic coefficient). Let A_n be the ℓ -class group of L_n and ℓ^{e_n} be the exact power of ℓ dividing the class number of L_n .

Proposition 7.2 ([16, Proposition 12]). *There exist an elementary Λ -module E and a finite Λ -module F such that*

$$|A_n| = |A_0| \cdot |F/\nu_n F| \cdot |E/\nu_n E| \geq \ell^{e_0 + \mu(\ell^n - 1)}.$$

In particular,

$$\mu \leq \frac{e_n - e_0}{\ell^n - 1}.$$

Hubbard and Washington prove the following theorem.

Theorem 7.3 ([16, Theorem 2]). *Suppose s distinct primes $q \neq \ell$ are inert in K_0/\mathbb{Q} and ramify in L_0/K_0 , a degree ℓ extension. Then $\mu \geq s - 1$ for the \mathbb{Z}_ℓ -extension L_∞/L_0 .*

Consider the class groups in the \mathbb{Z}_2 -extension (so $\ell = 2$). Assume two primes

ramify in L_0/K_0 and we have $e_0 = 1$ and $e_1 = 2$. Then by Proposition 7.2

$$\mu \leq \frac{e_1 - e_0}{\ell^1 - 1} = 1$$

and by Theorem 7.3,

$$\mu \geq 1.$$

Therefore $\mu = 1$.

By [16, Proposition 17], there exists a Λ -module E' such that

$$\ell^{e_n - e_0 - \mu(\ell^n - 1)} = |F/\nu_n F| \times |E'/\nu_n E'|.$$

For $n = 1$, the left-hand side is 1, and therefore both orders on the right must be 1.

Then by Nakayama's Lemma, both F and E' must be trivial.

Therefore $\ell^{e_n - e_0 - \mu(\ell^n - 1)} = 1$ for all n . Since $e_0 = 1$, $\mu = 1$ and $\ell = 2$, we have

$$e_n = 2^n. \tag{7.1}$$

Now let's consider the $\ell \neq p$ situation. Let $K_0 = \mathbb{Q}(i)$ and consider the cyclic cubic extension L_0/K_0 given by

$$x^3 - 76x^2 + 1636x - 7064$$

in which only primes over 7 and 31 ramify.

We have the following 3-class groups.

$$A_{L_0} = \mathbb{Z}/3\mathbb{Z}$$

$$A_{L_1} = (\mathbb{Z}/3\mathbb{Z})^2$$

$$A_{L_2} = (\mathbb{Z}/3\mathbb{Z})^6$$

By Chevalley's formula, $e_n \geq 2^n - 1$, so we are in the analogue of the $\mu \geq 1$ situation. But the sequence $e_0 = 1, e_1 = 2, e_2 = 6$ is not possible for the ℓ -part of class group (see Equation 7). So the theory resulting from the structure theorem for the ℓ -class group in \mathbb{Z}_ℓ -extensions does not extend to the p -class group in \mathbb{Z}_ℓ -extensions when $p \neq \ell$.

Bibliography

- [1] David Brink, *Prime decomposition in the anti-cyclotomic extension*, Math. Comp. **76** (2007), no. 260, 2127–2138.
- [2] Reinier Broker, 2019, Personal correspondence.
- [3] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Thompson Book Company Inc., Washington, D.C., 1967.
- [4] Claude Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, Ph.D. thesis, University of Paris, 1934, p. 476.
- [5] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.
- [6] David A. Cox, *Primes of the form $x^2 + ny^2$* , A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989, Fermat, class field theory and complex multiplication.
- [7] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 6.9)*, 2015, <http://www.sagemath.org>.
- [8] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395.
- [9] Frank Gerth, III, *Counting certain number fields with prescribed l -class numbers*, J. Reine Angew. Math. **337** (1982), 195–207.
- [10] ———, *An application of matrices over finite fields to algebraic number theory*, Math. Comp. **41** (1983), no. 163, 229–234.
- [11] ———, *Densities for ranks of certain parts of p -class groups*, Proc. Amer. Math. Soc. **99** (1987), no. 1, 1–8.

- [12] Georges Gras, *Sur le l -groupe des classes des extensions cycliques de degré premier l* , C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1145–A1148.
- [13] ———, *Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l . I, II*, Ann. Inst. Fourier (Grenoble) **23** (1973), no. 3, 1–48; *ibid.* **23** (1973), no. 4, 1–44.
- [14] Marie-Nicole Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de \mathbf{Q}* , J. Reine Angew. Math. **277** (1975), 89–116.
- [15] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.
- [16] David Hubbard and Lawrence C. Washington, *Iwasawa invariants of some non-cyclotomic \mathbf{Z}_p -extensions*, J. Number Theory **188** (2018), 18–47.
- [17] Kenkichi Iwasawa, *On Γ -extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.
- [18] ———, *On the μ -invariants of \mathbf{Z}_ℓ -extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11.
- [19] Franz Lemmermeyer, *Galois action on class groups*, J. Algebra **264** (2003), no. 2, 553–564.
- [20] ———, *The ambiguous class number formula revisited*, J. Ramanujan Math. Soc. **28** (2013), no. 4, 415–421.
- [21] Johannes Lengler, *The Cohen-Lenstra heuristic for finite abelian groups*, Ph.D. thesis, Universität des Saarlandes, 2009.
- [22] L. Rédei and H. Reichardt, *Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1934), 69–74.
- [23] Alexander Smith, *2^∞ -selmer groups, 2^∞ -class groups, and Goldfeld's conjecture*, 2017.
- [24] Peter Stevenhagen, *Rédei-matrices and applications*, Number theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser., vol. 215, Cambridge Univ. Press, Cambridge, 1995, pp. 245–259.
- [25] Lawrence C. Washington, *Class numbers and \mathbf{Z}_p -extensions*, Math. Ann. **214** (1975), 177–193.
- [26] ———, *The non- p -part of the class number in a cyclotomic \mathbf{Z}_p -extension*, Invent. Math. **49** (1978), no. 1, 87–97.

- [27] ———, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.
- [28] Christian Wittmann, *Zetafunktionen über Gruppenringen und p -Klassengruppen zyklischer Erweiterungen vom Grad p* , Ph.D. thesis, Universität der Bundeswehr München, 2003.
- [29] Christian Wittmann, *p -class groups of certain extensions of degree p* , Math. Comp. **74** (2005), no. 250, 937–947.