ABSTRACT

Title of dissertation: UNRAMIFIED EXTENSIONS OF THE CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF $\mathbb{Q}(\sqrt{d}, i)$

David Lee Blagg, Doctor of Philosophy, 2014

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

Let $F_0 = \mathbb{Q}(\sqrt{-d})$, $K_0 = \mathbb{Q}(\sqrt{d})$, and $L_0 = \mathbb{Q}(\sqrt{d}, i)$ with d a square-free positive integer such that $2 \nmid d$. Let $L_j = L_0(\zeta_{2^{2+j}})$ so that $L_0 \subset L_1 \subset \cdots \subset \bigcup_j L_j$ is the cyclotomic $\mathbb{Z}_2$-extension of L_0. We determine when fourth roots of certain elements of K_0 generate unramified extensions of L_j. In particular, for elements of K_0 that are relatively prime to 2 and are generators of principal ideals that are fourth powers, we give explicit congruence conditions under which the fourth root of the element gives an unramified extension. For any such element γ, we show that if there is some j such that $L_j(\gamma^{1/4})/L_j$ is unramified, then $L_2(\gamma^{1/4})/L_2$ is unramified. We also show that when (2) is split in F_0, $L_2(\gamma^{1/4})/L_2$ is unramified for any such γ.

This result is analogous to a result by Hubbard and Washington in which they work with the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-d}, \zeta_3)$ when $3 \nmid d$ and consider extensions generated by cube roots of elements in $\mathbb{Q}(\sqrt{3d})$. However, many more technical problems arise in the present work because the degree of the extension L_j/K_j is not relatively prime to the degrees of the extensions being generated.

In order to prove our main results, we also give a congruence condition, which, for any number field K containing i and for any element $\gamma \in K$ with γ relatively prime to 2 and γ a generator of an ideal that is a fourth power, dictates whether or not adjoining a fourth root of γ to K gives an unramified extension.

UNRAMIFIED EXTENSIONS OF THE CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF $\mathbb{Q}(\sqrt{d}, i)$

by

David Lee Blagg

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
2014

Advisory Committee:
Professor Lawrence Washington, Chair/Advisor
Professor William Gasarch
Professor Thomas Haines
Professor Niranjan Ramachandran
Professor James Schafer

Acknowledgments

I am deeply indebted to my advisor, Professor Lawrence Washington. His time, his support, and his insights have been invaluable to me, and his flexibility allowed me to fit this dissertation into my life. Our frequent meetings were the highlight of the process, and I consider myself extremely lucky to have had the opportunity to work with him.

I would also like to thank my parents, Bill and Didi Blagg, and my brother, Jeff Blagg. They are the people who have made me who I am, and they deserve much of the credit for anything I do.

Finally, I would like to thank my wife, Julianna Blagg. She found so many ways to make this process easier for me, and I could not have finished without her support. I look forward to a lifetime of paying her back.

Table of Contents

List of Tables

List of Figures

Chapter 1: Background

Let $d \in \mathbb{Z}$ be square-free and positive. In [1], the authors work with the cyclotomic $\mathbb{Z}_3$-extensions of $F_0 = \mathbb{Q}(\sqrt{-d})$, $K_0 = \mathbb{Q}(\sqrt{3d})$, and $L_0 = \mathbb{Q}(\sqrt{d}, \zeta_3)$. Taking $\mathbb{B}_j$ to be the jth level of the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$, they write $F_j = F_0\mathbb{B}_j$, $K_j = K_0\mathbb{B}_j$, and $L_j = L_0\mathbb{B}_j$.

$$
\begin{tikzcd}[column sep=small]
 & \cdot \arrow[dl, dotted, no head] \arrow[d, dotted, no head] \arrow[dr, dotted, no head] & \\
\vdots \arrow[d, dotted, no head] & L_1 \arrow[dl, no head] \arrow[dr, no head] \arrow[dd, no head] & \vdots \arrow[d, dotted, no head] \\
F_1 \arrow[dd, no head] & & K_1 \arrow[dd, no head] \\
 & L_0 \arrow[dl, no head] \arrow[dr, no head] \arrow[dd, no head] & \\
\mathbb{Q}(\sqrt{-d}) = F_0 \arrow[dr, no head] & & K_0 = \mathbb{Q}(\sqrt{3d}) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Figure 1.1: Cyclotomic $\mathbb{Z}_3$-extensions of $\mathbb{Q}(\sqrt{-d})$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\sqrt{d}, \zeta_3)$

For certain conditions on d and on the class group of K_0, they note that as we go up the tower of fields in the cyclotomic $\mathbb{Z}_3$-extension of F_0, we find that there are unramified extensions of degree 3. This suggests a natural question: what are those unramified extensions? After adjoining a cube root of unity to F_j to get L_j, they show that many of these unramified extensions can be generated by cube roots of elements of K_0. Restricting to the case that $j > 0$ and $d \equiv 2 \bmod 3$ (so (3) splits in $F_0 = \mathbb{Q}(\sqrt{-d})$ and in L_0), they show that $L_j(\varepsilon_0^{1/3})/L_j$ is unramified when ε_0 is the fundamental unit of K_0 and that $L_j(\gamma^{1/3})/L_j$ is unramified when (γ) is a cube of an order-3 ideal. Explicitly, their result as stated in [1] is:

Theorem 1.0.1. *Let $d \equiv 2$ mod 3 and let ε_0 be the fundamental unit of $K_0 = \mathbb{Q}(\sqrt{3d})$. Let r be the 3-rank of the class group of K_0 and let A_1 be the 3-part of the class group of F_1. Then rank$(A_1) \geq r+1$. Let $I_1, \ldots, I_r$ represent independent ideal classes of order 3 in K_0, and write $I_i^3 = (\gamma)$ with $\gamma \in K_0$. Let $L_1 = \mathbb{Q}(\sqrt{d}, \sqrt{3d}, \zeta_9)$. Then*

$$L_1(\varepsilon_0^{1/3}, \gamma^{1/3}, \ldots, \gamma_r^{1/3})/L_1$$

is an everywhere unramified extension of degree 3^{r+1}.

Some of these generators may also give an unramified extension of L_0, but all of them give unramified extensions of L_1.

At a high level, we would like to prove something like an analogue to this result, but for degree-2 extensions of a cyclotomic $\mathbb{Z}_2$-extension of F_0 rather than degree-3 extensions of the cyclotomic $\mathbb{Z}_3$-extension of F_0. If we want such an analogue, we must first determine what K_0 and L_0 should be. For the $\mathbb{Z}_3$-extension, the role of the L-tower is essentially to add ζ_3 to the fields of the F-tower. This ensures that the degree-3 extensions of fields of the L-tower are generated by the cube root of some element of the field being extended.

If we are interested in degree-2 extensions of fields in the $\mathbb{Z}_2$-extension of F_0, this step is unnecessary because F_0 already has a primitive square root of unity.

It is natural, then, to take $L_j = F_j$ for all j. In such a setup, the generators of the unramified extensions of F_j are not particularly interesting. We know that any such generator must be the square root of a non-square element in F_j. Moreover, if $\gamma^{1/2}$ is going to generate an unramified degree-2 extension, we must have $(\gamma) = I^2$ for some ideal I of F_j. To see this, write $(\gamma) = \wp_1^{a_1}\wp_2^{a_2}\cdots\wp_n^{a_n}$. Then $(\gamma^{1/2}) = \wp_1^{a_1/2}\wp_2^{a_2/2}\cdots\wp_n^{a_n/2}$ in $F_j(\gamma^{1/2})$. If any of the a_is are odd, then the corresponding $\wp_i$ must ramify because this is an integral ideal. Since the extension is unramified, this is impossible, so all of the exponents must be even. This allows us to write (γ) as I^2 in F_j. So in this case, we do not need to resort to a K-tower or an L-tower to understand the generators for the Hilbert 2-class field of F_n.

It turns out that a more interesting case, and one that more closely parallels Theorem 1.0.1, is to look at degree-4 extensions of the L-tower. In this case, we adjoin a primitive fourth root of unity to the F-tower to get the L-tower, so we take $K_0 = \mathbb{Q}(\sqrt{d})$ and $L_0 = F_0(i)$.

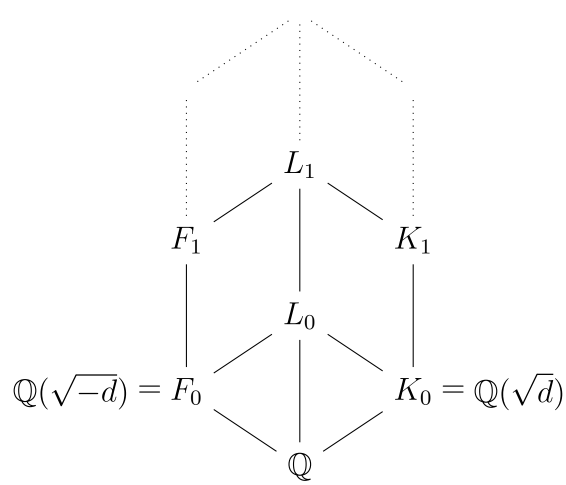

Figure 1.2: Cyclotomic $\mathbb{Z}_2$-extensions of $\mathbb{Q}(\sqrt{-d})$, $\mathbb{Q}(\sqrt{d})$, and $\mathbb{Q}(\sqrt{d}, i)$

This means that degree-4 extensions of the L-tower are Kummer extensions and are generated by fourth roots of elements in the base field. This is exactly the scenario we explore in this paper. In particular, for d odd and for all j, when $\gamma \in K_0$ with γ relatively prime to 2, $\sqrt{\gamma} \notin K_0$, and $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$, we establish exactly when $L_j(\gamma^{1/4})/L_j$ is unramified based on simple congruence conditions on γ. Since ε_0 satisfies all of those criteria for γ, the result includes ε_0.

Combining and condensing these results, we have the following theorem, which is the main result of the paper:

Theorem 1.0.2. *Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$.*

When $d \equiv 3 \bmod 4$, write $\gamma = a+b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Then, for all $j \geq 2$, $L_j(\gamma^{1/4})/L_j$ is unramified iff $a \equiv 0 \bmod 4$ or $b \equiv 0 \bmod 4$.

When $d \equiv 1 \bmod 8$, write $\gamma = a+b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Then, for all $j \geq 2$, $L_j(\gamma^{1/4})/L_j$ is unramified iff $a \equiv 0 \bmod 8$ or $b \equiv 0 \bmod 8$.

When $d \equiv 5 \bmod 8$, write $\gamma \equiv a + bz \bmod 8$ with $a, b \in \mathbb{Z}$ and $z = \frac{-1+k\sqrt{d}}{2}$ where $k \in \mathbb{Z}$ is such that $k^2 d \equiv -3 \bmod 64$. Then for all $j \geq 1$, $L_j(\gamma^{1/4})/L_j$ is unramified iff $(a, b) \in \{\pm(0, 1), \pm(1, 0), \pm(1, 1)\}$.

Moreover, if $\sqrt{\gamma} \notin K_0$, these extensions are never trivial, and, in that case, if $d \not\equiv 7 \bmod 8$ and the extension is unramified, then it is degree 4.

If $I_1, \ldots, I_n$ represent independent ideal classes of order 4 in K_0 with $I_j^4 = (\gamma_j)$ and γ_j satisfying the constraints above, then the 2-rank of $L_j(\varepsilon_0^{1/4}, \gamma_1^{1/4}, \ldots, \gamma_n^{1/4})/L_j$ is $n + 1$.

Similarly to Theorem 1.0.1, when (2) is split in F_0, we find that the fourth root of any such γ generates an unramified extension of L_j for large enough j. In this case, though, we may have to wait until L_2 before the extension is unramified. When (2) is not split in F_0, some values for γ result in $L_j(\gamma^{1/4})/L_j$ being ramified for all j. Also note that the independence result does not allow us to say that the extension has degree 4^{n+1}. Although none of the degree-4 extensions can totally collapse, some could be degree 2 rather than degree 4 to begin with, or could become degree 2 rather than degree 4 when combined with the other extensions.

Along the way to proving this result, we give a somewhat more complicated congruence condition, which, for any number field K containing i and for any element $\gamma \in K$ with γ relatively prime to 2, dictates whether adjoining a fourth root of γ to K gives an unramified extension.

We also prove everything necessary to give the following result regarding adjoining square roots:

Theorem 1.0.3. *Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. Then for $j \geq 1$, $L_j(\gamma^{1/2})/L_j$ is ramified iff $d \equiv 5 \bmod 8$ and Norm$(\gamma) = -1$. Moreover, when $L_j(\gamma^{1/2})/L_j$ is ramified, it is ramified at both primes above (2).*

Proof. We see in Proposition 4.1.3, Proposition 4.2.2, and Proposition 4.4.2 that when d is not 5 mod 8, $L_1(\gamma^{1/2})/L_1$ is unramified. When $d \equiv 5 \bmod 8$, combining Lemma 4.3.1 and Proposition 4.3.2 with norm calculations gives the result. □

For several reasons, looking at degree-2 and degree-4 extensions of fields in the cyclotomic $\mathbb{Z}_2$-extension of F_0 ends up being quite different from looking at degree-3 extensions of fields in the cyclotomic $\mathbb{Z}_3$-extension. One of these reasons is that the degree of the extensions we are studying is not relatively prime to the degree of L_j/F_j. In the context of the $\mathbb{Z}_3$-extension, any degree-3 extension of F_j is guaranteed to lift to an extension of L_j of the same degree. In particular, non-trivial extensions are guaranteed to lift to non-trivial extensions. For degree-2 and degree-4 extensions of the $\mathbb{Z}_2$-extension, that is not guaranteed because L_j/F_j might absorb some or all of the extension of F_j that is being lifted. Still, if there are multiple independent non-trivial extensions of F_j, all but at most one of them must lift to non-trivial extensions of L_j.

Because our primary focus is degree-4 extensions, another key difference is that 3 is prime and 4 is not. In the next chapter, we begin by giving our fundamental tool for showing whether an extension is unramified or not. The standard method works only for extensions generated by adjoining pth roots to a field, where p is prime. To handle extensions generated by fourth roots, we have to do some extra work to see how to apply this method twice.

1.1 Basics

Before progressing to our results, we establish some notation that we use throughout the paper:

- $\mathcal{O}_K$ is the ring of integers of a number field K
- d is an odd integer greater than 1
- $F_0 = \mathbb{Q}(\sqrt{-d})$

- $K_0 = \mathbb{Q}(\sqrt{d})$
- $L_j = L_0(\sqrt{d}, \zeta_{2^{2+j}})$, so $L_0 = \mathbb{Q}(\sqrt{d}, i)$
- ε_0 is the fundamental unit of $\mathcal{O}_{K_0}$
- ζ_n is a primitive nth root of unity
- $v_\wp(\alpha)$ is the $\wp$-adic valuation of α, and $v(\alpha)$ is the 2-adic valuation of α.

We also note some facts that are relevant to the scenario described and that we use repeatedly throughout the rest of the paper. The first two of these are easy generalizations of lemmas in [3] and we follow the proofs there closely.

Lemma 1.1.1. *Let n be a positive integer and K be a field containing ζ_{2^n}. Let r and s be odd integers. Then $(\zeta_{2^n}^r - 1)/(\zeta_{2^n}^s - 1)$ is a unit in $\mathcal{O}_K$.*

Proof. Because r and s are both odd, we can write $r \equiv st \bmod 2^n$ for some t. Then we have

$$\frac{\zeta_{2^n}^r - 1}{\zeta_{2^n}^s - 1} = \frac{\zeta_{2^n}^{st} - 1}{\zeta_{2^n}^s - 1} = 1 + \zeta_{2^n}^s + \cdots + \zeta_{2^n}^{s(t-1)} \in \mathcal{O}_K.$$

The exact same argument shows that $(\zeta_{2^n}^s - 1)/(\zeta_{2^n}^r - 1) \in \mathcal{O}_K$. □

Lemma 1.1.2. *Let n be a positive integer and K be a field containing ζ_{2^n}. Then $(1 - \zeta_{2^n})^{2^{n-1}} = (2)$ as ideals in $\mathcal{O}_K$.*

Proof. Since $X^{2^{n-1}} + 1 = \Phi_{2^n}(X) = \prod_{j=1; j \text{ odd}}^{2^n - 1} (X - \zeta_{2^n}^j)$, we can take $X = 1$ to see that $2 = \prod_{j=1; j \text{ odd}}^{2^n-1} (1 - \zeta_{2^n}^j)$. Our previous lemma shows that, as ideals, each of the terms in the product on the right are equal, so we get the equality of ideals $(2) = (1 - \zeta_{2^n})^{\phi(2^n)} = (1 - \zeta_{2^n})^{2^{n-1}}$ as desired. □

Corollary 1.1.3. *Let n be a positive integer and K be a field containing ζ_{2^n}. If*

$n \geq 1$, $v_2(1-\zeta_{2^n}) = 2^{-(n-1)}$. *If* $n \geq 2$, $v_2(1+\zeta_{2^n}) = 2^{-(n-1)}$.

Proof. The first claim follows immediately from the previous lemma. For the second claim, note that $1+\zeta_{2^n} = (1-\zeta_{2^n}) + 2\zeta_{2^n}$. The valuation of the final term is 1. For $n \geq 2$, $v_2(1-\zeta_{2^n}) < 1$, so we have $v_2(1+\zeta_{2^n}) = v_2(1-\zeta_{2^n})$. $\square$

Corollary 1.1.4. *Let $n > 1$ be an integer and K be a field containing $\zeta_{2^{n+1}}$. As ideals in $\mathcal{O}_K$, $(1+\zeta_{2^{n+1}})^2 = (1+\zeta_{2^n})$.*

Proof. This follows immediately from the lemma above. $\square$

Lemma 1.1.5. $K_1 = K_0(\sqrt{2})$.

Proof. We know that $\zeta_8 \in L_1$. This means that $\sqrt{2} = \zeta_8^7(1+i) \in L_1$. But $\sqrt{2}$ is real, so must be in the maximal real subfield of L_1, namely K_1. Since we always take d odd, we do not have $\sqrt{2} \in K_0$, so $K_1 = K_0(\sqrt{2})$. $\square$

Lemma 1.1.6. *Let K be a number field such that there is only one prime above 2. Let n be a positive integer and $x, y \in \mathcal{O}_K$ be relatively prime to 2. If $x^2 \equiv y^2$ mod 2^{n+1}, then $x \equiv \pm y$ mod 2^n.*

Proof. We can write $(x-y)(x+y) = x^2 - y^2 \equiv 0 \bmod 2^{n+1}$. The difference between the two factors is $2y$. Since y is relatively prime to 2, one of the two factors must not be divisible by any power of (the prime above) 2 greater than 2 itself. Since there is only one prime above 2, the other factor must be divisible by 2^n, so $x \equiv \pm y$ mod 2^n as desired. $\square$

This is not necessarily true if (2) has split somewhere in $K/\mathbb{Q}$. For example, let $(2) = \wp_1\wp_2$. Then we could have $(x-y)$ divisible by $\wp_1^n\wp_2$ and $(x+y)$ divisible by $\wp_1 \wp_2^n$. If these are the largest powers of $\wp_j$ dividing the two factors, then $x \equiv y$ mod 2, but not mod 2^n for any $n > 1$. Still, $x^2 - y^2$ is divisible by $\wp_1^{n+1} \wp_2^{n+1} = 2^{n+1}$. When (2) has more than one prime above it, we can say something similar as long as we are working mod small enough powers of 2:

Lemma 1.1.7. *Let K be a number field, let $\wp$ be a prime ideal in $\mathcal{O}_K$, and let n be a positive integer with $\wp^n \mid (2)$. Let $x, y \in \mathcal{O}_K$. If $x^2 \equiv y^2 \bmod \wp^{2n}$, then $x \equiv y \equiv -y \bmod \wp^n$.*

Proof. As in the previous proof, we can write $(x - y)(x + y) \equiv 0 \bmod \wp^{2n}$. These two factors are congruent to each other mod 2. Since $\wp^n \mid 2$, this means either of the factors is divisible by $\wp^n$ iff the other is. Thus, both factors must be divisible by $\wp^n$ for their product to be divisible by $\wp^{2n}$. $\square$

Chapter 2: Machinery

Throughout the paper, our approach for showing whether adjoining something to L_j gives an unramified extension is to apply Exercise 9.3 part c from [3]. Because we rely on this exercise so heavily, we state it here, modified to be specific to the situations we care about.

From the proof, it is easy to see that $K(\alpha^{1/2})$ is unramified at $\wp$ iff $\exists \mu \in \mathcal{O}_K$ such that $\mu^2 \equiv \alpha \mod \wp^{2a}$. Also note that although we have stated the result globally, the proof works just as well when K is the completion of a number field. This is true for the rest of our results as well. We are particularly interested in the global results, but in proving these, we will often need temporarily to work locally and then use the local result to deduce a global result. This situation will arise when the congruence class of $\sqrt{d}$ mod some power of 2 depends on the completion. When we derive global results from local results, we rely on the fact that an extension is ramified at a prime iff it is ramified in the completion at that prime.

Proposition 2.0.8. *Let K be a number field that is totally complex, and let $\alpha \in \mathcal{O}_K$ be relatively prime to 2 and not a square. Let $\wp_1, \ldots, \wp_n$ be the primes above 2 in $\mathcal{O}_K$, and let a_j be the largest integer such that $\wp_j^{a_j} \mid 2$. Then $K(\alpha^{1/2})/K$ is unramified at all primes iff $(\alpha) = I^2$ for some ideal I of K and for $1 \leq j \leq n$, $\exists \mu_j \in \mathcal{O}_K$ such* *that* $\mu_j^2 \equiv \alpha$ *mod* $\wp_j^{2a_j}$.

Proof. ($\Rightarrow$) To see that (α) must be the square of an ideal, write $(\alpha) = \rho_1^{b_1}\rho_2^{b_2}\cdots\rho_r^{b_r}$. Then $(\sqrt{\alpha}) = \rho_1^{b_1/2}\rho_2^{b_2/2}\cdots\rho_r^{b_r/2}$. If any of the b_js are odd, then to make this an integral ideal, the corresponding ρ_j must be ramified. Since the extension is unramified, this is impossible, so all of the exponents must be even.

The proof that α is a square mod $\wp_j^{2a_j}$ in $\mathcal{O}_K$ is identical for all j, so we will simplify notation by simply using $\wp$, a, and μ. Let c be the largest power of $\wp$ such that $\exists x$ with $x^2 \equiv \alpha \bmod \wp^c$. We will show by contradiction that $c \geq 2a$, so assume that $c < 2a$. We first claim that c is odd.

If $c = 2b$, then let $w \in \mathcal{O}_K$ be such that $v_\wp(w) = 1$. Also, let $y \in \mathcal{O}_K$ be such that $y^2 \equiv \frac{\alpha-\mu^2}{w^{2b}} \bmod \wp$. We know that such a y exists because squaring is the Frobenius automorphism of $\mathcal{O}_K/\wp\mathcal{O}_K$. Then $(\mu + w^b y)^2 - \alpha = (\mu^2 - \alpha) + 2\mu w^b y + w^{2b}y^2$. Since $2a > c = 2b$, we have $a > b$. Since both a and b are integers, we have $v_\wp(2\mu w^b y) = a + b \geq 2b + 1$. Thus $(\mu + w^b y)^2 - \alpha \equiv (\mu^2 - \alpha) + w^{2b}y^2 \bmod \wp^{2b+1}$. By construction, $w^{2b}y^2 \equiv \alpha - \mu^2 \bmod \wp^{2b+1}$, so $(\mu + w^b y)^2 - \alpha \equiv 0 \bmod \wp^{2b+1}$. This contradicts the fact that $c = 2b$ is the largest power of $\wp$ such that α is a square mod $\wp^c$, so c must be odd.

If we have $\mu^2 \equiv \alpha \bmod \wp^c$, we can write $(\mu - \alpha^{1/2})(\mu + \alpha^{1/2}) \equiv 0 \bmod \wp^c$. Since we have assumed $c < 2a$, one of the two factors must have $\wp$-adic valuation less than a. Without loss of generality, assume $v_\wp(\mu - \alpha^{1/2}) < a$. Since $\mu + \alpha^{1/2} = \mu - \alpha^{1/2} + 2\alpha^{1/2}$ and $v_\wp(2\alpha^{1/2}) = a$, we must have $v_\wp(\mu - \alpha^{1/2}) = v_\wp(\mu + \alpha^{1/2})$. But then $c = 2v_\wp(\mu - \alpha^{1/2})$, which is even. This is a contradiction, so we must have

$c \geq 2a$ as desired.

($\Leftarrow$) First we show that $(\alpha) = I^2$ implies that $K(\alpha^{1/2})/K$ is unramified away from (2). The completion of $\mathcal{O}_K$ at any prime is a principal ideal domain, so I becomes principal. We write it $I = (\gamma)$. This means that we have $\alpha = u\gamma^2$ for some $\wp$-adic unit. Then $\alpha^{1/2} = u^{1/2}\gamma$, so in the completion, the extension is generated by $u^{1/2}$. The relative different for this extension is generated by $(2u^{1/2}) = (2)$, so only primes above 2 can ramify.

Now we show that the extension is unramified at $\wp_j$ for $1 \leq j \leq n$. Again, the calculations are the same for all j, so we will use $\wp$, a, and μ. Consider the polynomial $f(X) = \frac{(2X+\mu)^2-\alpha}{4} = X^2 + \mu X + \frac{\mu^2-\alpha}{4}$. Clearly $f(X)$ is monic and since $\alpha \equiv \mu^2 \bmod 4$, each of the coefficients is in $\mathcal{O}_K$.

A root β of this polynomial satisfies $(2\beta + \mu)^2 = \alpha$, so we can take $\alpha^{1/2}$ to be $2\beta + \mu$. This means that $K(\alpha^{1/2})/K = K(\beta)/K$. In particular, they have the same different. This different must divide $f'(\beta) = 2\beta + \mu$. Since $v_\wp(\beta) \geq 1$ and μ is relatively prime to $\wp$, this different is also relatively prime to $\wp$. Thus, the extension is unramified at $\wp$. $\square$

From the proof, it is easy to see that $K(\alpha^{1/2})$ is unramified at $\wp$ iff $\exists \mu \in \mathcal{O}_K$ such that $\mu^2 \equiv \alpha \bmod \wp^{2a}$. Also note that this proof works just as well when K is the completion of a number field. This is true for the rest of our results as well. We are particularly interested in the global results, but in proving these, we will often need temporarily to work locally and then use the local result to deduce a global result. This situation will arise when the congruence class of $\sqrt{d}$ mod some power of 2 depends on the completion. When we derive global results from local results, we rely on the fact that an extension is ramified at a prime iff it is ramified in the completion at that prime.

When adjoining a fourth root, we need to be able to apply Proposition 2.0.8 twice: once for adjoining a square root of some element γ to L_j and once for adjoining a fourth root of γ to $L_j(\gamma^{1/2})$. To apply this proposition, we need to understand whether certain elements are squares in the appropriate ring of integers. For the second application of the proposition, then, we need to understand the ring of integers of $L_j(\gamma^{1/2})$.

The following two lemmas allow us to prove easily the fact that we need about this ring of integers. The resulting corollary shows us that if $\gamma \equiv \mu^2 \bmod 4$ for some $\mu \in \mathcal{O}_{L_j}$, then an element of $\mathcal{O}_{L_j(\gamma^{1/2})}$ is a square mod some power of 2 in that ring iff it is a square mod the same power of 2 in $\mathcal{O}_{L_j}\left[\frac{\mu+\gamma^{1/2}}{2}\right]$. The latter ring is easier to work with because it is easier to characterize its elements.

Lemma 2.0.9. *Let $K(\alpha)$ be a quadratic extension of a number field K, with τ the non-trivial element of Gal($K(\alpha)/K$). Let $\lambda \in \mathcal{O}_{K(\alpha)}$ be such that $\lambda^\tau - \lambda$ is relatively prime to 2. Then for any $n \in \mathbb{Z}^+$ and $x \in \mathcal{O}_{K(\alpha)}$, there is some $y \in \mathcal{O}_K[\lambda]$ such that $x \equiv y \bmod 2^n$.*

Proof. Let S be the set of elements in $\mathcal{O}_K$ that are relatively prime to (2) and let $(R)_2 = RS^{-1}$ for any ring R containing S. We begin by showing that $\left(\mathcal{O}_{K(\alpha)}\right)_2 = (\mathcal{O}_K)_2\,[\lambda]$.

Since $(\mathcal{O}_K)_2$ is a Dedekind domain with finitely many prime ideals, it must be a principal ideal domain. Since $(\mathcal{O}_K)_2$ is a P.I.D. and $\left(\mathcal{O}_{K(\alpha)}\right)_2$ is finitely generated over it, we can write $\left(\mathcal{O}_{K(\alpha)}\right)_2 = \beta_1 (\mathcal{O}_K)_2 \oplus \beta_2 (\mathcal{O}_K)_2$. We can also write $(\mathcal{O}_K)_2 [\lambda]$ as $(\mathcal{O}_K)_2 \oplus (\mathcal{O}_K)_2 \lambda$. Since $(\mathcal{O}_K)_2 [\lambda] \subseteq \left(\mathcal{O}_{K(\alpha)}\right)_2$, we can write the basis of the former in terms of the basis of the latter: $1 = a\beta_1 + b\beta_2$ and $\lambda = c\beta_1 + d\beta_2$ with $a, b, c, d \in (\mathcal{O}_K)_2$. Applying τ to both of these equations gives $1 = a\beta_1^\tau + b\beta_2^\tau$ and $\lambda^\tau = c\beta_1^\tau + d\beta_2^\tau$. This gives us the following matrix equation:

$$\begin{pmatrix} 1 & 1 \\ \lambda & \lambda^\tau \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \beta_1 & \beta_1^\tau \\ \beta_2 & \beta_2^\tau \end{pmatrix}.$$

The determinant of the left-most matrix is $\lambda^\tau - \lambda$. We have assumed this to be relatively prime to 2. This means that the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ must also be prime to 2, which means that we can invert $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over $(\mathcal{O}_K)_2$. By writing

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ \lambda & \lambda^\tau \end{pmatrix} = \begin{pmatrix} \beta_1 & \beta_1^\tau \\ \beta_2 & \beta_2^\tau \end{pmatrix},$$

we can write the β_is in terms of 1 and λ with coefficients in $(\mathcal{O}_K)_2$, so we have that $\left(\mathcal{O}_{K(\alpha)}\right)_2 \subseteq (\mathcal{O}_K)_2 [\lambda]$. Since we already had the reverse inclusion, we get equality.

Now let $x \in \mathcal{O}_{K(\alpha)}$. Identifying x with its image under the natural injection, we can think of $x \in \left(\mathcal{O}_{K(\alpha)}\right)_2$. We have just seen that this means $x \in (\mathcal{O}_K)_2 [\lambda]$. This means that there is some $m \in \mathcal{O}_K$ relatively prime to 2 such that $xm \in \mathcal{O}_K[\lambda]$. Since m is relatively prime to 2, then for any n, it has an inverse in $\mathcal{O}_K$ mod 2^n, which we call m_n^{-1}. Then mm_n^{-1} is 1 mod 2^n, so $x \equiv xmm_n^{-1}$ mod 2^n. Moreover, we have $xm, m_n^{-1} \in \mathcal{O}_K[\lambda]$, so $xmm_n^{-1} \in \mathcal{O}_K[\lambda]$. $\square$

Now we can apply the previous lemma to a more specific scenario that is particularly relevant for us. In this more specific situation, we take on two additional contraints: α is the square root of an element of the base field K, and its square is a square mod 4 in that field.

Lemma 2.0.10. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2. If $\gamma \equiv \mu^2$ mod 4 for some $\mu \in \mathcal{O}_K$, then $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right] \subseteq \mathcal{O}_{K(\gamma^{1/2})}$ and, for any $n \in \mathbb{Z}^+$, every element of the ring of integers of $K(\gamma^{1/2})$ is congruent mod 2^n to an element of $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$.*

Proof. Write $\gamma = \mu^2 + 4k$ with $k \in \mathcal{O}_K$. Then $\frac{\mu+\gamma^{1/2}}{2}$ satisfies $x^2 - \mu x - k = 0$. Thus, $\frac{\mu+\gamma^{1/2}}{2} \in \mathcal{O}_{K(\gamma^{1/2})}$. If $\gamma^{1/2} \in \mathcal{O}_K$, this tells us that $\mathcal{O}_K \subseteq \mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right] \subseteq \mathcal{O}_{K(\gamma^{1/2})} = \mathcal{O}_K$. This immediately implies that all of these are equal, so $\mathcal{O}_{K(\gamma^{1/2})} = \mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$, and the rest of the lemma is trivially true.

If $\gamma^{1/2} \notin \mathcal{O}_K$, then in the notation of Lemma 2.0.9, we can take $\lambda = \frac{\mu+\gamma^{1/2}}{2}$. Then $\lambda^\tau - \lambda = \frac{\mu-\gamma^{1/2}}{2} - \frac{\mu+\gamma^{1/2}}{2} = -\gamma^{1/2}$. Since γ is relatively prime to 2, $-\gamma^{1/2}$ is as well. Then taking $\alpha = \gamma^{1/2}$, the rest of the lemma is exactly the statement of Lemma 2.0.9. □

We can use the previous lemma to prove the following corollary, which gives us the tool we need to answer whether something is a square mod 4 in $\mathcal{O}_{L_j(\gamma^{1/2})}$.

Corollary 2.0.11. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2. If $\gamma \equiv \mu^2$ mod 4 for some $\mu \in \mathcal{O}_K$, then $\alpha \in \mathcal{O}_{K(\gamma^{1/2})}$ is a square mod 2^n in $\mathcal{O}_{K(\gamma^{1/2})}$ iff it is a square mod 2^n in $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$.*

Proof. If α is a square mod 2^n in $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$, it is clearly a square mod 2^n in

$\mathcal{O}_{K(\gamma^{1/2})}$ because $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right] \subseteq \mathcal{O}_{K(\gamma^{1/2})}$.

If α is a square mod 2^n in $\mathcal{O}_{K(\gamma^{1/2})}$, then write $\alpha \equiv x^2 \bmod 2^n$ with $x \in \mathcal{O}_{K(\gamma^{1/2})}$. The lemma shows that $\exists y \in \mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$ such that $x \equiv y \bmod 2^n$. Thus, we have $\alpha \equiv x^2 \equiv y^2 \bmod 2^n$. $\square$

To show whether or not something is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$, we examine what a generic square mod 4 looks like in $\mathcal{O}_{K(\gamma^{1/2})}$ and then see whether or not our element can be written in that form. The previous corollary allows us to work in $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$, where we can easily write down what a square looks like.

The next few results apply Proposition 2.0.8 in $\mathcal{O}_{K(\gamma^{1/2})}$ using the facts that we have learned about elements being a square in that ring. They culminate in a theorem that is our instrument any time we wish to show whether $L_j(\gamma^{1/4})/L_j$ is ramified or not.

The first of these is similar to the obvious fact that if $\gamma^{1/2}$ is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4, then γ is a fourth power mod 4 in the same ring. This proposition is stronger, though. In it, we show that γ actually has to be a fourth power mod 4 in $\mathcal{O}_K$. Before proving this proposition, we need to prove a brief lemma.

Lemma 2.0.12. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2 with $\gamma^{1/2} \notin \mathcal{O}_K$. Let $a, b, \mu \in \mathcal{O}_K$ and $\frac{\mu+\gamma^{1/2}}{2} \in \mathcal{O}_{K(\gamma^{1/2})}$. Then $0 \equiv a + b\frac{\mu+\gamma^{1/2}}{2}$ mod 4 iff $a \equiv 0$ mod 4 and $b \equiv 0$ mod 4.*

Proof. By assumption, we have $0 \equiv a + b\frac{\mu+\gamma^{1/2}}{2} \bmod 4$. We can take the conjugate of both sides, giving us $0 \equiv a + b\frac{\mu-\gamma^{1/2}}{2} \bmod 4$. If we subtract the latter congruence from the former, we get $b\gamma^{1/2} \equiv 0 \bmod 4$. Since γ is relatively prime to 2, this means that $b \equiv 0 \bmod 4$. Replacing b with 0 in either of the two congruences gives us $a \equiv 0 \bmod 4$.

The other direction is obvious. $\square$

Now we are in a position to prove the proposition we mentioned above.

Proposition 2.0.13. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2 and satisfy $\gamma \equiv \mu^2 \bmod 4$ for some $\mu \in \mathcal{O}_K$. If $\gamma^{1/2}$ is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4, then γ is a fourth power mod 4 in $\mathcal{O}_K$.*

Proof. If $\gamma^{1/2} \in K$, then $\mathcal{O}_{K(\gamma^{1/2})} = \mathcal{O}_K$, so the fact that $\gamma^{1/2}$ is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 means there is some $x \in \mathcal{O}_K$ such that $\gamma^{1/2} \equiv x^2 \bmod 4$. Squaring both sides gives $\gamma \equiv \alpha^4 \bmod 4$. (In fact, in this case, the congruence has to hold mod 8, and the restriction that γ be relatively prime to 2 is unnecessary.)

Now we assume that $\gamma^{1/2}$ is not in K. Corollary 2.0.11 shows that $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$ iff it is a square mod 4 in $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$. An arbitrary square in $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$ is $(x+y\frac{\mu+\gamma^{1/2}}{2})^2$ with $x, y \in \mathcal{O}_K$. Expanding this, we get the following:

$$\begin{aligned}
(x+y\frac{\mu+\gamma^{1/2}}{2})^2 &= x^2 + y^2\frac{\mu^2+\gamma+2\mu\gamma^{1/2}}{4} + 2xy\frac{\mu+\gamma^{1/2}}{2} \\
&= x^2 + y^2\frac{2\mu^2+2\mu\gamma^{1/2}+\gamma-\mu^2}{4} + 2xy\frac{\mu+\gamma^{1/2}}{2} \\
&= x^2 + y^2\frac{\mu^2+\mu\gamma^{1/2}}{2} + y^2\frac{\gamma-\mu^2}{4} + 2xy\frac{\mu+\gamma^{1/2}}{2} \\
&= x^2 + y^2\frac{\gamma-\mu^2}{4} + (\mu y^2 + 2xy)\frac{\mu+\gamma^{1/2}}{2}.
\end{aligned}$$

Since this is what an arbitrary square in $\mathcal{O}_K\left[\frac{\mu+\gamma^{1/2}}{2}\right]$ looks like, we now have that $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$ iff $\exists x, y \in \mathcal{O}_K$ such that we can write

$$\gamma^{1/2} \equiv x^2 + y^2\frac{\gamma - \mu^2}{4} + (\mu y^2 + 2xy)\frac{\mu + \gamma^{1/2}}{2} \bmod 4.$$

Subtracting $\gamma^{1/2}$ from both sides, we can rewrite this as

$$0 \equiv x^2 + y^2\frac{\gamma - \mu^2}{4} + \mu + (\mu y^2 + 2xy - 2)\frac{\mu + \gamma^{1/2}}{2} \bmod 4.$$

Applying the previous lemma, we find that this congruence is equivalent to the following two congruences:

$$\begin{aligned} x^2 + y^2\frac{\gamma - \mu^2}{4} + \mu &\equiv 0 \bmod 4 \\ \mu y^2 + 2xy - 2 &\equiv 0 \bmod 4. \end{aligned}$$

Reducing the second of these congruences mod 2, we see that $\mu y^2 \equiv 0 \bmod 2$. Since γ is relatively prime to 2, μ must be as well, so we have $y^2 \equiv 0 \bmod 2$. Now if we look at the first of the two congruences mod 2, we have $x^2 + \mu \equiv 0 \bmod 2$. Since $x^2 + \mu$ and $x^2 - \mu$ differ by a multiple of 2, we get $x^4 - \mu^2 = (x^2 + \mu)(x^2 - \mu) \equiv 0 \bmod 4$. This gives us $\gamma \equiv \mu^2 \equiv x^4 \bmod 4$ as desired. $\square$

We have just seen that if $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$, then γ is a fourth power mod 4 in $\mathcal{O}_K$. It is tempting to think that γ also must be a fourth power mod 8, reaching that conclusion by noting that if $\gamma^{1/2}$ is a square mod 4 (say, $\gamma^{1/2} \equiv \alpha^2 \bmod 4$), we have $(\gamma^{1/2} - \alpha^2)(\gamma^{1/2} + \alpha^2)$ divisible by 8. The problem with this line of reasoning is that $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$ rather than in $\mathcal{O}_K$ itself. So this argument tells us only that γ is a fourth power mod 8 in this larger ring.

In fact, γ does not have to be a fourth power mod 8 in $\mathcal{O}_K$ when $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$. Consider, for example, the case that $d = 155$. In this case, the fundamental unit in $\mathcal{O}_{K_0}$ is $249 + 20\sqrt{d} \equiv 1 + 4\sqrt{d}$ mod 8. Since $d \equiv -1$ mod 4, we have $\sqrt{d} \equiv i$ mod 2, so $\varepsilon_0 \equiv 1 + 4i$ mod 8 in $\mathcal{O}_{L_0}$. To determine whether this is a fourth power mod 8, we need only to consider potential fourth roots mod 2. If we take $\pi = (1 + i)$ and complete L_0 π-adically, then the only such potential roots are 1 and $1 + (1 + i) \equiv i$. The fourth power of both of these is 1, which is not congruent to $1 + 4i$ mod 8. Since it is not a fourth power mod 8 in the completion, it must not be one in L_0. Our results show that $\varepsilon_0^{1/2}$ is a square mod 4 in $\mathcal{O}_{L_0(\varepsilon_0^{1/2})}$. Thus, γ being a fourth power mod 8 in $\mathcal{O}_K$ is not necessary for $\gamma^{1/2}$ being a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$.

On the other hand, if $i \in K$ and there is only one prime above 2, it is easy to see that if γ is a fourth power mod 8 in $\mathcal{O}_K$, then $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$. (We see in the next result that this is also true when (2) is split.) This is because if $\gamma \equiv \alpha^4$ mod 8, we have $\gamma^{1/2} \equiv \pm\alpha^2$ mod 4, so $\gamma^{1/2}$ is a square mod 4.

Here, we see that a necessary and sufficient condition is stronger than requiring γ to be a fourth power mod 4 and is weaker than requiring γ to be a fourth power mod 8.

Proposition 2.0.14. *Let K be a number field with ring of integers $\mathcal{O}_K$ with $i \in K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2 and satisfy $\gamma \equiv \alpha^4$ mod 4 for some $\alpha \in \mathcal{O}_K$. Then $\gamma^{1/2}$ is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 iff there exists $\beta \in \mathcal{O}_K$ such that the following congruence is satisfied:*

$$\gamma \equiv \alpha^4(1 + 4i(1 + \beta)(1 + \beta i)) \textit{ mod } 8.$$

Proof. As in the previous proposition, if $\gamma^{1/2} \in K$, then $\mathcal{O}_{K(\gamma^{1/2})} = \mathcal{O}_K$. Then $\gamma^{1/2}$

is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 means there is some $x \in \mathcal{O}_K$ such that $\gamma^{1/2} \equiv x^2$ mod 4. Then $\gamma - x^4 = (\gamma^{1/2} - x^2)(\gamma^{1/2} + x^2) \equiv 0$ mod 8, because the two factors differ by a multiple of 2. If we take $\alpha = x$ and $\beta = 0$, then γ can be written in the desired form. On the other hand, if we can write γ as $\alpha^4(1 + 4i(1 + \beta)(1 + \beta i))$, take α^{-1} to be the inverse of α mod 4 and consider $((\alpha + \alpha\beta(1+i)) + \alpha^{-1}(1+i)\frac{\alpha^2+\gamma^{1/2}}{2})^2$, we find that this is congruent to $\alpha^2 + 2\alpha^2\beta(1 + i) + 2i\alpha^2\beta^2 + 2i\alpha^{-2}\frac{\gamma-\alpha^4}{4} + 2\frac{\alpha^2+\gamma^{1/2}}{2} =$ $\alpha^2 + 2\alpha^2\beta(1 + i) + 2i\alpha^2\beta^2 + 2i\alpha^{-2}\frac{\gamma-\alpha^4}{4} + \alpha^2 + \gamma^{1/2}$ mod 4. For this to be $\gamma^{1/2}$ mod 4, we need $2\alpha^2 + 2\alpha^2\beta(1 + i) + 2i\alpha^2\beta^2 + 2i\alpha^{-2}\frac{\gamma-\alpha^4}{4}$ to be 0 mod 4. So we need to show that $2i\alpha^{-2}\frac{\gamma-\alpha^4}{4} \equiv 2\alpha^2 + 2\alpha^2\beta(1+i) + 2i\alpha^2\beta^2$ mod 4. If we multiply both sides by $2i\alpha^2$, this is equivalent to $\gamma - \alpha^4 \equiv 4i\alpha^4 + 4\alpha^4\beta(1 + i) + 4\alpha^4\beta^2$ mod 8. This is equivalent to $\gamma \equiv \alpha^4(1 + 4i + 4\beta(1 + i) + 4\beta^2)$ mod 8. But this is the form that we have already assumed for γ, so this is true. Thus, the two conditions are equivalent when $\gamma^{1/2} \in K$.

If $\gamma^{1/2} \notin K$, in our proof of Proposition 2.0.13, we saw that $\gamma^{1/2}$ is a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 iff $\exists x, y \in \mathcal{O}_K$ satisfying

$$\begin{aligned} x^2 + y^2\frac{\gamma - \mu^2}{4} + \mu &\equiv 0 \bmod 4 \\ \mu y^2 + 2xy - 2 &\equiv 0 \bmod 4. \end{aligned}$$

In this case, we have taken μ to be α^2, so $\gamma^{1/2}$ being a square mod 4 in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 is equivalent to the existence of $x, y \in \mathcal{O}_K$ satisfying

$$\begin{aligned} x^2 + y^2\frac{\gamma - \alpha^4}{4} + \alpha^2 &\equiv 0 \bmod 4 \\ \alpha^2 y^2 + 2xy - 2 &\equiv 0 \bmod 4. \end{aligned}$$

The same argument we used in Proposition 2.0.13 shows that y^2 is divisible by 2. Since $i \in K$, this means that y is divisible by $(1+i)$. We write $y = z(1+i)$ with $z \in \mathcal{O}_K$. This lets us rewrite the two congruences as

$$\begin{aligned} x^2 + 2z^2 i\frac{\gamma - \alpha^4}{4} + \alpha^2 &\equiv 0 \bmod 4 \\ 2\alpha^2 z^2 i + 2xz(1+i) &\equiv 2 \bmod 4. \end{aligned}$$

We can divide the second of the two congruences by 2 to get

$$\begin{aligned} x^2 + 2z^2 i\frac{\gamma - \alpha^4}{4} + \alpha^2 &\equiv 0 \bmod 4 \\ \alpha^2 z^2 i + xz(1+i) &\equiv 1 \bmod 2. \end{aligned}$$

Now note that looking at the first congruence mod 2 gives $\alpha^2 \equiv x^2 \bmod 2$. This means that $\alpha \equiv x \bmod (1+i)$, so we can replace $xz(1+i)$ with $\alpha z(1+i)$ in the second congruence. This allows us to rewrite the two congruences as

$$\begin{aligned} x^2 + 2z^2 i\frac{\gamma - \alpha^4}{4} + \alpha^2 &\equiv 0 \bmod 4 \\ (\alpha z)^2 i + (\alpha z)(1+i) &\equiv 1 \bmod 2. \end{aligned}$$

Note that in the second congruence, we can move the 1 to the left-hand side and factor to get $(1+\alpha z)(1+\alpha z i) \equiv 0 \bmod 2$. At least one of these factors must be divisible by $1+i$ and the two factors differ by a multiple of $1+i$, so both factors are divisible by $1+i$. (The argument for this is essentially identical to the proof of Lemma 1.1.7.) In particular, we have $\alpha z \equiv 1 \bmod 1+i$. Thus, the second of these two congruences implies that $\alpha z \equiv 1 \bmod 1+i$. On the other hand, if $\alpha z \equiv 1 \bmod 1+i$, that congruence is certainly satisfied. Taken together, these two implications mean that $\alpha z \equiv 1 \bmod 1+i$ is equivalent to $(\alpha z)^2 i + (\alpha z)(1+i) \equiv 1 \bmod 2$.

Thus, satisfying the two congruences above is equivalent to satisfying the following two congruences:

$$\begin{aligned} x^2 + 2z^2 i\frac{\gamma - \alpha^4}{4} + \alpha^2 &\equiv 0 \bmod 4 \\ \alpha z &\equiv 1 \bmod (1+i). \end{aligned}$$

Moreover, the second congruence implies that $z \equiv \alpha^{-1} \bmod (1+i)$, which implies that $z^2 \equiv \alpha^{-2} \bmod 2$. (This is because $(z-\alpha^{-1})$ and $(z+\alpha^{-1})$ are both divisible by $(1+i)$.) Multiplying the latter congruence by 2 gives $2z^2 \equiv 2\alpha^{-2} \bmod 4$. Replacing $2z^2$ with $2\alpha^{-2}$ in the first congruence gives this equivalent pair of congruences:

$$\begin{aligned} x^2 + 2\alpha^{-2} i\frac{\gamma - \alpha^4}{4} + \alpha^2 &\equiv 0 \bmod 4 \\ \alpha z &\equiv 1 \bmod (1+i). \end{aligned}$$

Since γ is relatively prime to 2, α is as well. This means that we know that α has an inverse mod $(1+i)$. But now that z has been removed from the first congruence, this is all that the second congruence is saying. So under our assumptions, the existence of an x and z satisfying both of the above congruences is equivalent to the existence of an x satisfying the single congruence:

$$x^2 + 2\alpha^{-2} i\frac{\gamma - \alpha^4}{4} + \alpha^2 \equiv 0 \bmod 4.$$

We can rewrite this as

$$2\alpha^{-2} i\frac{\gamma - \alpha^4}{4} \equiv -(x^2 + \alpha^2) \bmod 4.$$

Now multiplying both sides by $-2i\alpha^2$ and moving the α^4 to the right-hand side gives the equivalent

$$\gamma \equiv \alpha^4 + 2i\alpha^2(x^2 + \alpha^2) \bmod 8.$$

Since $x^2 \equiv \alpha^2 \bmod 2$, we have $x \equiv \alpha \bmod (1+i)$, so write $x = \alpha + b(1+i)$ to get

$$\begin{aligned}
\gamma &\equiv \alpha^4 + 2i\alpha^2(\alpha^2 + 2b(1+i)\alpha + 2ib^2 + \alpha^2) \bmod 8 \\
&\equiv \alpha^4 + 4i\alpha^4(1 + b(1+i)\alpha^{-1} + ib^2\alpha^{-2}) \bmod 8 \\
&\equiv \alpha^4(1 + 4i(1 + b(1+i)\alpha^{-1} + ib^2\alpha^{-2})) \bmod 8.
\end{aligned}$$

Since $b\alpha^{-1}$ is relevant only mod $1+i$ and α is relatively prime to 2, multiplying the set of possible b values by α^{-1} permutes, but does not change, that set of possible values. Thus, the existence of a b that satisfies this congruence is equivalent to the existence of a β satisfying the following congruence:

$$\begin{aligned}
\gamma &\equiv \alpha^4(1 + 4i(1 + \beta(1+i) + i\beta^2)) \bmod 8 \\
&\equiv \alpha^4(1 + 4i(1+\beta)(1+\beta i)) \bmod 8.
\end{aligned}$$

□

We often find it more convenient to work with a slightly different form of the statement above:

Corollary 2.0.15. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2 and satisfy $\gamma \equiv \alpha^4 \bmod 4$ for some $\alpha \in \mathcal{O}_K$. Then $\gamma^{1/2}$ is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 iff there exists $\delta \in \mathcal{O}_K$ such that the following congruence is satisfied:*

$$\gamma \equiv \alpha^4(1 + 4(1+i)\delta + 4\delta^2) \bmod 8.$$

Proof. We have just seen that $\gamma^{1/2}$ is a square in $\mathcal{O}_{K(\gamma^{1/2})}$ mod 4 iff there is some $\beta \in \mathcal{O}_K$ satisfying $\gamma \equiv \alpha^4(1 + 4i(1+\beta)(1+\beta i)) \bmod 8$. Now we rewrite this congruence after a change of variables of $\delta = 1 + \beta$.

With $\delta = 1+\beta$, we have $1+\beta i \equiv 1+i+i+\beta i = (1+i)+i\delta \bmod 2$. Then the congruence can be written

$$\gamma \equiv \alpha^4(1+4i\delta((1+i)+\delta i)) \bmod 8.$$

Distributing the $4i\delta$ (and ignoring the signs of terms divisible by 4) results in

$$\gamma \equiv \alpha^4(1+4(1+i)\delta+4\delta^2) \bmod 8.$$

□

We can combine these results with Proposition 2.0.8 to get the following theorem:

Theorem 2.0.16. *Let K be a number field with ring of integers $\mathcal{O}_K$ with $i \in K$. Let $\gamma \in \mathcal{O}_K$ be relatively prime to 2 be such that $(\gamma) = I^4$ for some ideal I in $\mathcal{O}_K$ and satisfies $\gamma \equiv \mu^2$ mod 4 for some $\mu \in \mathcal{O}_K$. Then the following are equivalent:*

1. *$K(\gamma^{1/4})/K$ is unramified*
2. *$\exists \alpha, \beta \in \mathcal{O}_K$ such that $\gamma \equiv \alpha^4(1+4i(1+\beta)(1+\beta i))$ mod 8*
3. *$\exists \alpha, \delta \in \mathcal{O}_K$ such that $\gamma \equiv \alpha^4(1+4(1+i)\delta+4\delta^2)$ mod 8*
4. *$\exists \alpha \in \mathcal{O}_K$ such that $\gamma \equiv \alpha^4$ mod 4 and, for any such α, $\exists \beta \in \mathcal{O}_K$ satisfying $\gamma \equiv \alpha^4(1+4i(1+\beta)(1+\beta i))$ mod 8*
5. *$\exists \alpha \in \mathcal{O}_K$ such that $\gamma \equiv \alpha^4$ mod 4 and, for any such α, $\exists \delta \in \mathcal{O}_K$ satisfying $\gamma \equiv \alpha^4(1+4(1+i)\delta+4\delta^2)$ mod 8.*

Proof. $K(\gamma^{1/4})/K$ is unramified iff $K(\gamma^{1/2})/K$ and $K(\gamma^{1/4})/K(\gamma^{1/2})$ are both unramified. Because $(\gamma) = (I^2)^2$ and $(\gamma^{1/2}) = I^2$, we can apply Proposition 2.0.8. This tells us that both of those extensions are unramified iff γ is a square mod 4 in K

and $\gamma^{1/2}$ is a square mod 4 in $K(\gamma^{1/2})$. We have assumed that γ is a square mod 4 in K, so in our case, $K(\gamma^{1/4})/K$ is totally unramified iff $\gamma^{1/2}$ is a square mod 4 in $K(\gamma^{1/2})$.

Proposition 2.0.8, Proposition 2.0.13 and Proposition 2.0.14 show that 1 implies 4. Proposition 2.0.8, Proposition 2.0.13 and Corollary 2.0.15 show that 1 implies 5. It is obvious that 4 implies 2 and 5 implies 3. Proposition 2.0.8 and Proposition 2.0.14 together show that 2 implies 1 and Proposition 2.0.8 and Corollary 2.0.15 shows that 3 implies 1. Thus, all five are equivalent. $\square$

The rest of our results come from applications of this theorem.

Chapter 3: Ramification Implications of Particular Congruence Conditions

Our main results give the generators of some unramified extensions of L_j for various j. In particular, for $d \equiv 1 \bmod 2$ and for all j, we give necessary and sufficient conditions for $\gamma^{1/4}$ to give an unramified extension of L_j when $\gamma \in K_0$ is such that γ is relatively prime to 2, $\sqrt{\gamma} \notin K_0$, and $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. Note that when $\gamma = \varepsilon_0$, the fundamental unit of K_0, these last three conditions are satisfied. We also occasionally point out some additional restrictions that arise in this special case.

Each congruence class of d mod 8 (with $d \equiv 1 \bmod 2$) is handled separately, but before we delve into each of these congruence classes, it is useful to establish the ramification behavior associated with the fourth roots of certain values.

3.1 Congruences resulting in unramified extensions

The first congruences we deal with are ones that have fourth roots that, at least somewhere in the L-tower, result in unramified extensions. The proofs that result in unramified extensions are very straightforward. They consist of providing an α and β (or δ) that satisfy Proposition 2.0.14 or Corollary 2.0.15. The proofs also show that, for some low values of j, adjoining some of these fourth roots results in a ramified extension. These aspects of the proofs are slightly more complicated.

Lemma 3.1.1. *Let* $\gamma \in \mathcal{O}_{L_0}$ *be such that* $\gamma \equiv 1 \bmod 8$*. Then* $L_j(\gamma^{1/4})/L_j$ *is unramified for all* $j \geq 0$*.*

Proof. We can take $\alpha = 1$ and $\delta = 0$ to have γ be of the proper form to satisfy statement 3 of Theorem 2.0.16. This tells us that $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 0$. □

The next lemma we would like to prove is one that shows what the ramification behavior is when $\gamma \equiv -1 \bmod 8$. In that case, the extension of L_0 turns out to be ramified, which requires a little more work to prove. We need to reuse the argument for this in other lemmas, so we find it useful to prove first a helper lemma.

Lemma 3.1.2. *Let* $\gamma \in \mathcal{O}_{L_0}$ *be such that* $L_0((-\gamma)^{1/4})/L_0$ *is unramified. Then* $L_0(\gamma^{1/4})/L_0$ *is ramified and* $L_j(\gamma^{1/4})/L_j$ *is unramified for all* $j \geq 1$*.*

Proof. Since $L_0((-\gamma)^{1/4})/L_0$ is unramified and unramified extensions lift to unramified extensions, it follows that $L_j(\gamma^{1/4})/L_j = L_j((-\gamma)^{1/4})/L_j$ is unramified for all $j \geq 1$.

Note that $L_0(\gamma^{1/4}, \zeta_8)/L_0(\gamma^{1/4})$ is the lift of $L_0((-\gamma)^{1/4})/L_0(\gamma^{1/2})$. That extension is a subextension of $L_0((-\gamma)^{1/4})/L_0$, which we have assumed to be unramified. Since unramified extensions lift to unramified extensions, $L_0(\gamma^{1/4}, \zeta_8)/L_0(\gamma^{1/4})$ must be unramified. But $L_0(\gamma^{1/4}, \zeta_8)/L_0$ cannot be unramified because it contains $L_0(\zeta_8)/L_0$, which ramifies above 2 ($(1+i) = (1+\zeta_8)^2$). Thus $L_0(\gamma^{1/4})/L_0$ must be ramified. □

$$\begin{tikzcd}
& L_0(\gamma^{1/4}, \zeta_8) \arrow[dl, dash] \arrow[dr, dash] & \\
L_0(\gamma^{1/4}) \arrow[dr, dash] & & L_0((-\gamma)^{1/4}) \arrow[dl, dash] \\
& L_0(\gamma^{1/2}) \arrow[d, dash] & \\
& L_0 &
\end{tikzcd}$$

Figure 3.1: $L_0(\gamma^{1/4}, \zeta_8)/L_0(\gamma^{1/4})$ is the lift of $L_0((-\gamma)^{1/4})/L_0(\gamma^{1/2})$

Combining Lemma 3.1.1 and Lemma 3.1.2 immediately gives us:

Lemma 3.1.3. *Let $\gamma \in \mathcal{O}_{L_0}$ be such that $\gamma \equiv -1$ mod 8. Then $L_0(\gamma^{1/4})/L_0$ is ramified, and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$.*

We can generalize these slightly to the following pair of lemmas where the second one follows immediately from the first and Lemma 3.1.2.

Lemma 3.1.4. *Let $\gamma \in \mathcal{O}_{L_0}$ be such that $\gamma \equiv 1 + bi$ with $b \in \mathbb{Z}$ satisfying $b \equiv 0$ mod 4. Then $L_j(\gamma^{1/4})/L_j$ is unramified for all j.*

Proof. If $b \equiv 0$ mod 8, this is just Lemma 3.1.1.

If $b \equiv 4$ mod 8, then we have $1 + 4i$. Now let $\alpha = \delta = 1$ and note that $\alpha^4(1 + 4(1 + i)\delta + 4\delta^2) = (1 + 4 + 4i + 4) \equiv 1 + 4i$ mod 8. Thus, the equivalence of 1 and 3 in Theorem 2.0.16 proves the result. □

Lemma 3.1.5. *Let $\gamma \in \mathcal{O}_{L_0}$ be such that $\gamma \equiv -1 + bi$ with $b \in \mathbb{Z}$ satisfying $b \equiv 0$ mod 4. Then $L_0(\gamma^{1/4})/L_0$ is ramified and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$.*

Now we deal with a scenario that requires us to show that both $L_0(\gamma^{1/4})/L_0$ and $L_1(\gamma^{1/4})/L_1$ ramify in a situation where $L_0((-\gamma)^{1/4})/L_0$ ramifies as well. This requires a little more work than the lemmas we have proved so far in this chapter.

Lemma 3.1.6. *Let $\gamma \in \mathcal{O}_{L_0}$ be such that $\gamma \equiv a \pm i$ with $a \in \mathbb{Z}$ satisfying $a \equiv 0$ mod 4. Then $L_0(\gamma^{1/4})/L_0$ and $L_1(\gamma^{1/4})/L_1$ are both ramified, while $L_j(\gamma^{1/4})/L_j$ is unramified for $j \geq 2$.*

Proof. First, we show that adjoining $\gamma^{1/4}$ to L_0 or L_1 gives a ramified extension. Because unramified extensions lift to unramified extensions, it is sufficient to show that $L_1(\gamma^{1/4})/L_1$ is ramified.

Theorem 2.0.16 tells us that it is enough to show that γ is not a fourth power mod 4 in L_1. The congruence conditions on a and b imply that $\gamma \equiv \pm i$ mod 4. Since -1 is a fourth power in L_1, i is a fourth power mod 4 iff $-i$ is. Thus, we need only to show that i is not a fourth power mod 4 in L_1.

Although we are trying to show something about L_1, we find it convenient to start by working in L_2 where we have ζ_{16}. Let $\alpha \in L_2$ be such that $\alpha^4 \equiv i$ mod 4. This is equivalent to $\alpha^2 \equiv \zeta_8$ mod 2, so $\alpha \equiv \zeta_{16}$ mod $(1+i)$. This means we have $\alpha = \zeta_{16} + (1+i)\lambda$. Now write $1 + \alpha - (1+i)\lambda = 1 + \zeta_{16}$ and consider the 2-adic valuations on both sides. The right-hand side has valuation $\frac{1}{8}$. The valuation of the left-hand side is at least as large as the minimum of $v(1+\alpha)$ and $v(1+i) + v(\lambda)$, and if those are not the same, it must be exactly that minimum. Moreover, since λ must be in the ring of integers, it cannot have negative valuation. Thus, we have $v(1+i)+v(\lambda) \geq v(1+i) = \frac{1}{2} > \frac{1}{8}$. This means $v(1+\alpha)$ must be $\frac{1}{8}$. Since nothing in L_1 has such a valuation (the smallest positive valuation comes from $(1+\zeta_8)$ which has valuation $\frac{1}{4}$), there can be no such $\alpha \in L_2$, which means there can also be no such $\alpha \in L_1$.

Now we consider $L_j(\gamma^{1/4})/L_j$ for $j \geq 2$. Again, we show that γ has the necessary form mod 8 and apply Theorem 2.0.16 . Since -1 is a fourth power this far up on the L-tower, it is sufficient to consider the behavior when $\gamma \equiv i \bmod 8$ and when $\gamma \equiv 4+i \bmod 8$.

If $\gamma \equiv i \bmod 8$, then we can satisfy the form $\alpha^4(1+4(1+i)\delta+4\delta^2)$ with $\alpha = \zeta_{16}$ and $\delta = 0$. If $\gamma \equiv 4+i \bmod 8$, then we satisfy the form $\alpha^4(1+4i(1+\beta)(1+\beta i))$ by taking $\alpha = \zeta_{16}$ and $\beta = 0$. $\square$

The previous lemmas have all shown congruence conditions on γ that cause $L_j(\gamma^{1/4})/L_j$ to be unramified. The last such lemmas that we give are particularly useful when there is a cube root of unity in the base field. Of course, sometimes L_j does not have a primitive cube root of unity mod 4 or mod 8. It does, however, when $d \equiv \pm 3$ mod a high enough power of 2, because $\sqrt{d} \equiv \pm\sqrt{\pm 3} \bmod 8$, and, $\sqrt{-3}$ can be used to build the cube root of unity.

Lemma 3.1.7. *Let $\gamma \in \mathcal{O}_{L_0}$ be such that $\gamma^3 \equiv 1$ mod 8. Then $L_j(\gamma^{1/4})/L_j$ is unramified for all j.*

Proof. We can take $\alpha = \gamma$ and $\delta = 0$ to have γ be of the proper form to satisfy 3 of Theorem 2.0.16. This tells us that $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 0$. $\square$

Just as with Lemma 3.1.1, we can combine Lemma 3.1.2 with the previous lemma to get a lemma describing the behavior of the negative.

Lemma 3.1.8. *Let $\gamma \in \mathcal{O}_{L_0}$ be such that $\gamma^3 \equiv -1$ mod 8. Then $L_0(\gamma^{1/4})/L_0$ is ramified and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$.*

3.2 Congruences resulting in ramified extensions

In Section 3.1 we gave certain congruence conditions for γ that would mean that $L_j(\gamma^{1/4})/L_j$ was unramified for some γ. Now we show some congruence conditions on γ that imply that $L_j(\gamma^{1/4})/L_j$ is ramified for all j. Not surprisingly, this is somewhat more complicated. One reason for this is that we are trying to show the behavior for all j rather than for a particular j. (In the last section, we did this as well, but trivially so because unramified extensions lift to unramified extensions.) Another source of additional complication is that, when showing that extensions were unramified, Theorem 2.0.16 allowed us to prove it simply by offering an α and a β (or δ) that satisfy a particular congruence. Now we have to show that no such α and β (or δ) can exist. We got a taste for this complication in the previous section. The bulk of the work in that section was in proving Lemma 3.1.2 and in proving that $L_0(\gamma^{1/4})/L_0$ and $L_1(\gamma^{1/4})/L_1$ ramify in Lemma 3.1.6.

3.2.1 Tools for showing extensions are ramified

The extra complications mean that we can benefit from some additional machinery. When we are trying to show that no such α and β (or δ) can exist, we do one of two things. Either we show that there is no α anywhere in the L-tower such that $\gamma \equiv \alpha^4 \bmod 4$, or we give some α such that $\gamma \equiv \alpha^4 \bmod 4$ and show that there is no β satisfying $\gamma \equiv \alpha^4(1 + 4i(1 + \beta)(1 + \beta i)) \bmod 8$ (or that there is no δ satisfying $\gamma \equiv \alpha^4(1 + 4(1 + i)\delta + 4\delta^2) \bmod 8$). The extra machinery is for handling this latter case, particularly in the δ form.

Observe that if we have $\gamma \equiv \alpha^4 \bmod 4$, then $\alpha^4 - \gamma = 4k$. By subtracting γ from both sides and dividing by 4, we convert $\gamma \equiv \alpha^4(1+4(1+i)\delta+4\delta^2) \bmod 8$ to $0 \equiv k+(1+i)\delta+\delta^2 \bmod 2$. The following proposition and associated corollaries are useful for working with congruences of this form, so are powerful tools for showing that certain extensions are ramified everywhere in the L-tower. There are other, similar, congruences that arise, so we make the proposition fairly general. Before the proposition, we have a technical lemma that helps prove the proposition.

Lemma 3.2.1. *Let $n > 2$ be a power of 2 and let ζ_n be a primitive nth root of unity. Let k be an algebraic integer in $\overline{\mathbb{Q}}$. Let $\delta \in \overline{\mathbb{Q}}$ satisfy $k + \delta(1+\zeta_n)^z + \delta^2 \equiv 0$ mod $(1+\zeta_n)^{2z}$ where $z > 0$ and $z \cdot v(1+\zeta_n) \leq \frac{1}{2}$. Then $\delta = k^{1/2} + \lambda(1+\zeta_{2n})^z$ with λ satisfying $k^{1/2} + \lambda(1+\zeta_{2n})^z + \lambda^2 \equiv 0$ mod $(1+\zeta_n)^z$.*

Proof. Reducing the congruence mod $(1+\zeta_n)^z$, we have $\delta^2 \equiv k \bmod (1+\zeta_n)^z$. This means $\delta \equiv k^{1/2} \bmod (1+\zeta_{2n})^z$. Now we write $\delta = k^{1/2} + \lambda(1+\zeta_{2n})^z$. Substituting this into the original congruence gives

$$\begin{aligned} 0 &\equiv k + \delta(1+\zeta_n)^z + \delta^2 \\ &\equiv k + (k^{1/2} + \lambda(1+\zeta_{2n})^z)(1+\zeta_n)^z + k + \lambda^2(1+\zeta_{2n})^{2z} \\ &\equiv (k^{1/2} + \lambda(1+\zeta_{2n})^z)(1+\zeta_n)^z + \lambda^2(1+\zeta_n)^z \bmod (1+\zeta_n)^{2z}. \end{aligned}$$

Throughout this, we have taken advantage of the restriction on z, which ensures that $(1+\zeta_n)^{2z}$ divides 2. Dividing through by $(1+\zeta_n)^z$ gives $k^{1/2} + \lambda(1+\zeta_{2n})^z + \lambda^2 \equiv 0$ mod $(1+\zeta_n)^z$. □

Now that we have that technical lemma, we can use it to prove the following proposition. Note that the condition that $k^{1/(2^{j+3-N})} \in L_j$ is ensuring that we have a particular power of k in L_0 and that, starting with that value, we can take successive square roots as we move up the L-tower.

Proposition 3.2.2. *Let $j \in \mathbb{N}$. Let $n = 2^N \geq 4$ with $j > N - 3$, and let ζ_n be a primitive nth root of unity. Let k be an algebraic integer in $\overline{\mathbb{Q}}$ and z be an odd integer such that the following conditions are true:*

- *$\exists x \in L_j$ such that $x^{2^{j+3-N}} \equiv k \text{ mod } (1+\zeta_n)^{2z}$*
- *$v(k) < z2^{1-N}$*
- *$v(v(k)) > 2 - N$*
- *$z \cdot v(1+\zeta_n) \leq \frac{1}{2}$.*

(Note that if k is relatively prime to 2, then $v(k) = 0$ and $v(v(k)) = \infty$, so the second and third conditions are immediately satisfied.) Let $\delta \in \overline{\mathbb{Q}}$ satisfy $k + \delta(1+\zeta_n)^z + \delta^2 \equiv 0 \text{ mod } (1+\zeta_n)^{2z}$. Then $\delta \notin L_j$.

Proof. We can apply the previous lemma $j + 4 - N$ times to get

$$\begin{aligned}\delta &= k^{1/2} + k^{1/4}(1+\zeta_{2n})^z + \cdots + k^{1/(2^{j+4}/n)}(1+\zeta_{2n})^z(1+\zeta_{4n})^z \cdots (1+\zeta_{2^{j+3}})^z \\ &\quad + (1+\zeta_{2n})^z(1+\zeta_{4n})^z \cdots (1+\zeta_{2^{j+4}})^z \alpha.\end{aligned}$$

In an abuse of notation, we use $k^{1/2^m}$ to represent $x^{2^{j+3-N-m}}$. In the last of the $j + 4 - N$ applications, we need $k^{1/(2^{j+4}/n)} = x^{1/2}$. There may not be such an element in L_j, so we use the true root in $\overline{\mathbb{Q}}$.

Assume that $\delta \in L_j$. Now we move all but the last two terms on the right-hand side to the left-hand side to get

$$\delta + k^{1/2} + k^{1/4}(1+\zeta_{2n})^z + \cdots + k^{1/(2^{j+3}/n)}(1+\zeta_{2n})^z(1+\zeta_{4n})^z \cdots (1+\zeta_{2^{j+2}})^z =$$

$$k^{1/(2^{j+4}/n)}(1+\zeta_{2n})^z(1+\zeta_{4n})^z\cdots(1+\zeta_{2^{j+3}})^z+(1+\zeta_{2n})^z(1+\zeta_{4n})^z\cdots(1+\zeta_{2^{j+4}})^z\alpha.$$

Note that $\zeta_{2^{j+2}} \in L_j$. Our powers of k on the left-hand side are actually powers of x, which is also in L_j. Thus, the left-hand side is a sum of elements of L_j so is in L_j itself.

Now consider the valuation of the right-hand side. The valuation of the first term is $\frac{1}{2^{j+4-N}}v(k)+z\frac{1}{2^N}+z\frac{1}{2^{N+1}}+\cdots+z\frac{1}{2^{j+2}}$ because the valuation of $(1-\zeta_{2^x})$ is $\frac{1}{2^{x-1}}$. The valuation of the second term is $z\frac{1}{2^N}+z\frac{1}{2^{N+1}}+\cdots+z\frac{1}{2^{j+2}}+z\frac{1}{2^{j+3}}+v(\alpha)$. By assumption $v(k) < z2^{1-N}$, so the valuation of the first term is strictly less than

$$\begin{aligned}
& z(\frac{1}{2^{j+4-N}}2^{1-N}+\frac{1}{2^N}+\frac{1}{2^{N+1}}+\cdots+\frac{1}{2^{j+2}}) \\
= \; & z(2^{-(j+3)}+\frac{1}{2^N}+\frac{1}{2^{N+1}}+\cdots+\frac{1}{2^{j+2}}) \\
= \; & z(\frac{1}{2^N}+\frac{1}{2^{N+1}}+\cdots+\frac{1}{2^{j+2}}+\frac{1}{2^{j+3}}) \\
\leq \; & z(\frac{1}{2^N}+\frac{1}{2^{N+1}}+\cdots+\frac{1}{2^{j+2}}+\frac{1}{2^{j+3}})+v(\alpha),
\end{aligned}$$

which is the valuation of the second term. Since the valuations of the two terms are not equal, the sum of their valuations is the minimum of the two valuations. Thus, the valuation of the right-hand side is the valuation of its first term, namely $\frac{1}{2^{j+4-N}}v(k)+z\frac{1}{2^N}+z\frac{1}{2^{N+1}}+\cdots+z\frac{1}{2^{j+2}}$.

Since $v(v(k)) > 2-N$, the valuation of the first term of this valuation is greater than $-(j+4-N)+2-N = -(j+2)$. Thus, the valuation of the sum $\frac{1}{2^{j+4-N}}v(k)+z\frac{1}{2^N}+z\frac{1}{2^{N+1}}+\cdots+z\frac{1}{2^{j+2}}$ is exactly the valuation of the term with the minimum valuation, namely $-(j+2)$, which is the valuation of $z\frac{1}{2^{j+2}}$ (recall that z is an odd integer). But the minimum valuation of a valuation in L_j is $-(j+1)$. Thus, the right-hand side cannot be in L_j.

This contradicts the fact that the left-hand side is in L_j, so we must have $\delta \notin L_j$. □

In proving our corollaries, we use the fact that the second and third conditions above are satisfied if k is relatively prime to 2. The first of these corollaries addresses the case that k is congruent to a root of unity ζ_m. In order to satisfy the condition in the previous proposition that we can keep taking square roots as we go up the L-tower, we have to put some restrictions on the value of m.

Corollary 3.2.3. *Let $n = 2^N \geq 4$ and let ζ_n be a primitive nth root of unity. Let $m, M, m_1 \in \mathbb{Z}$ be such that $m = m_1 2^M$, $M \leq N-1$, and m_1 is relatively prime to 2. Let z be an odd, positive integer satisfying $z \cdot v_2(1+\zeta_n) \leq \frac{1}{2}$. Let $k, k_e \in L_0$ be such that $k \equiv k_e \zeta_{2^M}$ mod $(1+\zeta_n)^{2z}$ and $k_e^{m_1} \equiv 1$ mod $(1+\zeta_n)^{2z}$. Let δ be an algebraic integer in $\overline{\mathbb{Q}}$ satisfying $k + \delta(1+\zeta_n)^z + \delta^2 \equiv 0$ mod $(1+\zeta_n)^{2z}$. Then $\delta \notin L_j$ for any j.*

Proof. Showing that $\delta \notin L_J$ for $J > j$ also shows that $\delta \notin L_j$. This means that it suffices to show the result for sufficiently large j. In particular, we may assume that $j > N-3$ so that we can apply the previous proposition.

Note that $k^m \equiv 1 \bmod (1+\zeta_n)^{2z}$, so k is relatively prime to 2, and the valuation conditions from Proposition 3.2.2 are satisfied. It remains to show that, for every j, $\exists k_j \in L_j$ such that $k_j^{(2^{j+3-N})} \equiv k \bmod (1+\zeta_n)^{2z}$.

We claim that we can take k_j to be $k_e^{t_j}\zeta_{2^{s_j+M}}$ where $s_j = j+3-N$ and t_j is the inverse of 2^{s_j} mod m_1, which must exist since 2 is relatively prime to m_1. To confirm this, we must show that this choice of k_j is in L_j and that $k_j^{(2^{j+3-N})} \equiv k$

mod $(1+\zeta_n)^{2z}$. We have assumed $k_e \in L_0$, so $k_e \in L_j$ for all j. Moreover, $\zeta_{2^{s_j+M}}$ is a $2^{j+3-N+M}$th root of unity. We know that L_j has a 2^{j+2}th root of unity. Since $M \leq N-1$, we know that $j+3-N+M \leq j+2$, so $\zeta_{2^{s_j+M}} \in L_j$. Thus, $k_j \in L_j$ for all j. Moreover, $k_j^{(2^{j+3-N})} = k_j^{2^{s_j}} = (k_e^{t_j}\zeta_{2^{s_j+M}})^{2^{s_j}} = k_e^{t_j 2^{s_j}}\zeta_{2^M}$. Since $k_e^{m_1} \equiv 1$ mod $(1+\zeta_n)^{2z}$ and t_j was chosen to be the inverse of 2^{s_j} mod m_1, it follows that $k_e^{t_j 2^{s_j}} \equiv k_e$ mod $(1+\zeta_n)^{2z}$. Thus, $k_j^{(2^{j+3-N})} \equiv k_e\zeta_{2^M} \equiv k$ mod $(1+\zeta_n)^{2z}$ as desired. □

We now use the preceding corollary to prove the same result for three specific congruence conditions on k. The first of these has $k \equiv 1$. Based on Proposition 3.2.2, we should expect this to work, because we can obviously start with 1 and keep taking square roots as often as we want. The roots do not have to be primitive, so 1 suffices at each level.

Corollary 3.2.4. *Let $n = 2^N \geq 4$ and let ζ_n be a primitive nth root of unity. Let δ be an algebraic integer in $\overline{\mathbb{Q}}$ satisfying $1+\delta(1+\zeta_n)^z+\delta^2 \equiv 0$ mod $(1+\zeta_n)^{2z}$, where z is an odd, positive integer satisfying $z \cdot v(1+\zeta_n) \leq \frac{1}{2}$. Then $\delta \notin L_j$ for any j.*

Proof. In terms of the previous corollary, we have $m_1 = 1$ and $M = 0$. Obviously $m_1 = 1$ is relatively prime to 2. Moreover, since $n > 2$, we have $N > 1$, so $M = 0 < N-1$, so the conditions of the corollary are met. □

In fact, the same argument suffices for proving something slightly more general. If we have something congruent to ζ_m in L_0, we can expect to be able to take a new square root each time we move up the L-tower because when m is relatively prime to 2, any power of 2 has an inverse mod m, so a $\frac{1}{2^n}$th root of ζ_m can just be written as a power of ζ_m.

Corollary 3.2.5. *Let $n = 2^N \geq 4$ and let ζ_n be a primitive nth root of unity. Let δ be an algebraic integer in $\overline{\mathbb{Q}}$ satisfying $k + \delta(1+\zeta_n)^z + \delta^2 \equiv 0 \bmod (1+\zeta_n)^{2z}$, where z is an odd, positive integer with $z \cdot v(1+\zeta_n) \leq \frac{1}{2}$, m is odd, and $k^m \equiv 1 \bmod (1+\zeta_n)^{2z}$. Then $\delta \notin L_j$ for any j.*

Proof. This is the same argument as in Corollary 3.2.4. In terms of Corollary 3.2.3, we have $m_1 = m$ and $M = 0$. We have taken m to be odd, so it is relatively prime to 2. Moreover, since $n > 2$, we have $N > 1$, so $M = 0 < N - 1$, so the conditions of the corollary are met. $\square$

There are times, however, that we need to deal with a more complicated value for k. In particular, we have to consider cases where k is congruent to a sum of roots of unity, some of which are not in L_0 mod 4. For this situation, we have the following corollary:

Corollary 3.2.6. *Let $n = 2^N \geq 4$ and let ζ_n be a primitive nth root of unity. Let k be a finite sum of roots of unity in L_{N-3} with $v(k) < z2^{1-N}$ and $v(v(k)) > 2 - N$. Let δ be an algebraic integer in $\overline{\mathbb{Q}}$ satisfying $k + \delta(1+\zeta_n)^z + \delta^2 \equiv 0 \bmod (1+\zeta_n)^{2z}$, where z is an odd, positive integer with $z \cdot v(1+\zeta_n) \leq \frac{1}{2}$. Then $\delta \notin L_j$ for any j.*

Proof. As in the proof of Corollary 3.2.3, we can take $j > N-3$. Then we have kept most of the conditions of Proposition 3.2.2. The only thing that we need to prove is that if k is a finite sum of roots of unity in L_{N-3}, then $\exists k_j \in L_j$ with $k_j^{2^{j+3-N}} \equiv k$ mod $(1+\zeta_n)^{2z}$. Since k is a finite sum of roots of unity and we are looking at it only mod some divisor of 2, we can create k_j by replacing each term ζ_x^y in k with $\zeta_{2^m x}^y$. Because ζ_x was in L_{N-3}, this term must be in L_{N-3+m}. In particular, k_j must be in $L_{N-3+j+3-N} = L_j$. $\square$

An alternate approach

Although the previous proposition and corollaries are our tools throughout the rest of this section, it is interesting to note another approach to handling congruences of the form $0 \equiv k + (1+i)\delta + \delta^2 \bmod 2$ (or similar forms). Because $(1+i) \in L_0$, the following proposition tells us that if there is going to be a δ satisfying the congruence, it must come from the same field as k. When k comes from a particularly low field on the tower, there are not many possibilities for δ and the fact that none of them satisfies the congruence can be proven directly. While this does not seem to be as powerful or easy to work with as the tools above, it has the advantage that it limits the search space that must be explored to look for possible δs if it is unknown whether one exists.

Proposition 3.2.7. *Let $\wp$ be a prime above 2 in L_j. Let $c, k \in \mathcal{O}_{L_{j-1}}$ and $\delta \in \mathcal{O}_{L_j}$ satisfy $\delta^2 + c\delta + k \equiv 0 \bmod \wp^x$ for some $x \in \mathbb{Z}$ with $\wp^x$ dividing 2 and $v_\wp(c) \leq \frac{x}{2}$. Then $\exists \lambda \in \mathcal{O}_{L_{j-1}}$ such that $\lambda^2 + c\lambda + k \equiv 0 \bmod \wp^x$.*

Proof. We will work locally at $\wp$. Since $\zeta_{2^{2+j}} \in L_j$, $\zeta_{2^{3+j}} \notin L_j$ and $(1+\zeta_{2^{2+j}})^{2^{1+j}} = (2)$ as ideals, $\pi_j = (1+\zeta_{2^{2+j}})$ is a uniformizer in the local ring with $(\pi_j) = \wp$. Now all the proposition's assumptions involving $\wp$ hold for π_j as well.

We write δ π_j-adically as $\sum_n g_n \pi_j^n$. Then we can write

$$\sum_{n=0}^{\frac{x}{2}-1} g_n^2 \pi_j^{2n} + c \sum_{n=0}^{x-1} g_n \pi_j^n + k \equiv 0 \bmod \pi_j^x.$$

Breaking the middle sum into two pieces based on the parity of the indices, we get

$$\sum_{n=0}^{\frac{x}{2}-1} g_n^2 \pi_j^{2n} + c \sum_{n=0}^{\frac{x}{2}-1} g_{2n} \pi_j^{2n} + c \sum_{n=0}^{\frac{x}{2}-1} g_{2n+1} \pi_j^{2n+1} + k \equiv 0 \bmod \pi_j^x.$$

Because L_j/L_{j-1} is ramified, we can take the g_n coefficients in the π_j-adic expansion in the localization of $\mathcal{O}_{L_j}$ to be from $\mathcal{O}_{L_{j-1}}$. Moreover $\pi_j^{2m} \equiv \pi_{j-1}^m \bmod 2$ for any $m \in \mathbb{Z}$, and the latter element is in L_{j-1}. Thus, we rewrite the congruence as

$$\sum_{n=0}^{\frac{x}{2}-1} g_n^2 \pi_{j-1}^{n} + c \sum_{n=0}^{\frac{x}{2}-1} g_{2n} \pi_{j-1}^{n} + k \equiv c \sum_{n=0}^{\frac{x}{2}-1} g_{2n+1} \pi_j^{2n+1} \bmod \pi_j^x.$$

We find that the left-hand side is a sum of terms in $\mathcal{O}_{L_{j-1}}$, so must also be in that ring. This means that it has even π_j-adic valuation. But since $c \in L_{j-1}$, it has even π_j-adic valuation. Thus, any non-zero term on the right-hand side has odd π-adic valuation. This means the right-hand side must be 0:

$$\sum_{n=0}^{\frac{x}{2}-1} g_n^2 \pi_{j-1}^{n} + c \sum_{n=0}^{\frac{x}{2}-1} g_{2n} \pi_{j-1}^{n} + k \equiv 0 \bmod \pi_j^x.$$

It also means that $g_{2n+1} = 0$ when $2n+1+v_{\pi_j}(c) < x$, so when $2n+1 < x - v_{\pi_j}(c)$. In order to get λ to behave identically to δ in the congruence, it is sufficient for δ^2 to be congruent to $\lambda^2 \bmod \pi_j^x$ and $c\lambda \equiv c\delta \bmod \pi_j^x$. For the former, it is enough for λ to match δ up to the $\frac{x}{2}$th coefficient; for the latter, it is enough for the two to match up to the $(x - v_{\pi_j}(c))$th coefficient. Since $v_{\pi_j}(c) \leq \frac{x}{2}$, satisfying the second of these also satisfies the former. We take $\lambda = \sum_{n=0}^{\frac{x-v_{\pi_j}(c)}{2}-1} g_{2n} \pi_{j-1}^n$. Then λ is in $\mathcal{O}_{L_{j-1}}$ because the g_n coefficients and π_{j-1} are both in that ring.

As we have seen, to show that λ satisfies the same congruence that δ did, it is sufficient to see that λ matches δ up to the $(x - v_{\pi_j}(c))$th coefficient. We have given λ the same coefficients for $\pi_j^{2n} \equiv \pi_{j-1}^n$ that δ has, and we have seen that the coefficient of π_j^n in the π_j-adic expansion of δ is 0 when n is odd and less than $x - v_{\pi_j}(c)$, so $\lambda \equiv \delta \bmod \pi_j^{x-v_{\pi_j}(c)}$, which is exactly what we needed. $\square$

We can use this proposition as the inductive step allowing us to move δ from anywhere in the L-tower down to any field that contains c, k, and π^x.

Corollary 3.2.8. *Let $\wp$ be a prime above 2 in L_n. Let $c, k \in \mathcal{O}_{L_j}$ with $j < n$, and let $\delta \in \mathcal{O}_{L_n}$ satisfy $\delta^2 + c\delta + k \equiv 0 \bmod \wp^x$ for some $x \in \mathbb{Z}$ with x a multiple of 2^{n-j-1}, $\wp^x$ dividing 2, and $v_\wp(c) \leq \frac{x}{2}$. Then $\exists \lambda \in \mathcal{O}_{L_{j-1}}$ such that $\lambda^2 + c\lambda + k \equiv 0 \bmod \wp^x$.*

Proof. If $n = j + 1$, this is just the statement of the previous proposition. Now assume the statement is true for some $n = N$ and take $n = N + 1$. Then a single application of the previous proposition says that $\exists \lambda \in L_N$ such that $\lambda^2 + c\lambda + k \equiv 0 \bmod \wp^x$. (Here $\wp$ is a prime above 2 in L_{N+1}.) Since x is a multiple of $2^{N+1-j-1} = 2^{N-j}$ and $N > j$, x is even, so $\wp^x$ is also a power of $\wp^2$, which is a prime above 2 in L_N. This gives us the necessary conditions to apply the induction, so the claim is true for all $j > n$. $\square$

3.2.2 Some ramified extensions

If $\gamma \equiv \alpha^4(1 + 4(1 + i)\delta + 4\delta^2) \bmod 8$, then $\frac{\gamma - \alpha^4}{4} + (1 + i)\delta + \delta^2 \equiv 0 \bmod 2$. Combining this fact with Corollary 3.2.4 and Corollary 3.2.5 gives us the following summarizing corollary:

Corollary 3.2.9. *Let $\gamma \in \mathcal{O}_{L_j}$ and let $\alpha, k \in \mathcal{O}_{L_j}$ be such that $\gamma \equiv \alpha^4 \bmod 4$ and*

$\frac{\gamma - \alpha^4}{4} = k$. *If $k^m \equiv 1$ mod 2 for some odd m, then $L_j(\gamma^{1/4})/L_j$ is ramified for all j.*

Proof. By Theorem 2.0.16 (parts 1 and 5), we know that $L_j(\gamma^{1/4})/L_j$ is ramified if there is no $\delta \in \mathcal{O}_{L_j}$ satisfying $\gamma \equiv \alpha^4(1 + 4(1+i)\delta + 4\delta^2)$ mod 8. Since $\frac{\gamma-\alpha^4}{4} = k$, this is equivalent to $0 \equiv k + (1+i)\delta + \delta^2$ mod 2. Now apply Corollary 3.2.4 and Corollary 3.2.5. $\square$

One specific application of this which arises a couple of times is the following:

Corollary 3.2.10. *Let $\gamma \in \mathcal{O}_{L_j}$ be such that $\gamma \equiv \pm 3$ mod 8. Then $L_j(\gamma^{1/4})/L_j$ is ramified for all j.*

Proof. Since unramified extensions lift to unramified extensions, it is sufficient to show this for $j \geq 1$ where we have ζ_8 available. Since $L_j(\gamma^{1/4}) = L_j((-\gamma)^{1/4})$ for $j \geq 1$, it is enough to prove the claim when $\gamma \equiv 3$ mod 8. In this case $\gamma \equiv -1 = \zeta_8^4$ mod 4. If we write $\gamma = 3 + 8l$, then, in terms of the previous corollary, we have $k = \frac{3+8l-\zeta_8^4}{4} = \frac{4+8l}{4} = 1 + 2l \equiv 1$ mod 2. The result now follows immediately from the previous corollary. $\square$

Chapter 4: Ramification Behavior of Elements of K_0

We now look at the ramification behavior of fourth roots (and square roots) of certain elements of $\mathcal{O}_{K_0}$. Specifically, we are interested in generators of principal ideals that are fourth powers. Although the tools we have detailed above are useful for all values of d, the ramification behavior still differs substantially depending on the value of d mod 8. Thus, we handle each of these cases separately. We consider only the cases where $d \equiv 1 \bmod 2$.

For each value of d mod 8, we follow the same general approach. We begin by showing congruence conditions that must be satisfied by an element that has norm ± 1 mod 16. For most values of d mod 8, we do this by thinking of the element as $a + b\sqrt{d}$ and then by showing restrictions on the possible values of a and b. Obviously, the restriction that the element of K_0 has norm ± 1 is satisfied by all units. Since the only odd fourth power in $\mathbb{Z}/16\mathbb{Z}$ is 1, it is also satisfied by any generator of a principal ideal that is a fourth power and is relatively prime to 2.

We then show the ramification behavior that results when we adjoin a square root of such an element to a field in the L-tower. Finally, we show the ramification behavior that results from adjoining a fourth root.

The case that $d \equiv 1 \bmod 8$ is, perhaps, the most straightforward. It is the first one that we examine, and we think of it as a baseline. For each of the others, we discuss what makes them different from this baseline case.

4.1 $d \equiv 1 \bmod 8$

Lemma 4.1.1. *Let $d \in \mathbb{Z}$ be congruent to 1 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be such that* $\mathrm{Norm}(\gamma) \equiv 1$ *mod 16, and write $\gamma = a + b\sqrt{d}$ with $a, b \in \frac{1}{2}\mathbb{Z}$. Then $a, b \in \mathbb{Z}$ with $a \equiv \pm 1$ mod 8 and $b \equiv 0$ mod 4.*

Proof. First, we write $a = \frac{a_1}{2}$ and $b = \frac{b_1}{2}$ with $a_1, b_1 \in \mathbb{Z}$. Then we can rewrite the norm calculation ($a^2 - db^2 \equiv 1 \bmod 16$) as $a_1^2 - db_1^2 \equiv 4 \bmod 64$. Since $d \equiv 1 \bmod 8$, this gives us $a_1^2 - b_1^2 \equiv 4 \bmod 8$. The only squares mod 8 in $\mathbb{Z}$ are 0, 1, and 4, so the only possible choices for a_1^2 and b_1^2 are 0 and 4 in some order. This means that both a_1 and b_1 are even, so $a, b \in \mathbb{Z}$.

Now we have $a^2 - db^2 \equiv 1 \bmod 16$. Since $d \equiv 1 \bmod 8$, this is $a^2 - b^2 \equiv 1 \bmod 8$. Because the only squares mod 8 are 0, 1, and 4, we must have $a^2 \equiv 1 \bmod 8$ and $b^2 \equiv 0 \bmod 8$. The latter fact means that $b \equiv 0 \bmod 4$, which, in turn, implies that $b^2 \equiv 0 \bmod 16$. This means that $db^2 \equiv 0 \bmod 16$, so we can write the norm calculation as $a^2 \equiv 1 \bmod 16$. This forces $a \equiv \pm 1 \bmod 8$. □

Lemma 4.1.2. *Let $d \in \mathbb{Z}$ be congruent to 1 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be such that* $\mathrm{Norm}(\gamma) \equiv -1$ *mod 8 and write $\gamma = a + b\sqrt{d}$ with $a, b \in \frac{1}{2}\mathbb{Z}$. Then $a, b \in \mathbb{Z}$ with $a \equiv 0$ mod 4 and $b \equiv 1$ mod 2. Moreover, if* $\mathrm{Norm}(\gamma) = -1$*, then $b \equiv 1$ mod 4.*

Proof. The argument to show that $a, b \in \mathbb{Z}$ is essentially identical to that used in Lemma 4.1.1. We begin by writing $a = \frac{a_1}{2}$ and $b = \frac{b_1}{2}$ with $a_1, b_1 \in \mathbb{Z}$. Then we can rewrite the norm calculation as $a_1^2 - db_1^2 \equiv -4 \bmod 64$. Since $d \equiv 1 \bmod 8$, this gives us $a_1^2 - b_1^2 \equiv 4 \bmod 8$. The only squares mod 8 in $\mathbb{Z}$ are 0, 1, and 4, so the only possible choices for a_1^2 and b_1^2 are 0 and 4 in some order. This means that both a_1 and b_1 are even, so $a, b \in \mathbb{Z}$.

Now we have $a^2 - b^2 \equiv -1 \bmod 8$. Because the only squares mod 8 are 0, 1, and 4, we must have $a^2 \equiv 0 \bmod 8$ and $b^2 \equiv 1 \bmod 8$. This means that a must be 0 mod 4 and that b must be odd.

Now consider the case that $a^2 - db^2 = -1$. In this case, -1 is a quadratic residue mod b. This means that $b \equiv 1 \bmod 4$. □

In the next couple of results, we take advantage of the fact that if $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$, then $\mathrm{Norm}(\gamma) \equiv \pm 1 \bmod 16$ because 1 is the only fourth power mod 16 in $\mathbb{Z}$ that is relatively prime to 2. This fact lets us apply the previous lemmas to γ when we have $(\gamma) = I^4$ rather than an explicit condition on the norm.

Now we begin by establishing that under these conditions $L_j(\gamma^{1/2})/L_j$ is always unramified.

Proposition 4.1.3. *Let d be 1 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. Then $L_j(\gamma^{1/2})/L_j$ is an unramified extension for all j.*

Proof. To show that this extension is unramified, we can show that γ is a square mod 4 in L_0 and apply Proposition 2.0.8.

By Lemma 4.1.1 and Lemma 4.1.2, we see that γ is $\pm 1 \bmod 4$ or $\pm\sqrt{d} \bmod 4$. Clearly, 1 is a square. Since $i \in L_0$, -1 is also a square. Since $d \equiv 1 \bmod 8$, we have $\sqrt{d} \equiv \pm 1 \bmod 4$, so γ is either 1 or $-1 \bmod 4$, depending on the choice of prime over 2 at which we complete. (Note that (2) is split in this case.) Since γ is a square mod 4 in each completion $\gamma^{1/2}$ gives an unramified extension at both completions, so also gives one in the global case.

Since $L_0(\gamma^{1/2})/L_0$ is an unramified extension and unramified extensions lift to unramified extensions, $L_j(\gamma^{1/2})/L_j$ is an unramified extension for all j. (In fact, since L_{j+1}/L_j is ramified above 2 for all j, this lift can never be absorbed, so L_{j+1}/L_j has the same degree as $L_0(\gamma^{1/2})/L_0$. Later in the paper we explore this further.) $\square$

We can now address what happens when we adjoin a fourth root of such a γ to L_j. Note that we use the results in Lemma 4.1.1 and Lemma 4.1.2 to be able to take $a, b \in \mathbb{Z}$ in the statement of the following theorem.

Theorem 4.1.4. *Let $d \in \mathbb{Z}$ be congruent to 1 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$, and write $\gamma = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Then for $j > 0$, $L_j(\gamma^{1/4})/L_j$ is unramified iff $a \equiv 0$ mod 8 or $b \equiv 0$ mod 8. Moreover, $L_0(\gamma^{1/4})/L_0$ is unramified iff $a \equiv 1$ mod 8 and $b \equiv 0$ mod 8.*

When the extensions are ramified, they are ramified at both primes above (2) unless $a \equiv 0$ mod 8, in which case they are ramified at exactly one of the two primes above (2).

Proof. Our previous lemmas Lemma 4.1.1 and Lemma 4.1.2 tell us that it is equivalent to show that exactly one of the following is true:

- $a \equiv 1 \bmod 8$, $b \equiv 0 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is unramified for all j
- $a \equiv -1 \bmod 8$, $b \equiv 0 \bmod 8$, $L_0(\gamma^{1/4})/L_0$ is ramified at both primes above

(2), and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$

- $a \equiv 1 \bmod 8$, $b \equiv 4 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified at both primes above (2) for all j
- $a \equiv -1 \bmod 8$, $b \equiv 4 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified at both primes above (2) for all j
- $a \equiv 4 \bmod 8$, $b \equiv 1 \bmod 2$, and $L_j(\gamma^{1/4})/L_j$ is ramified at both primes above (2) for all j
- $a \equiv 0 \bmod 8$, $b \equiv 1 \bmod 2$, $L_0(\gamma^{1/4})/L_0$ is ramified at exactly one of the two primes above (2), and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j > 0$.

The first and second cases are proven by Lemma 3.1.1 and Lemma 3.1.3, respectively.

Since $d \equiv 1 \bmod 8$, $\sqrt{d} \equiv \pm 1 \bmod 4$, so $\sqrt{d} \equiv 1 \bmod 2$. This means that $4\sqrt{d} \equiv 4 \bmod 8$. Thus, in the next two cases, we have $\gamma \equiv \pm 5 \bmod 8$, depending on the choice of completion. That this results in ramified extensions was proved in Corollary 3.2.10. Since the result is true for both completions, we have ramification at both primes above (2).

In the final two cases, we have $a \equiv 0 \bmod 4$, so $a^2 \equiv 0 \bmod 16$. Since we have assumed that $a^2 - db^2 \equiv \pm 1 \bmod 16$, this gives us $db^2 \equiv \pm 1 \bmod 16$. Recall that a was even only when the norm was $-1 \bmod 16$. This means we actually have $a^2 - db^2 \equiv -1 \bmod 16$, so $db^2 \equiv 1 \bmod 16$.

Since $db^2 \equiv 1 \bmod 16$, we know that $b\sqrt{d} \equiv \pm 1 \bmod 8$. Now we can examine the final two congruence possibilities for a and b. If a is 4 mod 8, then $\gamma = a + b\sqrt{d}$ is $\pm 5 \bmod 8$. Again, we work locally, apply Corollary 3.2.10 to see that the extensions must be ramified in the local case, and then use the fact that the extension is ramified at a prime iff it is ramified in the completion at that prime.

If a is 0 mod 8, then $\gamma = a + b\sqrt{d}$ is ± 1 mod 8. Note that whether γ is 1 mod 8 or -1 mod 8 depends on the choice of completion. Using Lemma 3.1.1 and Lemma 3.1.3, we find that at L_0, the extension is unramified in one completion, but ramified in the other, so the extension ramifies at exactly one of the prime above (2). The same lemmas show that $L_j(\gamma^{1/4})/L_j$ is unramified for $j > 0$. □

4.2 $d \equiv 3 \bmod 8$

When $d \equiv 1 \bmod 8$, $\sqrt{d}$ is always congruent to an integer mod 8 because d has a square root in the 2-adics. When $d \equiv 3 \bmod 8$, this is no longer true. In this case, we have $\sqrt{d} \equiv \pm i(2\zeta_3 + 1) \bmod 4$ if we are in a field that has i and the cube roots of unity. Since we are always looking at extensions of the L-tower, we can think of this congruence as a congruence in $\mathcal{O}_{L_0}$, where we have i available. Note that we do not have ζ_3 in the L-tower, but we can get arbitrarily close to ζ_3 2-adically. When we need to work with this form, we can choose some element sufficiently close to ζ_3. We will abuse notation and call that element ζ_3.

Working with the γs, then, requires working with elements of the form $x + yi(2\zeta_3 + 1)$. This turns out to be somewhat more complicated. These extra complications do not arise until we try to understand the ramification behavior of $L_j(\gamma^{1/4})/L_j$, so as with $d \equiv 1 \bmod 8$, we begin by establishing the possibilities for γ mod 8 and understanding the ramification behavior of $L_j(\gamma^{1/2})/L_j$.

Lemma 4.2.1. *Let $d \in \mathbb{Z}$ be congruent to 3 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be such that* $\mathrm{Norm}(\gamma) \equiv \pm 1$ *mod 16, and write $\gamma = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Then one of the following is true:*

- $a \equiv 2$ *mod 4 and* $b \equiv 1$ *mod 2*
- $a \equiv \pm 1$ *mod 8 and* $b \equiv 0$ *mod 4.*

Proof. The norm of γ to $\mathbb{Q}$ is $a^2 - db^2 \equiv a^2 - 3b^2$ mod 8, and this must be congruent to ± 1. Because the only squares mod 8 are 0, 1, and 4, we must have $a^2 \in \{0, 1, 4\}$ and $3b^2 \in \{0, 3, 4\}$. So the only possibilities for $[a^2, 3b^2]$ are $[1, 0]$ and $[4, 3]$. (Note that in both cases, the norm is 1 mod 16.) This gives us that either a is odd and b is 0 mod 4, or a is 2 mod 4 and b is odd.

If $b \equiv 0$ mod 4, then looking at the congruence mod 16, we get $a^2 \equiv 1$ mod 16, so $a \equiv \pm 1$ mod 8. □

Again, we take advantage of the fact that taking $(\gamma) = I^4$ is sufficient for forcing $\mathrm{Norm}(\gamma) \equiv \pm 1$ mod 16.

When d was 1 mod 8, Proposition 4.1.3 tells us that $L_j(\gamma^{1/2})/L_j$ is always unramified. When d is 3 mod 8, the situation is not quite as simple.

Proposition 4.2.2. *Let d be 3 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. Then $L_0(\gamma^{1/2})/L_0$ is unramified iff $a \equiv 1$ mod 2. Moreover, in all cases $L_j(\gamma^{1/2})/L_j$ is an unramified extension for $j \geq 1$.*

Proof. It is sufficient to show that $L_0(\gamma^{1/2})/L_0$ and $L_1(\gamma^{1/2})/L_1$ are unramified under the claimed conditions.

Proposition 2.0.8 tells us that, to show these extensions are unramified, it is equivalent to show that γ is a square mod 4 in the field being extended. By Lemma 4.2.1, we know that mod 4, γ is $1, -1, 2+\sqrt{d}$, or $2+3\sqrt{d} = -(2+\sqrt{d})$. Our claim that $L_0(\gamma^{1/2})/L_0$ is unramified iff $a \equiv 1 \bmod 2$ is now equivalent to the claim that 1 and -1 are both squares mod 4 in L_0 and that $2 \pm \sqrt{d}$ is not. That 1 and -1 are squares is clear since both 1 and i are in L_0. If $2 \pm \sqrt{d}$ is a square mod 4, it is also one mod 2. This would mean that $\sqrt{d}$ is a square mod 2. Since $d \equiv -1$ mod 4, we have $(\sqrt{d}+i)(\sqrt{d}-i) \equiv 0 \bmod 4$. At least one of the two factors must be divisible by 2 and since their difference is $2i$, both are. So we have $\sqrt{d} \equiv i$ mod 2. This means that if $2 \pm \sqrt{d}$ were a square mod 2, then i would be a square mod 2. We would need only to define its square root mod $1+i$, and the only such value in L_0 is 1, which does not square to i mod 2. So $2 \pm \sqrt{d}$ is not a square mod 4 in L_0.

To prove our claim for L_1, we need to see that ± 1 and $2 \pm \sqrt{d}$ are squares mod 4 in L_1. Again, this is clearly true for ± 1. Since $2 - \sqrt{d} = -(2+\sqrt{d})$ and -1 is a square, it is sufficient to show that $2+\sqrt{d}$ is a square mod 4 in L_1. Note that $\frac{1+d}{2} \equiv 2 \bmod 4$ because $1 + d \equiv 4 \bmod 8$. Thus, we need only to note that $(\frac{1}{\sqrt{2}}(1+\sqrt{d}))^2 = \frac{1}{2}(1+d+2\sqrt{d}) = \frac{1+d}{2} + \sqrt{d}$ is a square in L_1. □

Theorem 4.2.3. *Let $d \in \mathbb{Z}$ be congruent to 3 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$, and write $\gamma = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Then for $j > 0$, $L_j(\gamma^{1/4})/L_j$ is unramified iff a is odd. Moreover, $L_0(\gamma^{1/4})/L_0$ is unramified iff $a \equiv 1$ mod 8.*

Proof. With Lemma 4.2.1, we see that this is equivalent to showing that exactly one of the following is true:

- $a \equiv 1 \bmod 8$, $b \equiv 0 \bmod 4$, and $L_j(\gamma^{1/4})/L_j$ is unramified for all j
- $a \equiv -1 \bmod 8$, $b \equiv 0 \bmod 4$, $L_0(\gamma^{1/4})/L_0$ is ramified, and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$
- $a \equiv 2 \bmod 4$, $b \equiv 1 \bmod 2$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j.

Since $\sqrt{3} = -i(2\zeta_3 + 1)$ and $d \equiv 3 \bmod 8$, we have $\sqrt{d} \equiv \pm i(2\zeta_3 + 1) \bmod 4$. This means that in the first two cases, we have $\gamma \equiv \pm 1 \bmod 8$ or $\gamma \equiv \pm 1 + 4i(2\zeta_3 + 1) \equiv \pm 1 + 4i \bmod 8$. Then for these two cases, the claims follow directly from Lemma 3.1.4 and Lemma 3.1.5.

The third case is more complicated. Note that this can be broken into 8 cases for $a + b\sqrt{d}$, based on the two choices for a mod 8 and the four choices for b mod 8. Moreover, note that if $d \equiv 3 \bmod 16$, then $\sqrt{d} \equiv \pm\sqrt{3} \bmod 8$. If $d \equiv 11 \equiv 27 \bmod 16$, then $\sqrt{d} \equiv \pm 3\sqrt{3} \bmod 8$. This means that the 8 possibilities for $a + b\sqrt{d}$ with $a \equiv 2 \bmod 4$ and $b \equiv 1 \bmod 2$, cover the cases for either congruence condition on d mod 16. We find it convenient to write $\sqrt{3}$ as $i(2\zeta_3 + 1)$, so our 8 cases become $x + yi(2\zeta_3 + 1)$. (Recall that by ζ_3, we mean an element that is congruent to a primitive cube root of unity mod a high power of 2.)

These 8 cases can be grouped into 4 pairs: $\pm(2 + i(2\zeta_3 + 1))$, $\pm(2 + 5i(2\zeta_3 + 1))$, $\pm(2 + 3i(2\zeta_3 + 1))$, and $\pm(2 + 7i(2\zeta_3 + 1))$. Since $\zeta_8 \in L_1$, adjoining the fourth root of one member of a pair to L_j is the same as adjoining the other member as long as $j \geq 1$. This means that if we can show that adjoining the fourth root of one member to L_j gives a ramified extension for all j, that would imply the same for the other member of the pair when $j \geq 1$. Since unramified extensions lift to unramified extensions, that would also force ramified extensions of L_0. In fact, we find it convenient to work in L_j with $j \geq 2$, where ζ_{16} is available and use the fact that unramified extensions lift to unramified extensions to obtain the result for L_0 and L_1.

We work with $2+2i\zeta_3+i$, $2+10i\zeta_3+5i \equiv 2+2i\zeta_3+5i$, $-(2+6i\zeta_3+3i) \equiv 6+2i\zeta_3+5i$, and $-(2+14i\zeta_3+7i) \equiv 6+2i\zeta_3+i$. Note that each of these is congruent to $2+2i\zeta_3+i \bmod 4$, so we can use the same α for all of them.

We claim that we can take $\alpha = \zeta_{48}^{19}+\zeta_{48}^{-19}$. For the purposes of doing arithmetic on these roots of unity, we mention that we choose an element to be ζ_{48} and then define $\zeta_m = \zeta_{48}^{\frac{48}{m}}$. To see that we can take $\alpha = \zeta_{48}^{19}+\zeta_{48}^{-19}$, note that

$$\begin{aligned} \alpha^4 &= \zeta_{12}^{7} + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7} \\ &\equiv \zeta_{12}^{7} + 2 + \zeta_{12}^{-7} \bmod 4. \end{aligned}$$

To show that $\alpha^4 \equiv \gamma \bmod 4$, we must show that $\zeta_{12}^{7}+\zeta_{12}^{-7} \equiv 2i\zeta_3+i = 2\zeta_{12}^{3}\zeta_{12}^{4}+\zeta_{12}^{3} \bmod 4$. Subtracting ζ_{12}^{7} from both sides, we find that this reduces to showing that $\zeta_{12}^{-7} \equiv \zeta_{12}^{7}+\zeta_{12}^{3} \bmod 4$. In fact, the two sides are equal, which can be seen by multiplying both sides by ζ_{12}: $\zeta_{12}^{-6} = \zeta_{12}^{8}+\zeta_{12}^{4}$. This can be rewritten as $-1 = \zeta_3^2+\zeta_3$, which is true.

With α established, we first consider the case that $\gamma \equiv 2+2i\zeta_3+i \bmod 8$. By Theorem 2.0.16, $L_j(\gamma^{1/4})/L_j$ is unramified iff $\exists \delta \in L_j$ satisfying

$$\begin{aligned} 2+2i\zeta_3+i &\equiv (\zeta_{12}^{7} + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7})(1+4(1+i)\delta+4\delta^2) \\ &\equiv (\zeta_{12}^{7} + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7}) + \\ &\qquad (\zeta_{12}^{7} + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7})(4(1+i)\delta+4\delta^2) \bmod 8. \end{aligned}$$

We saw above that $\zeta_{12}^{7}+\zeta_{12}^{-7} = 2i\zeta_3+i$, so we can subtract $2+\zeta_{12}^{7}+\zeta_{12}^{-7}$ from both sides to get

$$0 \equiv (4\zeta_{24}^{19} + 4 + 4\zeta_{24}^{-19}) + (\zeta_{12}^{7} + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7})(4(1+i)\delta + 4\delta^2) \bmod 8.$$

Dividing through by 4, we get an equivalent congruence mod 2:

$$\begin{aligned} 0 &\equiv (\zeta_{24}^{19} + 1 + \zeta_{24}^{-19}) + (\zeta_{12}^{7} + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7})((1+i)\delta + \delta^2) \\ &\equiv (\zeta_{24}^{19} + 1 + \zeta_{24}^{-19}) + (\zeta_{12}^{7} + \zeta_{12}^{-7})((1+i)\delta + \delta^2) \\ &\equiv (\zeta_{24}^{19} + 1 + \zeta_{24}^{-19}) + (2i\zeta_3 + i)((1+i)\delta + \delta^2) \\ &\equiv (\zeta_{24}^{19} + 1 + \zeta_{24}^{-19}) + i((1+i)\delta + \delta^2) \\ &\equiv (\zeta_{24}^{19} + 1 + \zeta_{24}^{-19}) + (1+i)\delta + i\delta^2 \bmod 2. \end{aligned}$$

We can multiply both sides by $i = \zeta_{24}^{6}$ to get

$$0 \equiv (\zeta_{24} + i + \zeta_{24}^{-13}) + (1+i)\delta + \delta^2 \bmod 2.$$

But $\zeta_{24}^{-12} = -1 \equiv 1 \bmod 2$, so this is

$$0 \equiv (\zeta_{24} + i + \zeta_{24}^{-1}) + (1+i)\delta + \delta^2 \bmod 2.$$

At this point, it would be nice to appeal directly to Corollary 3.2.6, but we are not able to do so because in the terms of our proposition, we would have $n = 4$, so $N = 2$. But then k is not in $L_{N-3} = L_{-1} = \mathbb{Q}$. Note, however, that $(\zeta_{24} + i + \zeta_{24}^{-1}) \equiv \zeta_8(1+\zeta_8)(1+\zeta_{24}^{16}+\zeta_{24}^{19}) \bmod 2$, so is divisible by $(1+\zeta_8)$. Reducing mod $(1+i)$ gives us

$$\delta^2 \equiv \zeta_8(1+\zeta_8)(1+\zeta_{24}^{16}+\zeta_{24}^{19}) \bmod 1+i.$$

In particular, δ^2 must be divisible by $1+\zeta_8$, so δ must be divisible by $1+\zeta_{16}$. If we let $\kappa = \delta/(1+\zeta_{16})$, we can rewrite our congruence as

$$0 \equiv \zeta_8(1+\zeta_8)(1+\zeta_{24}^{16}+\zeta_{24}^{19}) + (1+i)(1+\zeta_{16})\kappa + (1+\zeta_{16})^2\kappa^2 \bmod 2.$$

Dividing through by $(1+\zeta_{16})^2 \equiv (1+\zeta_8)$ gives the equivalent

$$0 \equiv \zeta_8(1+\zeta_{24}^{16}+\zeta_{24}^{19}) + (1+\zeta_8)(1+\zeta_{16})\kappa + \kappa^2 \bmod (1+i)(1+\zeta_8).$$

We can rewrite this as

$$0 \equiv \zeta_8(1+\zeta_{24}^{16}+\zeta_{24}^{19}) + (1+\zeta_{16})^3\kappa + \kappa^2 \bmod (1+\zeta_{16})^6.$$

Now we claim we can invoke Corollary 3.2.6. This time, we have $n = 16$, so $N = 4$. Our constant $k = \zeta_8(1+\zeta_{24}^{16}+\zeta_{24}^{19}) = \zeta_8(1+\zeta_3^2+\zeta_8\zeta_3^2)$ is a finite sum of roots of unity in L_1 because L_1 has ζ_8 and also has ζ_3 mod 2. Moreover, k is relatively prime to 2 because we have

$$\begin{aligned} k &= \zeta_8(1+\zeta_{24}^{16}+\zeta_{24}^{19}) \\ &= \zeta_8(1+\zeta_3^2+\zeta_{24}^3\zeta_3^2) \\ &= \zeta_8(1+\zeta_3^2+\zeta_8\zeta_3^2) \\ &\equiv 1+2\zeta_3^2 \\ &\equiv 1 \bmod 1+\zeta_8. \end{aligned}$$

This means that $v(k) = 0 < \frac{3}{8} = z2^{1-N}$ and $v(v(k)) = \infty > 2-N = -2$. All of the conditions for the corollary are satisfied, so $\delta \notin L_j$ for any j. This means that $L_j(\gamma^{1/4})/L_j$ is ramified for all j.

Now we consider the second case, where $\gamma \equiv 2 + 2i\zeta_3 + 5i \bmod 8$. This time $L_j(\gamma^{1/4})/L_j$ is unramified iff $\exists \delta \in L_j$ satisfying

$$2 + 2i\zeta_3 + 5i \equiv (\zeta_{12}^7 + 4\zeta_{24}^{19} + 6 + 4\zeta_{24}^{-19} + \zeta_{12}^{-7})(1 + 4(1+i)\delta + 4\delta^2) \bmod 8.$$

We can perform the same manipulation on this congruence that we did in the first case and get a similar congruence. This time we are starting with an extra $4i$ and all of the manipulations in the first case were subtracting things from both sides, dividing through by 4, and multiplying both sides by $\zeta_{24}^6 = i$. So we end up with the same congruence, except with an additional term of $-1 \equiv 1$:

$$0 \equiv (1 + \zeta_{24} + i + \zeta_{24}^{-1}) + (1+i)\delta + \delta^2 \bmod 2.$$

Note that $\delta^2 \equiv \zeta_{24} + \zeta_{24}^{-1} \bmod 1+i$. Thus, $\delta \equiv \zeta_{48} + \zeta_{48}^{-1} \bmod 1+\zeta_8$. Write $\delta = \zeta_{48} + \zeta_{48}^{-1} + \kappa(1+\zeta_8)$ and substitute this back in to get

$$\begin{aligned} 0 &\equiv (1 + i + \zeta_{24} + \zeta_{24}^{-1}) + (1+i)(\zeta_{48} + \zeta_{48}^{-1}) + \kappa(1+i)(1+\zeta_8) + \\ &\qquad \zeta_{24} + \zeta_{24}^{-1} + \kappa^2(1+i) \\ &\equiv (1+i) + (1+i)(\zeta_{48} + \zeta_{48}^{-1}) + \kappa(1+i)(1+\zeta_8) + \kappa^2(1+i) \bmod 2. \end{aligned}$$

We divide through by $(1+i)$ to get

$$0 \equiv 1 + \zeta_{48} + \zeta_{48}^{-1} + \kappa(1+\zeta_8) + \kappa^2 \bmod (1+i).$$

Since

$$\begin{aligned}
1+\zeta_{48}+\zeta_{48}^{-1} &= 1+\zeta_3\zeta_{16}^{11}+\zeta_3^2\zeta_{16}^5 \\
&= -(1-\zeta_{16})(\zeta_3(1+\zeta_{16}+\zeta_{16}^2+\cdots+\zeta_{16}^{10})+ \\
&\qquad \zeta_3^2(1+\zeta_{16}+\zeta_{16}^2+\zeta_{16}^3+\zeta_{16}^4)) \\
&\equiv (1+\zeta_{16})(\zeta_3(1+\zeta_{16}+\zeta_{16}^2+\cdots+\zeta_{16}^{10})+ \\
&\qquad \zeta_3^2(1+\zeta_{16}+\zeta_{16}^2+\zeta_{16}^3+\zeta_{16}^4)) \bmod 2,
\end{aligned}$$

we know that $\kappa^2 \equiv 0 \bmod (1+\zeta_{16})$, so $\kappa \equiv 0 \bmod (1+\zeta_{32})$. We can replace κ with $(1+\zeta_{32})\lambda$ to get

$$0 \equiv 1+\zeta_{48}+\zeta_{48}^{-1}+\lambda(1+\zeta_{32})(1+\zeta_8)+\lambda^2(1+\zeta_{16}) \bmod (1+i).$$

Now we can divide by $(1+\zeta_{16})$ to get a congruence mod $(1+\zeta_{32})^6$:

$$\begin{aligned}
0 &\equiv \zeta_3(1+\zeta_{16}+\zeta_{16}^2+\cdots+\zeta_{16}^{10})+\zeta_3^2(1+\zeta_{16}+\zeta_{16}^2+\zeta_{16}^3+\zeta_{16}^4))+ \\
&\qquad \lambda(1+\zeta_{32})(1+\zeta_{16})+\lambda^2 \\
&= \zeta_3(1+\zeta_{16}+\zeta_{16}^2+\cdots+\zeta_{16}^{10})+\zeta_3^2(1+\zeta_{16}+\zeta_{16}^2+\zeta_{16}^3+\zeta_{16}^4))+ \\
&\qquad \lambda(1+\zeta_{32})^3+\lambda^2.
\end{aligned}$$

Now we again invoke our corollary. This time, we have $n = 32$, so $N = 5$. The constant term $k = \zeta_3(1+\zeta_{16}+\zeta_{16}^2+\cdots+\zeta_{16}^{10})+\zeta_3^2(1+\zeta_{16}+\zeta_{16}^2+\zeta_{16}^3+\zeta_{16}^4))$ is a finite sum of roots of unity in L_2. Also, looking at it mod $1+\zeta_{16}$, we find that $k \equiv 11\zeta_3+5\zeta_3^2 \equiv \zeta_3+\zeta_3^2 \equiv 1$, so k is again relatively prime to 2. As before, this ensures the conditions on the valuation of k are satisfied, so again $\delta \notin L_j$.

For the third case, we have $\gamma \equiv 6+2i\zeta_3+5i \bmod 8$. This time, we are starting with an extra $4i+4$ relative to the first case. This means that after the manipulations we have added an $i+1$ to the congruence that needed to be satisfied in the first case. This yields the following congruence:

$$0 \equiv (\zeta_{24} + 1 + \zeta_{24}^{-1}) + (1+i)\delta + \delta^2 \bmod 2.$$

We can avoid going through the rest of the manipulations. Note that $0 \equiv k+(1+i)\delta+\delta^2 \bmod 2$ has a solution iff $(k+i)+(1+i)\gamma+\gamma^2 \bmod 2$ does. To see this, let $\gamma = \delta+1$, and the second congruence becomes $(k+i)+(1+i)+(1+i)\delta+\delta^2+2\delta+1 \equiv k+(1+i)\delta+\delta^2 \bmod 2$. This proves one direction, but since we are working mod 2, applying the same argument works for the other direction.

In our second case, we already saw that there is no solution for

$$0 \equiv (1 + \zeta_{24} + i + \zeta_{24}^{-1}) + (1+i)\delta + \delta^2 \bmod 2.$$

Applying the argument from the previous paragraph immediately gives us that there is no solution in this third case either.

Finally, we treat the fourth case: $\gamma \equiv -(2 + 6i\zeta_3 + 7i) \bmod 8$. This time, we are starting with an extra 4 relative to the first case, so after the manipulations we have added an i to the congruence that needed to be satisfied in the first case. We then have the following congruence:

$$0 \equiv (\zeta_{24} + \zeta_{24}^{-1}) + (1+i)\delta + \delta^2 \bmod 2.$$

The same trick that we used in the third case works just as well in this case. The only difference is that we are basing our result here on the result from the first case rather than the result from the second case. $\square$

4.3 $d \equiv 5 \bmod 8$

In the case that $d \equiv 5 \bmod 8$, we again have $\zeta_3 \bmod 8$ present. Unlike in the $d \equiv 3 \bmod 8$ case, in this case we find it more convenient to look at $\gamma \bmod 8$ in terms of ζ_3 rather than in terms of $\sqrt{d}$. Again, we will abuse notation and write ζ_3 when we mean some element of L_j that is sufficiently close to ζ_3 2-adically.

There are a couple of reasons that we prefer to look at γ in terms of ζ_3. First, since $d \equiv 1 \bmod 4$, if we write $a + b\sqrt{d}$, then we have to take $a, b \in \frac{1}{2}\mathbb{Z}$ rather than in $\mathbb{Z}$. When we took $d \equiv 1 \bmod 8$, the norm condition forced $a, b \in \mathbb{Z}$, but this does not happen when $d \equiv 5 \bmod 8$. Another, perhaps more subtle, reason can be seen by considering the following two cases:

- $d = 77$, $\varepsilon_0 = \frac{9}{2} + \frac{1}{2}\sqrt{d}$
- $d = 85$, $\varepsilon_0 = \frac{9}{2} + \frac{1}{2}\sqrt{d}$.

If we look at ε_0 as $a + b\sqrt{d}$ and try to determine the ramification behavior solely by looking at conditions on a and b, as we have done for $d \in \{1, 3\} \bmod 8$, we are bound to fail: these two examples have the same a and b, but have different ramification behavior. It turns out that when we write these two in terms of ζ_3, we have $\varepsilon_0 \equiv 1 + \zeta_3 \bmod 8$ for $d = 77$ and $\varepsilon_0 \equiv 7 + 5\zeta_3 \bmod 8$ for $d = 85$. We see in this section that this means that $L_1(\varepsilon_0^{1/4})/L_1$ is unramified when $d = 77$, but is ramified when $d = 85$.

We begin the section by looking at the relationship between the representation in terms of $\sqrt{d}$ and the representation in terms of ζ_3.

Since $-3d^{-1} \equiv 1 \bmod 8$, it has a square root mod 64 in $\mathbb{Z}$. In fact, it has two:

one that is 1 mod 4 and one that is -1 mod 4. Let k be the square root that is 1 mod 4. We think of $\frac{-1+k\sqrt{d}}{2}$ as ζ_3. This will not cause any problems because we will be working mod 8, and the only properties of ζ_3 we will use are the fact that its cube is 1 and the fact that $\zeta_3^2 + \zeta_3 + 1 = 0$. The former is implied by the latter, and the following calculation shows the latter is true mod 8:

$$\begin{aligned}
\left(\frac{-1+k\sqrt{d}}{2}\right)^2 + \left(\frac{-1+k\sqrt{d}}{2}\right) + 1 &= \frac{1+dk^2-2k\sqrt{d}}{4} + \frac{-1+k\sqrt{d}}{2} + 1 \\
&= \frac{1+dk^2}{4} + \frac{-1}{2} + 1 \\
&= \frac{dk^2-1}{4} + 1 \\
&= 0.
\end{aligned}$$

The last line follows because we have chosen k such that $k^2 \equiv -3d^{-1}$ mod 64, so $dk^2 \equiv -3$.

In this conversion from writing in terms of $\sqrt{d}$ to writing in terms of ζ_3, it is important to note that, when taking $\sqrt{d}$ to be positive or negative, we are also choosing a value for our ζ_3. (This determines whether our ζ_3 is congruent to $e^{\frac{2\pi i}{3}}$ or $e^{\frac{-2\pi i}{3}}$. The behavior of the two is the same, so which we choose does not matter.)

To make our final notation a little cleaner, we will take $c = k^{-1}$. If we write

$\gamma = \frac{a+b\sqrt{d}}{2}$ with $a, b \in \mathbb{Z}$, then we have

$$\begin{aligned}
\gamma &= \frac{a+b\sqrt{d}}{2} \\
&= \frac{a+bck\sqrt{d}}{2} \\
&= \frac{a+bc-bc+bck\sqrt{d}}{2} \\
&= \frac{a+bc}{2} + bc\frac{-1+k\sqrt{d}}{2} \\
&\equiv \frac{a+bc}{2} + bc\zeta_3 \bmod 8.
\end{aligned}$$

Since a and b have the same parity, and c is odd, we know that $a+bc$ is even. Thus, we can write $\gamma \equiv x + y\zeta_3 \bmod 8$ with $x, y \in \mathbb{Z}$. To be explicit, the conversion is that $x \equiv \frac{a+bc}{2} \bmod 8$ and $y \equiv bc \bmod 8$. Note that since $c \equiv 1 \bmod 4$, y has the same parity as a and b (which must have the same parity as each other because the ring of integers of K_0 is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$).

It is also useful to be able to convert from x and y to a and b. Since $c \equiv 1 \bmod 4$, we can write $y \equiv bc \equiv b \bmod 4$. Since $x \equiv \frac{a+bc}{2} \bmod 8$, we can multiply by 2 to get $2x \equiv a + bc \bmod 16$. We already know that $y \equiv bc \bmod 8$, so this gives us $a \equiv 2x - y \bmod 8$.

Lemma 4.3.1. *Let $d \in \mathbb{Z}$ be congruent to 5 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be such that $\mathrm{Norm}(\gamma) \equiv \pm 1$ mod 8, and let $\gamma \equiv x + y\zeta_3$ with $x, y \in \mathbb{Z}$. Then exactly one of the following is true:*

1. *$x \equiv 0$ mod 8 and $y \equiv 1$ mod 2*
2. *$x \equiv 1$ mod 2 and $y \equiv 0$ mod 8*
3. *$x \equiv 1$ mod 2 and $y \equiv x$ mod 8*
4. *$x \equiv 1$ mod 2 and $y \equiv 6x$ mod 8*

5. *$x \equiv 6y$ mod 8 and $y \equiv 1$ mod 2*

6. *$x \equiv 1$ mod 2 and $y \equiv 3x$ mod 8.*

Moreover, if $\text{Norm}(\gamma) = \pm 1$*, then we have the following additional restrictions:*

- *if $y \equiv 2$ mod 4, then $y \equiv 2$ mod 8*
- *if $x \equiv 1$ mod 4 and $y \equiv 1$ mod 2, then $y \equiv x$ mod 8*
- *if $x \equiv 2$ mod 4, then $x \equiv 6$ mod 8.*

Proof. Our restrictions on x and y all follow from the norm calculation: $(x+y\zeta_3)(x+y\zeta_3^2) \equiv \pm 1 \bmod 8$. This gives us $x^2 + xy\zeta_3 + xy\zeta_3^2 + y^2 \equiv \pm 1 \bmod 8$. Because $1 + \zeta_3 + \zeta_3^2 = 0$, we can write this more simply as $x^2 - xy + y^2 \equiv \pm 1 \bmod 8$.

First consider the case that y is even. In this case, we must have x odd because otherwise the norm would be even rather than ± 1. With x odd, the norm calculation gives us $\pm 1 \equiv x^2 - xy + y^2 \equiv 1 - xy + y^2 \bmod 8$.

If $y \equiv 0 \bmod 4$, then we have $\pm 1 \equiv 1 - xy \bmod 8$. Also, with $y \equiv 0 \bmod 4$ and x odd, $xy \equiv y \bmod 8$, so we actually have $\pm 1 \equiv 1 - y \bmod 8$. The forces y to be 0 mod 8. So in this case, we have $x \equiv 1 \bmod 2$ and $y \equiv 0 \bmod 8$. This establishes possibility 2.

If $y \equiv 2 \bmod 8$, then we have $y^2 \equiv 4 \bmod 8$, so $\pm 1 \equiv 5 - xy \bmod 8$. This means $xy \equiv 4 \bmod 8$ or $xy \equiv 6 \bmod 8$. Since x is odd and $y \equiv 2 \bmod 8$, the former is impossible. Thus, we have $xy \equiv 6 \bmod 8$. This gives us $x \equiv 3 \bmod 4$. Similarly if $y \equiv 6 \bmod 8$, we have $x \equiv 1 \bmod 4$. This gives us possibility 4.

Now we consider the case that y is odd. This means that $y^2 \equiv 1 \bmod 8$, so we have $x^2 - xy \in \{0, -2\} \bmod 8$.

If x is odd, then $x^2 \equiv 1 \bmod 8$ as well, so we have $-xy \in \{-1, -3\}$, so $xy \in \{1, 3\}$. This means that y is either $x^{-1} \bmod 8$ or $3x^{-1} \bmod 8$. Since x is odd, $x^{-1} \equiv x \bmod 8$, so y is either x or $3x \bmod 8$. This gives possibilities 3 and 6.

If x is $0 \bmod 4$, then $x^2 \equiv 0 \bmod 8$, so we have $-xy \in \{0, -2\} \bmod 8$, so $xy \in \{0, 2\} \bmod 8$. Since we are taking x to be $0 \bmod 4$, $xy \equiv 2 \bmod 8$ is impossible, so we have $xy \equiv 0 \bmod 8$, which means $y \equiv 0 \bmod 2$ or $x \equiv 0 \bmod 8$. We are working in a case where y is odd, so we must have $x \equiv 0 \bmod 8$. With $x \equiv 0 \bmod 8$, the norm calculation is satisfied with any odd value for y. This gives possibility 1.

If x is $2 \bmod 4$, then $x^2 \equiv 4 \bmod 8$, so we have $-xy \in \{4, -6\}$, so $xy \in \{4, 6\}$. Since x is $2 \bmod 4$ and y is odd, xy cannot be divisible by 4. This means that in this case $xy \equiv 6 \bmod 8$. If x is $2 \bmod 8$, we have $2y \equiv 6 \bmod 8$, so $y \equiv 3 \bmod 4$. If x is $6 \bmod 8$, we have $6y \equiv 6 \bmod 8$, so $y \equiv 1 \bmod 4$. This is possibility 5, the last possibility.

Now, we take on the additional restriction that $\mathrm{Norm}(\gamma) = \pm 1$ rather than that just being a congruence relationship. In this case, we need to work with γ in terms of $\sqrt{d}$ rather than ζ_3, so we write $\gamma = \frac{a+b\sqrt{d}}{2}$.

First consider the case that $y \equiv 2 \bmod 4$, which also means $x \equiv 1 \bmod 2$. Looking at the norm mod 4, we have $x^2 - xy + y^2 \equiv 1 - 2 + 4 = 3 \equiv -1$. Since the norm is ± 1, it must be -1. We can take $a' = \frac{a}{2} \bmod 4$ and $b' = \frac{b}{2} \bmod 2$. Note that $b \equiv y \equiv 2 \bmod 4$ and $a \equiv 2x - y \equiv 0 \bmod 4$, so $a', b' \in \mathbb{Z}$. Looking at the norm, we have $(a')^2 - d(b')^2 = -1$. This means that for every prime p dividing b', -1 is a square mod b'. Since $b \equiv y \equiv 2 \bmod 4$, we have $b' \equiv 1 \bmod 2$. Since b' is odd and -1 is a quadratic residue mod b', p is 1 mod 4 for every prime dividing b', so $b' \equiv 1$

mod 4. Equivalently, $b \equiv 2 \bmod 8$. Since $c \equiv 1 \bmod 4$ and $b \equiv 2 \bmod 8$, we have $y \equiv bc \equiv 2 \bmod 8$ as desired.

Now consider the case that $x \equiv 1 \bmod 4$ and $y \equiv 1 \bmod 2$. The norm of γ is congruent to $x^2-xy+y^2 \equiv 1-y+1 = 2-y \bmod 4$. We claim we must have $y \equiv 1 \bmod 4$. If we had $y \equiv 3 \bmod 4$, the norm would be congruent to -1, so would actually be -1. Then, as in the previous paragraph, if we write $\gamma = \frac{a+b\sqrt{d}}{2} = a' + b'\sqrt{d}$, we can write the norm as $(a')^2 - d(b')^2 = -1$. This gives us $a^2 - db^2 = -4$. Again, b is odd because $b \equiv y \bmod 4$. This means that 2 has an inverse mod b, so the fact that -4 is a quadratic residue mod b implies that -1 is. Since b is odd, this means that $b \equiv 1 \bmod 4$. Thus, we have $y \equiv b \equiv 1 \bmod 4$. This contradicts our having taken $y \equiv 3 \bmod 4$, so we must have had $y \equiv 1 \equiv x \bmod 4$ in the first place. We have already seen that if x and y are both odd, then $y \equiv x \bmod 8$ or $y \equiv 3x \bmod 8$. Since $y \equiv x \bmod 4$, we must be in the former case, so $y \equiv x \bmod 8$.

Finally, we claim that x cannot be 2 mod 8. If $x \equiv 2 \bmod 4$, we have already seen that $y \equiv 1 \bmod 2$, so the norm of γ is congruent to $x^2 - xy + y^2 \equiv 0 - 2 + 1 = -1 \bmod 4$, so the norm of γ must actually be -1. Again, we can write $\gamma = \frac{a+b\sqrt{d}}{2} = a' + b'\sqrt{d}$, and we can write the norm as $(a')^2 - d(b')^2 = -1$. This gives us $a^2 - db^2 = -4$. Just as in the last paragraph, this means that -1 is a quadratic residue mod b, which means $b \equiv 1 \bmod 4$. This gives us $y \equiv b \equiv 1 \bmod 4$. We have already seen that when $x \equiv 2 \bmod 4$ and $y \equiv 1 \bmod 4$, it is always the case that $x \equiv 6 \bmod 8$. $\square$

Looking at the congruence possibilities when the norm is just congruent to ± 1

mod 8, we can see a symmetry between x and y. Swapping them throughout the set of possibilities results in exactly the same set. This is because all of these restrictions arose from analysis of the norm of $x + y\zeta_3$, namely $x^2 - xy + y^2$. The symmetry in the results arises because swapping x and y in this function gives exactly the same function.

When restricting to cases where the norm was ± 1 rather than just being congruent to ± 1, we had to convert to the a and b representation, establish the restrictions there, and then convert back to the x and y representation. The conversion back to the x and y representation was just to be consistent in how we are listing the possible congruence conditions on γ. The conversion to the a and b representation, though, plays a more interesting role.

It is not surprising that we should have to do this because these extra restrictions rely on the norm value itself rather than on a congruence condition on the norm value. When we are working with the x and y representation, we are able to work only with a congruence condition on the norm. This is because in this representation, we are not working with γ itself, we are working with something congruent to it. If we tried to use the same argument on the x and y representation, we would end up trying to say something like: since $x^2 - xy + y^2 \equiv -1$, we have that -1 is a quadratic residue mod any prime dividing y. But in order for that statement to be true, we need an equality there, not a congruence. In order to get equality, we must go back to working with γ itself rather than something of the form $x + y\zeta_3$ that is congruent to γ.

In this case, the norm condition we needed was not as strong as it was in the previous two cases. Again, though, we satisfy that condition by taking $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$.

As with the case that $d \equiv 3 \bmod 8$, adjoining a square root of γ to a field in the L-tower sometimes yields a ramified extension and other times yields an unramified extension.

Proposition 4.3.2. *Let d be 5 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. Let $x, y \in \mathbb{Z}$ be such that $\gamma \equiv x + y\zeta_3 \bmod 8$. Then $L_j(\gamma^{1/2})/L_j$ is an unramified extension for all j if either x or y is congruent to 0 mod 8 or if $x \equiv y \bmod 8$, and is a ramified extension for all j otherwise.*

Moreover, when $L_j(\gamma^{1/2})/L_j$ is ramified, it is ramified at both primes above (2).

Proof. Because unramified extensions lift to unramified extensions, when we are showing that the extensions are unramified, it is sufficient to show that $L_0(\gamma^{1/2})/L_0$ is unramified. Proposition 2.0.8 tells us that for this, it is sufficient to show that γ is a square mod 4 in L_0. When we are showing that the extensions are ramified Proposition 2.0.8 tells us we need to show that γ is not a square mod 4 in L_j for any j.

Taking the congruence possibilities for γ from the previous lemma and reducing them mod 4 tells us that the possibilities for γ mod 4 are ± 1, $3 + 2\zeta_3 \equiv -(1 + 2\zeta_3)$, $1 + 2\zeta_3$, $\pm(1 + \zeta_3)$, $\pm(1 + 3\zeta_3)$, $\pm\zeta_3$, $2 + 3\zeta_3 \equiv -(2 + \zeta_3)$, and $2 + \zeta_3$.

Combining the previous two paragraphs, we find that to prove our claim we must show that ± 1, $\pm(1+\zeta_3)$, and $\pm\zeta_3$ are squares mod 4 in L_0 and that $\pm(1+2\zeta_3)$,

$\pm(1-\zeta_3)$, and $\pm(2+\zeta_3)$ are not. Since $-1 = i^2$ is a square in L_j for all j, it is equivalent to show that 1, $1+\zeta_3$, and ζ_3 are squares mod 4 in L_0 and that $2+\sqrt{d}$, $1-\zeta_3$, and $2+\zeta_3$ are not squares mod 4 in L_j for any j.

Clearly, 1 and $\zeta_3 \equiv (\zeta_3^2)^2$ are squares mod 4. Since $1+\zeta_3 \equiv -\zeta_3^2 = (i\zeta_3)^2$ mod 4, $i \in L_0$, and there are elements in L_0 that are congruent to ζ_3 mod arbitrarily high powers of 2, it follows that $1+\zeta_3$ is a square mod 4 in L_0, so in L_j for all j.

It remains to show that none of $1+2\zeta_3$, $1-\zeta_3$, and $2+\zeta_3$ is a square mod 4 in L_j for any j. We show this by showing that $1+2\zeta_3$ is not a square mod 4 in L_j for any j and that either of the other two values is a square mod 4 in L_j iff $1+2\zeta_3$ is. Again, recall that ζ_3 is an element sufficiently close to being a cube root of unity 2-adically.

First note that because $2+2\zeta_3+2\zeta_3^2 \equiv 0$ mod 4, we have $2+\zeta_3 \equiv 2\zeta_3^2-\zeta_3$ mod 4. But $2\zeta_3^2-\zeta_3 \equiv -\zeta_3(2\zeta_3+1)$ mod 4. Because -1 and $\zeta_3 \equiv \zeta_3^2$ are both squares mod 4, $2+\zeta_3$ is a square mod 4 iff $1+2\zeta_3$ is. Similarly, $1-\zeta_3 \equiv -2\zeta_3-\zeta_3^2 = -\zeta_3(2+\zeta_3)$, so $1-\zeta_3$ is a square iff $2+\zeta_3$ is.

Assume that there is some $v \in L_j$ such that $v^2 \equiv 1+2\zeta_3$ mod 4. Then $v^2 \equiv 1$ mod 2, so we have $v \equiv 1$ mod $(1+i)$, and we can write $v = 1+\delta(1+i)$. Squaring this, we have $v^2 = 1+2\delta(1+i)+2i\delta^2$. Since we have assumed that $v^2 \equiv 1+2\zeta_3$ mod 4, this gives us $1+2\zeta_3 \equiv 1+2\delta(1+i)+2i\delta^2$ mod 4. We can subtract $1+2\zeta_3$ from both sides and divide through by 2 to get $0 \equiv \zeta_3+(1+i)\delta+i\delta^2$ mod 2.

We can multiply both sides of the entire congruence by i to get $0 \equiv i\zeta_3+(1+i)\delta+\delta^2$ mod 2. Note that we have the same problem that we had when adjoining fourth roots with $d \equiv 3$ mod 8, namely that $i\zeta_3$ is not in a low enough field to apply Corollary 3.2.6. (We would need it to be in $\mathbb{Q}$.) Now consider the congruence mod $(1+i)$: $\delta^2 \equiv \zeta_3 \bmod (1+i)$. Then $\delta \equiv \zeta_3^2 \bmod (1+\zeta_8)$, so we can write $\delta = \zeta_3^2 + \lambda(1+\zeta_8)$ and $\delta^2 \equiv \zeta_3 + \lambda^2(1+i) \bmod 2$. Substituting this back in, we get

$$\begin{aligned} 0 &\equiv i\zeta_3 + \zeta_3^2(1+i) + \lambda(1+\zeta_8)(1+i) + \zeta_3 + \lambda^2(1+i) \\ &= (\zeta_3 + \zeta_3^2)(1+i) + \lambda(1+i)(1+\zeta_8) + \lambda^2(1+i) \\ &\equiv (1+i) + \lambda(1+i)(1+\zeta_8) + \lambda^2(1+i) \bmod 2. \end{aligned}$$

Dividing through by $(1+i)$, we get $1 + \lambda(1+\zeta_8) + \lambda^2 \bmod (1+i)$. But now we can apply Corollary 3.2.4 to see that no such λ can exist. This means no such δ, thus no such v can exist. This shows that x is not a square mod 4 in L_j for any j. These calculations are valid in the completion at both primes above (2), so the extension is ramified at both of these primes. □

With the knowledge of the ramification behavior that arises when adjoining a square root of γ to fields in the L-tower, we can now look at the ramification behavior we get when we adjoin a fourth root of γ.

Theorem 4.3.3. *Let $d \in \mathbb{Z}$ be congruent to 5 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. Let $k \in \mathbb{Z}$ be such that $k^2 d \equiv -3 \bmod 64$, and let $\zeta_3 = \left(\frac{-1+k\sqrt{d}}{2}\right)$. Let $x, y \in \mathbb{Z}$ be such that $\gamma \equiv x + y\zeta_3 \bmod 8$. Then for $j > 0$, $L_j(\gamma^{1/4})/L_j$ is unramified iff $(x,y) \in \{\pm(0,1), \pm(1,0), \pm(1,1)\}$. Moreover, $L_0(\gamma^{1/4})/L_0$ iff $(x,y) \in \{(0,1),(7,7)\}$.*

Proof. Based on Lemma 4.3.1, we wish to show that exactly one of the following is true:

1. $x \equiv 0 \bmod 8$, $y \equiv 1 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is unramified for all j

2. $x \equiv 0 \bmod 8$, $y \equiv \pm 3 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j

3. $x \equiv 0 \bmod 8$, $y \equiv 7 \bmod 8$, $L_0(\gamma^{1/4})/L_0$ is ramified, and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$

4. $x \equiv 1 \bmod 8$, $y \equiv 0 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is unramified for all j

5. $x \equiv \pm 3 \bmod 8$, $y \equiv 0 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j

6. $x \equiv 7 \bmod 8$, $y \equiv 0 \bmod 8$, $L_0(\gamma^{1/4})/L_0$ is ramified, and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$

7. $x \equiv 1 \bmod 8$, $y \equiv 1 \bmod 8$, $L_0(\gamma^{1/4})/L_0$ is ramified, and $L_j(\gamma^{1/4})/L_j$ is unramified for all $j \geq 1$

8. $x \equiv \pm 3 \bmod 8$, $y \equiv x \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j

9. $x \equiv 7 \bmod 8$, $y \equiv 7 \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is unramified for all j

10. $x \equiv 1 \bmod 2$, $y \equiv 6x \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j

11. $x \equiv 6y \bmod 8$, $y \equiv 1 \bmod 2$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j

12. $x \equiv 1 \bmod 2$, $y \equiv 3x \bmod 8$, and $L_j(\gamma^{1/4})/L_j$ is ramified for all j.

We handle this case by case:

Case 1: $x \equiv 0 \bmod 8$, $y \equiv 1 \bmod 8$

This follows immediately from Lemma 3.1.7.

Case 2: $x \equiv 0 \bmod 8$, $y \equiv \pm 3 \bmod 8$

We have $\gamma \equiv \pm 3\zeta_3 = \mp(3 + 3\zeta_3^2) \bmod 8$. Since -1 is a fourth power in L_1, showing the result for all j for $-3\zeta_3$ also shows it for $j \geq 1$ for $3\zeta_3$. But since unramified extensions lift to unramified extensions, this also shows it for $-(3+3\zeta_3^2)$ for L_0. Thus, it is enough to prove the claim for $x \equiv -3\zeta_3 = 3 + 3\zeta_3^2 \bmod 8$.

Mod 4, this is ζ_3, so we can take $\alpha = \gamma$, since $\gamma \equiv \zeta_3 \bmod 4$. Also $\gamma \equiv \zeta_3$ mod

4 implies that $\gamma^2 \equiv \zeta_3^2 \bmod 8$, so $\gamma^4 \equiv \zeta_3 \bmod 8$. Then we have $\gamma - \alpha^4 = \gamma - \gamma^4 \equiv -3\zeta_3 - \zeta_3 = -4\zeta_3 \bmod 8$, so $\frac{\gamma-\alpha^4}{4} \equiv \zeta_3 \bmod 2$. The result now follows immediately from Corollary 3.2.9.

This argument works locally, but that is sufficient for the global case.

Case 3: $x \equiv 0 \bmod 8$, $y \equiv 7 \bmod 8$

This follows immediately from Lemma 3.1.8.

Case 4: $x \equiv 1 \bmod 8$, $y \equiv 0 \bmod 8$

This is Lemma 3.1.1.

Case 5: $x \equiv \pm 3 \bmod 8$, $y \equiv 0 \bmod 8$

This is Corollary 3.2.10.

Case 6: $x \equiv 7 \bmod 8$, $y \equiv 0 \bmod 8$

This is Lemma 3.1.3.

Case 7: $x \equiv 1 \bmod 8$, $y \equiv 1 \bmod 8$

Here $\gamma \equiv 1 + \zeta_3 = -\zeta_3^2 \bmod 8$. With this observation, this follows immediately from Lemma 3.1.8.

Case 8: $x \equiv \pm 3 \bmod 8$, $y \equiv x \bmod 8$

In this case, $\gamma \equiv \pm(3 + 3\zeta_3) = \pm(\zeta_3^2)$. This is the same as case 2 with a different choice for the primitive cube root of unity, so the argument is the same as in that case.

Case 9: $x \equiv 7 \bmod 8$, $y \equiv 7 \bmod 8$

Here, $\gamma \equiv 7 + 7\zeta_3 \equiv -1 - \zeta_3 = \zeta_3^2$. Now the result follows immediately from Lemma 3.1.7.

Case 10: $x \equiv 1 \bmod 2$, $y \equiv 6m \bmod 8$

Case 11: $x \equiv 6y \bmod 8$, $y \equiv 1 \bmod 2$

Case 12: $x \equiv 1 \bmod 2$, $y \equiv 3x \bmod 8$

In each of these cases, we saw in the previous proposition that for this value of γ, $L_j(\gamma^{1/2})/L_j$ is ramified, so $L_j(\gamma^{1/4})/L_j$ must be as well. $\square$

There is an interesting symmetry in the above result: swapping x and y gives the same result. Although the underlying reason is the same, it is not as straightforward to see as it was in Lemma 4.3.1, where it just arose because of the symmetry in the norm calculation. Here, it is caused by a pair of properties working together. The first is that multiplying γ by something that is a fourth power mod 8 cannot affect its behavior because that can just be absorbed in α. The second, which we used a couple of times in the proof, is that ζ_3^2 also satisfies $x^2 + x + 1 \equiv 0 \bmod 8$ and, as a result, $x^3 \equiv 1 \bmod 8$. These are the only properties of ζ_3 we used, so the behavior of ζ_3^2 must be the same as that of ζ_3. Combining these, we find that if we multiply $\gamma \equiv x + y\zeta_3 \bmod 8$ by something that is congruent to $\zeta_3^2 \bmod 8$, we get something congruent to $y + x\zeta_3^2 \bmod 8$. This, in turn, must behave exactly like $y + x\zeta_3$, which is what comes out of swapping x and y in the original γ.

4.4 $d \equiv 7 \bmod 8$

In this section, we find that when $d \equiv 7 \bmod 8$, we have some elements that are congruent to $\pm i \bmod 8$. In order for the fourth root of such an element to give an unramified extension, i must be a fourth power. For this to happen, ζ_{16} must be available, and this is not true in the L-tower until L_2. Thus, it is reasonable to expect that, unlike in the other sections, we might have extensions that are ramified at both L_0 and L_1, but are unramified beginning at L_2. In fact, this is precisely what we find.

Lemma 4.4.1. *Let $d \in \mathbb{Z}$ be congruent to 7 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be such that Norm(γ) $\equiv \pm 1$ mod 16, and write $\gamma = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. Then one of the following is true:*

- *$a \equiv 0$ mod 4 and $b \equiv 1$ mod 2*
- *$a \equiv \pm 1$ mod 8 and $b \equiv 0$ mod 4.*

Proof. Consider the norm to $\mathbb{Q}$: $a^2 - db^2$. We have assumed that this is congruent to ± 1. If we look at this mod 4, we have $d \equiv -1$, so $a^2 + b^2 \equiv \pm 1$. Since 0 and 1 are the only squares mod 4, we find that one of a and b must be odd, the other must be even, and the norm must be 1.

Looking at the norm mod 8, we still have $a^2 + b^2 \equiv 1$. If either a or b were 2 mod 4, this congruence could not be satisfied, so one of a and b is 0 mod 4, and the other is odd. Now look at the norm mod 16: we have either $a^2 + b^2 \equiv 1$ or $a^2 - 7b^2 \equiv 1$. If b is 0 mod 4, we have $a^2 \equiv 1$ mod 16, so $a \equiv \pm 1$ mod 8. $\square$

As in the previous three cases, instead of explicitly making an assumption about the norm of γ, we get that as a consequence of γ being the fourth power of an ideal of $\mathcal{O}_{K_0}$.

In the following proposition, we see that the ramification behavior from adjoining $\gamma^{1/2}$ is identical to the behavior we got when d was 3 mod 8.

Proposition 4.4.2. *Let d be 7 mod 8. Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and* *such that* $(\gamma) = I^4$ *for some ideal* I *of* $\mathcal{O}_{K_0}$. *Then* $L_0(\gamma^{1/2})/L_0$ *is unramified iff* $a \equiv 1$ *mod 2. If it is ramified, it is ramified at both primes above* (2). *Moreover,* $L_j(\gamma^{1/2})/L_j$ *is an unramified extension for* $j \geq 1$.

Proof. The proof that we used when $d \equiv 3 \bmod 8$ case works just as well for this case, with the exception that we need to prove that $\pm\sqrt{d}$ are not squares mod 4 in L_0 but are squares in L_1. (In the $d \equiv 3 \bmod 8$ case, we needed to prove this for $\pm(2+\sqrt{d})$). Since $i \in L_0 \subset L_1$, it is sufficient to prove that $\sqrt{d}$ is a square mod 4 in L_1, but not in L_0.

Since $d \equiv -1 \bmod 8$, we must have $\sqrt{d} \equiv \pm i \bmod 4$, depending on the completion chosen. Since $\zeta_8 \in L_1$, both of these are squares in L_1. If $\pm i$ were a square mod 4 in L_0, it would be a square mod 2 as well. We would need only to define its square root mod $1+i$, and the only such value in L_0 is 1. This does not square to i mod 2, so $\sqrt{d}$ is not a square mod 4 in L_0 as desired. This calculation is valid in either completion, so the extension is ramified at both primes above (2). □

Theorem 4.4.3. *Let* $d \in \mathbb{Z}$ *be congruent to 7 mod 8. Let* $\gamma \in \mathcal{O}_{K_0}$ *be relatively prime to 2 and such that* $(\gamma) = I^4$ *for some ideal* I *of* $\mathcal{O}_{K_0}$. *Let* $a, b \in \mathbb{Z}$ *be such that* $\gamma = a + b\sqrt{d}$. *Then for* $j > 1$, $L_j(\gamma^{1/4})/L_j$ *is unramified. Moreover,* $L_1(\gamma^{1/4})/L_1$ *is unramified iff* a *is odd. Finally,* $L_0(\gamma^{1/4})/L_0$ *iff* $a \equiv 1$ *mod 8.*

When these extensions are ramified, they are ramified at both primes above (2).

Proof. This time, we need to show that exactly one of the following is true:

- $a \equiv 1 \bmod 8$, $b \equiv 0 \bmod 4$, and $L_j(\gamma^{1/4})/L_j$ is an unramified extension for all

j

- $a \equiv -1 \bmod 8$, $b \equiv 0 \bmod 4$, $L_0(\gamma^{1/4})/L_0$ is ramified at both primes above (2), and $L_j(\gamma^{1/4})/L_j$ is an unramified extension for $j \geq 1$
- $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 2$, $L_j(\gamma^{1/4})/L_j$ is ramified at both primes above (2) for $j \in \{0, 1\}$, and $L_j(\gamma^{1/4})/L_j$ is unramified for $j \geq 2$.

With the exception of the modification to address the fact that there are two primes above (2) in $\mathcal{O}_L$ here, this is exactly the same situation as the corresponding theorem for $d \equiv 3 \bmod 8$, except for the third case. In the third case, a is 0 mod 4 rather than being 2 mod 4, and the extension becomes unramified at L_2 rather than staying ramified all the way up the L-tower. When $b \equiv 4 \bmod 8$, one might expect the proof for the first two cases to differ from the proof for $d \equiv 3 \bmod 8$ because we have $\gamma \equiv \pm(1 + 4\sqrt{d}) \bmod 8$, and $\sqrt{d}$ is different when $d \equiv 3 \bmod 8$ and $d \equiv 7 \bmod 8$. But since $\sqrt{d}$ has a coefficient of 4, we are concerned here only with the congruence class of $\sqrt{d}$ mod 2. It turns out that this is the same any time $d \equiv 3 \equiv -1 \bmod 4$. In that case $\sqrt{d} \equiv \pm i \equiv i \bmod 2$. So the proof we used when $d \equiv 3 \bmod 8$ still works for the first two cases here. The calculation does not change based on the choice of completion, so when we get ramification at all, we get it at both primes above (2).

The only place where the proof needs to change is in the third case. For this, we want to change our representation of γ. If $d \equiv 7 \equiv -9 \bmod 16$, then $\sqrt{d} \equiv \pm 3i \bmod 8$. If $d \equiv -1 \bmod 16$, then $\sqrt{d} \equiv \pm i \bmod 8$. In either case, the 8 possibilities we need to deal with are $x + yi$ with $x \equiv 0 \bmod 4$ and $y \equiv 1 \bmod 2$. We can further restrict the possibilities for y. As usual, we do this by looking at the norm:

$x^2 + y^2 \equiv \pm 1 \bmod 16$. Since $x \equiv 0 \bmod 4$, this gives us $y^2 \equiv \pm 1 \bmod 16$. Since -1 is not a quadratic residue mod 16, we have $y^2 \equiv 1 \bmod 16$, so $y \equiv \pm 1 \bmod 8$.

Now the result for the third case is exactly the statement of Lemma 3.1.6. Note that the ramification results are the same at either completion, so when we get ramification, we get it at both primes above (2). $\square$

In Theorem 1.0.1, which is from [1], the authors restrict to the case that d splits in F_0. In this sense, the case that $d \equiv 7 \bmod 8$ is the most direct analogue to their result. Perhaps, then, it is not surprising that this is the one case where every possible choice of γ results in $L_j(\gamma^{1/4})/L_j$ being unramified for sufficiently large j. Unlike their result, which always gives an unramified extension when $j = 1$, the result here does not always give an unramified extension until $j = 2$.

4.5 Properties of these extensions

4.5.1 Independence

In [1], the authors show that if $I_1, \cdots, I_n$ represent independent ideal classes of order 3 with $I_j^3 = (\gamma_j)$, then $L_1(\varepsilon_0^{1/3}, \gamma_1^{1/3}, \ldots, \gamma_n^{1/3})/L_1$ has degree 3^{n+1}. We show an analogous result, but first we need a pair of easy results.

Lemma 4.5.1. *Let $L = K(\sqrt{d})$ be a quadratic field extension and let $\gamma \in K$. If γ is a fourth power in L, then one of the following is true:*

- *$\gamma = \alpha^4$ for some $\alpha \in K$*
- *$\gamma = d^2\alpha^4$ for some $\alpha \in K$*
- *$L = K(i)$ and $\gamma = -4\alpha^4$ for some $\alpha \in K$.*

Proof. If γ is a fourth power in L, we have $a, b \in K$ such that

$$\begin{aligned}
\gamma &= (a + b\sqrt{d})^4 \\
&= a^4 + 4a^3b\sqrt{d} + 6a^2b^2d + 4ab^3d\sqrt{d} + b^4d^2 \\
&= (a^4 + 6a^2b^2d + b^4d^2) + 4ab(a^2 + db^2)\sqrt{d}.
\end{aligned}$$

Since L is a quadratic extension, $\sqrt{d} \notin K$, so we must have $4ab(a^2 + db^2) = 0$. This means $a = 0$, $b = 0$, or $a^2 + db^2 = 0$. If $a = 0$, then $\gamma = b^4d^2$, which is the second option in the list. If $b = 0$, then $\gamma = a^4$, which is the first option in the list. If $a^2 + db^2 = 0$, then $d = -(\frac{a}{b})^2$ is the negative of a square in K. This means that $L = K(\sqrt{d}) = K(\sqrt{-1})$. Now if γ is a fourth power in L, we have $a, b \in K$ such that $\gamma = (a^4 - 6a^2b^2 + b^4) + 4ab(a^2 - b^2)i$. If either a or b is 0, the first case above is satisfied. If not, we must have $a^2 = b^2$, so $\gamma = -4a^4$. $\square$

The value $-4\alpha^4$ here is related to the element of the same form referenced in Theorem 4.5.4. In fact, if we weaken our condition from γ being a fourth power in L to $X^4 - \gamma$ is reducible in $K[X]$, that theorem tells us that either γ is a square in K, or that γ is of the form $-4\alpha^4$ for some $\alpha \in K$.

Corollary 4.5.2. *Let $\gamma \in K_0$ be such that $\gamma > 0$ in at least one embedding of K_0 into $\mathbb{R}$. If γ is a fourth power in L_j for any j, then γ is a fourth power in K_0.*

Proof. We do this in two steps. First, we show that γ must be a fourth power in L_0. Then, we show that this implies it must be a fourth power in K_0.

If $j > 0$, consider the extension L_j/L_{j-1}. The previous lemma tells us that either γ is a fourth power in L_{j-1} or $\gamma = \zeta_{2^{j+1}}\alpha^4$ for some $\alpha \in L_{j-1}$. (The third option is not relevant because L_j is not $L_{j-1}(i)$ for any $j > 0$.) We claim that it is impossible to have $\gamma = \zeta_{2^{j+1}}\alpha^4$ for some $\alpha \in L_{j-1}$.

Let σ be the non-trivial element of the Galois group of L_{j-1}/K_{j-1}. Applying this to that equation gives us $\sigma(\gamma) = \zeta_{2^{j+1}}^{-1}\sigma(\alpha)^4$. Since $\gamma \in K_0$, we have $\gamma = \sigma(\gamma)$, so $\zeta_{2^{j+1}}\alpha^4 = \zeta_{2^{j+1}}^{-1}\sigma(\alpha)^4$. Multiplying both sides by $\zeta_{2^{j+1}}\alpha^{-4}$ gives $\zeta_{2^j} = \alpha^{-4}\sigma(\alpha)^4$. But this means ζ_{2^j} is a fourth power in L_{j-1}, which isn't true.

So γ must be a fourth power in L_{j-1}. Repeating this argument j times, we find that γ is a fourth power in L_0.

Now the previous lemma tells us that either γ is a fourth power in K_0 or $\gamma = -4\alpha^4$ for some $\alpha \in K_0$. (The second of the three options in the lemma is redundant because $d = -1$ in this case, so $d^2 = 1$.) Since $\alpha \in K_0$, which is real, $\alpha^4 > 0$. Since $\gamma > 0$ in at least one real embedding, it is impossible for $\gamma = -4\alpha^4$, so we must have γ a fourth power in K_0. □

We can now follow the same argument as appears in [1] to get the following proposition:

Proposition 4.5.3. *Let $I_1, \ldots, I_n$ represent independent ideal classes of order 4 in K_0 with I_j relatively prime to 2 for all j. Write $I_j^4 = (\gamma_j)$ with $\gamma_j \in K_0$ and $\gamma_j > 0$ for all j in at least one embedding of K_0 into $\mathbb{R}$. Then $\varepsilon_0, \gamma_1, \ldots, \gamma_n$ are independent mod fourth powers in L_j.*

Proof. Suppose that $\varepsilon_0^{a_0}\gamma_1^{a_1}\cdots\gamma_n^{a_n} = \beta^4$ in L_j. Since β^4 is a product of elements in K_0, we have $\beta^4 \in K_0$. Now applying the previous corollary tells us that we can take $\beta \in K_0$.

Now we can write $I_1^{a_1} \cdots I_n^{a_n} = (\beta)$. Since these ideals represent independent classes, each with order 4, we must have $a_j \equiv 0 \bmod 4$ for all j. This means that $\varepsilon_0^{a_0} = \beta^4 \gamma_1^{-a_1} \cdots \gamma_n^{-a_n}$ is a fourth power in K_0, which means that $a_0 \equiv 0 \bmod 4$. $\square$

In [1], $L_1(\varepsilon_0^{1/3}, \gamma_1^{1/3}, \ldots, \gamma_n^{1/3})/L_1$ is a degree-3^{n+1} extension. The analogue in our case is not necessarily a degree-4^{n+1} extension.

4.5.2 Degrees

For all of these extensions, it is valuable to understand what degree the extension has. In particular, to say that a trivial extension is unramified is distinctly uninteresting. In many cases, we can say exactly what the degree of the extension is. When proving results about the degrees of these extensions, we frequently use the following theorem:

Theorem 4.5.4. *Let K be a field and n an integer ≥ 2. Let $\gamma \in K$, $\gamma \neq 0$. Assume that for all prime numbers p such that $p \mid n$ we have $\gamma \notin K^p$, and if $4 \mid n$ then $\gamma \notin -4K^4$. Then $X^n - \gamma$ is irreducible in $K[X]$.*

The above theorem is the subject of Section 9 of Chapter 8 in [2]. We need only the following interesting corollary, which arises from taking $n = 4$ and K a field in the L-tower:

Corollary 4.5.5. *Let $\gamma \in L_j$, $\gamma \neq 0$. Then the following are equivalent:*

1. *γ is not a square in L_j*
2. *$L_j(\gamma^{1/2})/L_j$ is a degree-2 extension*
3. *$L_j(\gamma^{1/4})/L_j$ is a degree-4 extension.*

Proof. Part 1 and Part 2 are obviously equivalent. Also, Part 3 clearly implies Part 2. To prove the result, then, it is sufficient to prove that Part 1 implies Part 3. To do this, we use the previous theorem.

Although we are taking $n = 4$, so $4 \mid n$, we do not have to take on the extra assumption that $\gamma \notin -4(L_j)^4$. This is because $-4 = (2i)^2$ is a square in L_j for all j. Thus, the fact that γ is not a square already implies that this extra assumption is satisfied. Our corollary now follows from noting that if $X^n - \gamma$ is irreducible in $K[X]$ for some field K, then $K(\gamma^{1/n})/K$ is a degree-n extension. $\square$

Understanding the degree of $L_j(\gamma^{1/2})/L_j$ is often important for understanding the degree of $L_j(\gamma^{1/4})/L_j$. The following two results, in addition to Proposition 2.0.8, are critical for this.

Proposition 4.5.6. *Let d be a positive square-free integer with $d > 2$. Let $K_0 = \mathbb{Q}(\sqrt{d})$, $K_1 = K_0(\sqrt{2})$, and let ε_0 be the fundamental unit of K_0. Then $\sqrt{\varepsilon_0} \in K_1$ iff (2) ramifies principally in K_0.*

Proof. ($\Rightarrow$) If $\sqrt{\varepsilon_0} \in K_1 = K_0(\sqrt{2})$, then $\sqrt{\varepsilon_0}/\sqrt{2} \in K_0$ because it is fixed by the action of the non-trivial element of $\mathrm{Gal}(K_1/K_0)$. Thus, $\sqrt{2\varepsilon_0} \in K_0$. Let $(a+b\sqrt{d})^2 = 2\varepsilon_0$. Then as ideals, we have $(a + b\sqrt{d})^2 = (2)$ so (2) is the square of a principal ideal.

($\Leftarrow$) If (2) ramifies principally, there is some unit $u \in K_0$ such that $2u$ has a square root in K_0. Since ε_0 is the fundamental unit, we can write $u = \pm\varepsilon_0^n$. Since 2 and ε_0 are positive in at least one real embedding and K_0 is real, we must have $u = \varepsilon_0^n$ for some $n \in \mathbb{Z}$. Since $2\varepsilon_0^n$ has a square root in K_0 iff $2\varepsilon_0^{n \bmod 2}$ has one, one of the following must be true: $2\varepsilon_0^0 = 2$ has a square root in K_0 or $2\varepsilon_0^1 = 2\varepsilon_0$ has a square root in K_0. The former can be true only for $d = 2$, but we have taken $d > 2$. Thus, we have that $2\varepsilon_0$ has a square root in K_0, so $\sqrt{\varepsilon_0} \in K_1$. $\square$

Since ε_0 is positive in at least one real embedding, we cannot have $\sqrt{\varepsilon_0} \in L_0$. If it were, we would have $L_0 = K_0(\varepsilon_0^{1/2})$. This is impossible because L_0 is totally imaginary, so must be generated by the square root of a totally negative element. The same argument shows that $\sqrt{\varepsilon_0}$ is not in $K_0(\sqrt{-2})$. Since $K_0(\varepsilon_0^{1/2})$ is degree 2, if $\varepsilon_0^{1/2} \in L_1$, it must also be in one of the degree-2 sub-extensions of L_1/K_0. We have just seen that the only possibility is K_1. So the result above can actually be stated as $\sqrt{\varepsilon_0} \in L_1$ iff $\sqrt{\varepsilon_0} \in K_1$ iff (2) ramifies as the square of a principal ideal in K_0.

If we are not dealing exclusively with units, we cannot say as much, but we can say something if γ is relatively prime to 2:

Proposition 4.5.7. *Let d be a positive square-free integer with $d > 2$. Let $K_0 = \mathbb{Q}(\sqrt{d})$, $K_1 = K_0(\sqrt{2})$, and let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 with $\sqrt{\gamma} \notin K_0$. Then $\sqrt{\gamma} \in K_1$ implies that (2) ramifies in K_0.*

Proof. If $\sqrt{\gamma} \in K_1 = K_0(\sqrt{2})$, then $\sqrt{\gamma}/\sqrt{2} \in K_0$ because it is fixed by the action of the non-trivial element of $\mathrm{Gal}(K_1/K_0)$. Thus, $\sqrt{2\gamma} \in K_0$. Let $(a + b\sqrt{d})^2 = 2\gamma$. Then as ideals, we have $(a + b\sqrt{d})^2 = (2\gamma)$ in K_0. Since γ is relatively prime to 2, (2) must be ramified. $\square$

Now we have the tools we need to start examining the degrees of the extensions we have dealt with throughout the paper. We start with a pair of propositions that shed light on the degree of $L_j(\gamma^{1/4})/L_j$ when $j \leq 1$.

Proposition 4.5.8. *Let $\gamma \in K_0$ be such that $\sqrt{\gamma} \notin K_0$ and $\gamma > 0$ in at least one embedding of K_0 into $\mathbb{R}$. Then $L_0(\gamma^{1/2})/L_0$ is a degree-2 extension and $L_0(\gamma^{1/4})/L_0$ is a degree-4 extension.*

Proof. Since γ is positive, we cannot have $\sqrt{\gamma} \in L_0$. If it were, we would have $L_0 = K_0(\gamma^{1/2})$, which would mean the square root of a positive element is generating a non-real extension. Since $\sqrt{\gamma} \notin L_0$, the result follows immediately from Corollary 4.5.5. □

Proposition 4.5.9. *Let $\gamma \in \mathcal{O}_{K_0}$ be such that $\sqrt{\gamma} \notin K_0$ and $\gamma > 0$ in at least one embedding of K_0 into $\mathbb{R}$. Assume that (2) does not ramify in K_0. Then $L_1(\gamma^{1/2})/L_1$ is a degree-2 extension and $L_1(\gamma^{1/4})/L_1$ is a degree-4 extension.*

Moreover, if $\gamma = \varepsilon_0$, the fundamental unit of K_0, then the following are equivalent:

1. *(2) does not ramify as the square of a principal ideal in K_0*
2. *ε_0 is not a square in L_1*
3. *$L_1(\varepsilon_0^{1/2})/L_1$ is a degree-2 extension*
4. *$L_1(\varepsilon_0^{1/4})/L_1$ is a degree-4 extension.*

Proof. We saw in Proposition 4.5.7 that if (2) does not ramify in K_0, then $\sqrt{\gamma} \notin K_1$. The same argument that we used in the previous proposition about γ being positive and the field in the L-tower being non-real holds here as well. Thus $\sqrt{\gamma} \notin L_1$. Now the result follows from Corollary 4.5.5.

For ε_0, we again use Corollary 4.5.5. With this, it is sufficient to show that ε_0 is a square in L_1 iff (2) ramifies principally in K_0. First note that ε_0 is a square in L_1 iff ε_0 is a square in K_1. Obviously, ε_0 being a square in K_1 implies it is one in L_1. To see the reverse direction, note that ε_0 is positive, so $\varepsilon_0^{1/2}$ is real. Since K_1 is real and L_1 is not, we cannot have $L_1 = K_1(\varepsilon_0^{1/2})$. Thus, if $\varepsilon_0^{1/2} \in L_1$, it must also be the case that $\varepsilon_0^{1/2} \in K_1$. The rest of the claim follows immediately from Proposition 4.5.6. □

Degrees of unramified extensions

Note that L_j/L_{j-1} is always ramified at 2. Since unramified extensions lift to unramified extensions, the degrees of unramified extensions are maintained as those extensions are lifted to extensions of higher fields in the L-tower. Using this argument, we claim that all of the unramified extensions mentioned in Theorem 4.1.4, Theorem 4.2.3, and Theorem 4.3.3 have degree 4 so long as $\gamma > 0$. The same is true for many of the extensions in Theorem 4.4.3.

Again, it is possible that we must choose a completion in order to say whether $\gamma > 0$, but if the extension is degree 4 in any completion, it must be globally as well. Once we have chosen a completion, we can always choose a $\gamma > 0$ as the generator of (γ) by multiplying γ by -1 if necessary. In addition to requiring $\gamma > 0$, the previous two propositions also require that $\sqrt{\gamma} \notin K_0$. One way of accomplishing this is to strengthen the restriction that $(\gamma) = I^4$ with the requirement that I be an ideal of order 4. When $\gamma = \varepsilon_0$, we do not need this extra restriction to ensure that $\sqrt{\gamma} \notin K_0$.

Consider the case that $d \equiv 1 \bmod 4$. We wish to show that all of the unramified extensions mentioned in Theorem 4.1.4 and Theorem 4.3.3 are degree-4 extensions when $\gamma > 0$ and $\sqrt{\gamma} \notin K_0$. Since $d \equiv 1 \bmod 4$, (2) does not ramify in K_0, so our last two propositions show that the unramified extensions of L_0 and L_1 all have degree 4. In Theorem 4.1.4 and Theorem 4.3.3, every time $L_j(\gamma^{1/4})/L_j$ is unramified for $j > 1$, it is the lift of an unramified extension $L_1(\gamma^{1/4})/L_1$. Thus, applying the previous two propositions and the argument that unramified extensions lift to unramified extensions, we find that all of the unramified extensions are degree-4 extensions.

When $d \equiv 3 \bmod 8$, a slightly different argument shows the same for Theorem 4.2.3. Note that for every congruence possibility for γ in that theorem such that $L_j(\gamma^{1/4})/L_j = L_j((-\gamma)^{1/4})/L_j$ is unramified for $j > 1$, it is also the case that either $L_0(\gamma^{1/4})/L_0$ or $L_0((-\gamma)^{1/4})/L_0$ is unramified. In either case, $L_j(\gamma^{1/4})/L_j$ is the lift of an unramified extension of L_0. Thus, it is sufficient to note that the unramified extensions of L_0 in this theorem are degree 4. Again, taking $\gamma > 0$ and $\sqrt{\gamma} \notin K_0$, we get this from Proposition 4.5.8.

Finally, we consider $d \equiv 7 \bmod 8$ and Theorem 4.4.3, which is the most complicated case. The same argument we used for $d \equiv 3 \bmod 8$ establishes that all of the unramified extensions have degree 4 when a is odd. When a is even, however, we have a scenario where $L_1(\gamma^{1/4})/L_1$ is still ramified, and we do not get an unramified extension until L_2. If $\gamma = \varepsilon_0$ and (2) fails to ramify principally, we know from Proposition 4.5.6 and Proposition 4.4.2 that $L_j(\gamma^{1/2})$ is an unramified degree-2 extension for $j \geq 1$. Then Corollary 4.5.5 tells us that $L_j(\gamma^{1/4})/L_j$ is degree 4. If $\gamma = \varepsilon_0$ and (2) ramifies principally, we know that $L_j(\gamma^{1/2})/L_j$ is trivial for $j \geq 1$. This means that $L_j(\varepsilon_0^{1/4})/L_j$ is either degree 2 or trivial. Proposition 4.5.3 tells us the extension cannot be trivial. For γs other than ε_0, the tools we have developed here do not tell us about the degrees of these extensions other than that they are non-trivial.

Degrees of ramified extensions

When we look at ramified extensions, one might expect us to lose one of the tools that we have available when we look at unramified extensions: non-trivial extensions are no longer guaranteed to keep their degree as they are lifted up the L-tower. Some of our ramified extensions, though, result from extending an unramified extension by a ramified one. This means that that tool continues to be useful in this case. We also gain an additional tool that we did not have before: ramified extensions cannot be trivial.

When looking at the case where $L_j(\gamma^{1/4})/L_j$ is ramified, we want to consider two different scenarios. The first is that $L_j(\gamma^{1/2})/L_j$ is ramified. The second is that $L_j(\gamma^{1/2})/L_j$ is unramified, but $L_j(\gamma^{1/4})/L_j$ is ramified.

In the first case, the argument is straightforward. Since $L_j(\gamma^{1/2})/L_j$ is ramified, γ is not a square in L_j. Applying Corollary 4.5.5, we see that the degree of $L_j(\gamma^{1/4})/L_j$ is 4.

In the second case, the argument is slightly more complicated. First we consider what happens when this situation arises at L_0. In this case, since we continue to take $\gamma > 0$ with $\sqrt{\gamma} \notin K_0$, we know from Proposition 4.5.8 that $L_0(\gamma^{1/4})/L_0$ is degree 4.

Now we look at L_j for $j \geq 1$. Because we are in the case where $L_j(\gamma^{1/2})/L_j$ is unramified but $L_j(\gamma^{1/4})/L_j$ is ramified, we must have $L_j(\gamma^{1/4})/L_j(\gamma^{1/2})$ ramified.

This means it is non-trivial, so must be degree 2. Thus $L_j(\gamma^{1/4})/L_j$ is either degree 4 or degree 2 depending on whether $\gamma^{1/2} \in L_j$. We can use Proposition 4.5.9 to see that these extensions are always degree 4 when $d \equiv 1 \bmod 4$ (so that (2) does not ramify in K_0). When $d \equiv 3 \bmod 4$, if $\gamma = \varepsilon_0$, $L_j(\gamma^{1/4})/L_j$ is degree 4 iff (2) fails to ramify principally.

Over the last two sections, we have proved the following proposition:

Proposition 4.5.10. *Let $\gamma \in \mathcal{O}_{K_0}$ be relatively prime to 2 and such that $\sqrt{\gamma} \notin K_0$ and $(\gamma) = I^4$. If $d \equiv 1 \bmod 4$, then $L_j(\gamma^{1/4})/L_j$ is a degree-4 extension. If $d \equiv 3 \bmod 8$, $L_j(\gamma^{1/4})/L_j$ is a degree-4 extension if it is an unramified extension.*

Chapter A: Examples

For each congruence class of d, we showed that a number of congruences mod 8 could not be satisfied by γ when $\mathrm{Norm}(\gamma) \equiv \pm 1 \bmod 16$ (or, in one case, mod 8). When $d \equiv 1 \bmod 4$, we gave further restrictions on the possible value of γ when $\mathrm{Norm}(\gamma) = \pm 1$. In the former case, we did this because we were interested in values of γ such that $(\gamma) = I^4$ for some ideal I of $\mathcal{O}_{K_0}$. In the latter, we were particularly interested in $\gamma = \varepsilon_0$.

Here, we give examples of γs such that $(\gamma) = I^4$ for some ideal I of order 4 in $\mathcal{O}_{K_0}$. We also give examples of fundamental units of K_0. We have an example for each congruence condition on γ or ε_0 that we have not shown is impossible. This shows that we did actually need to consider each of those possibilities mod 8.

A.1 $d \equiv 1 \bmod 8$

$a \bmod 8$	$b \bmod 8$	d	γ
1	0	897	$-32607 + 1008\sqrt{d}$
7	0	897	$32607 - 1008\sqrt{d}$
1	4	145	$521 - 36\sqrt{d}$
7	4	145	$-521 + 36\sqrt{d}$
4	1	689	$7691764 + 293033\sqrt{d}$
4	3	505	$8588 - 421\sqrt{d}$
4	5	505	$-8588 + 421\sqrt{d}$
4	7	689	$-7691764 - 293033\sqrt{d}$
0	1	145	$1032 + 89\sqrt{d}$
0	3	505	$-706088 - 31421\sqrt{d}$
0	5	505	$706088 + 31421\sqrt{d}$
0	7	145	$-1032 - 89\sqrt{d}$

Table A.1: Examples of $\gamma = a + b\sqrt{d}$ with $(\gamma) = I^4$ for some ideal I of order 4 in $\mathcal{O}_K$ for $d \equiv 1 \bmod 8$

$a \bmod 8$	$b \bmod 8$	d	ε_0
1	0	561	$522785 + 22072\sqrt{d}$
7	0	161	$11775 + 928\sqrt{d}$
1	4	105	$41 + 4\sqrt{d}$
7	4	33	$23 + 4\sqrt{d}$
4	1	17	$4 + \sqrt{d}$
4	5	73	$1068 + 125\sqrt{d}$
0	1	41	$32 + 5\sqrt{d}$
0	5	137	$1744 + 149\sqrt{d}$

Table A.2: Examples of $\varepsilon_0 = a + b\sqrt{d}$, the fundamental unit in $\mathcal{O}_K$ for $d \equiv 1 \bmod 8$

A.2 $d \equiv 3 \bmod 8$

a mod 8	b mod 8	d	γ
2	1	291	$122 - 7\sqrt{d}$
2	3	939	$338 + 11\sqrt{d}$
2	5	219	$194 + 13\sqrt{d}$
2	7	1139	$42 - \sqrt{d}$
6	1	1139	$-42 + \sqrt{d}$
6	3	219	$-194 - 13\sqrt{d}$
6	5	939	$-338 - 11\sqrt{d}$
6	7	291	$-122 + 7\sqrt{d}$
1	0	219	$121 - 8\sqrt{d}$
1	4	291	$-751 - 44\sqrt{d}$
7	0	219	$-121 + 8\sqrt{d}$
7	4	291	$751 + 44\sqrt{d}$

Table A.3: Examples of $\gamma = a + b\sqrt{d}$ with $(\gamma) = I^4$ for some ideal I of order 4 in $\mathcal{O}_K$ for $d \equiv 3 \bmod 8$

a mod 8	b mod 8	d	ε_0
2	1	3	$2+\sqrt{d}$
2	3	11	$10+3\sqrt{d}$
2	5	59	$530+69\sqrt{d}$
2	7	17	$170+39\sqrt{d}$
6	1	35	$6+\sqrt{d}$
6	3	235	$46+3\sqrt{d}$
6	5	91	$1574+165\sqrt{d}$
6	7	515	$17406+767\sqrt{d}$
1	0	579	$385+16\sqrt{d}$
1	4	155	$249+20\sqrt{d}$
7	0	299	$415+24\sqrt{d}$
7	4	651	$1735+68\sqrt{d}$

Table A.4: Examples of $\varepsilon_0 = a + b\sqrt{d}$, the fundamental unit in $\mathcal{O}_K$ for $d \equiv 3 \bmod 8$

A.3 $d \equiv 5 \bmod 8$

x mod 8	y mod 8	d	γ
0	1	3341	$\frac{12543}{2} + \frac{217}{2}\sqrt{d}$
0	3	1045	$\frac{37}{2} - \frac{1}{2}\sqrt{d}$
0	5	1045	$-\frac{37}{2} + \frac{1}{2}\sqrt{d}$
0	7	3341	$-\frac{12543}{2} - \frac{217}{2}\sqrt{d}$
1	0	445	$169 + 8\sqrt{d}$
3	0	2501	$-3001 - 60\sqrt{d}$
5	0	2501	$3001 + 60\sqrt{d}$
7	0	445	$-169 - 8\sqrt{d}$
1	1	1221	$\frac{457}{2} + \frac{13}{2}\sqrt{d}$
3	3	1045	$\frac{227}{2} + \frac{7}{2}\sqrt{d}$
5	5	1045	$-\frac{227}{2} - \frac{7}{2}\sqrt{d}$
7	7	1221	$-\frac{457}{2} - \frac{13}{2}\sqrt{d}$
1	6	2005	$-8642 - 193\sqrt{d}$
3	2	2605	$-242 + 5\sqrt{d}$
5	6	2605	$242 - 5\sqrt{d}$
7	2	2005	$8642 + 193\sqrt{d}$
6	1	445	$\frac{11}{2} + \frac{1}{2}\sqrt{d}$
2	3	2533	$-\frac{47}{2} - \frac{1}{2}\sqrt{d}$
6	5	2533	$\frac{47}{2} + \frac{1}{2}\sqrt{d}$
2	7	445	$-\frac{11}{2} - \frac{1}{2}\sqrt{d}$
1	3	2005	$-\frac{41}{2} - \frac{1}{2}\sqrt{d}$
3	1	2669	$\frac{13}{2} + \frac{1}{2}\sqrt{d}$
5	7	2669	$-\frac{13}{2} - \frac{1}{2}\sqrt{d}$
7	5	2005	$\frac{41}{2} + \frac{1}{2}\sqrt{d}$

Table A.5: Examples of $\gamma \equiv x + y\zeta_3 \bmod 8$ with $(\gamma) = I^4$ for some ideal I of order 4 in $\mathcal{O}_K$ for $d \equiv 5 \bmod 8$

x mod 8	y mod 8	d	ε_0
0	1	221	$\frac{15}{2}+\frac{1}{2}\sqrt{d}$
0	3	93	$\frac{29}{2}+\frac{3}{2}\sqrt{d}$
0	5	357	$\frac{19}{2}+\frac{1}{2}\sqrt{d}$
0	7	69	$\frac{25}{2}+\frac{3}{2}\sqrt{d}$
1	0	1605	$641+16\sqrt{d}$
3	0	381	$1015+52\sqrt{d}$
5	0	1173	$137+4\sqrt{d}$
7	0	141	$95+8\sqrt{d}$
1	1	77	$\frac{9}{2}+\frac{1}{2}\sqrt{d}$
3	3	205	$\frac{43}{2}+\frac{3}{2}\sqrt{d}$
5	5	21	$\frac{5}{2}+\frac{1}{2}\sqrt{d}$
7	7	805	$\frac{1447}{2}+\frac{51}{2}\sqrt{d}$
3	2	37	$6+\sqrt{d}\equiv$
7	2	101	$10+\sqrt{d}\equiv$
6	1	13	$\frac{3}{2}+\frac{1}{2}\sqrt{d}$
6	5	53	$\frac{7}{2}+\frac{1}{2}\sqrt{d}$
3	1	29	$\frac{5}{2}+\frac{1}{2}\sqrt{d}$
7	5	5	$\frac{1}{2}+\frac{1}{2}\sqrt{d}$

Table A.6: Examples of $\varepsilon_0 \equiv x + y\zeta_3$ mod 8, the fundamental unit in $\mathcal{O}_K$ for $d \equiv 5$ mod 8

A.4 $d \equiv 7 \bmod 8$

a mod 8	b mod 8	d	γ
0	1	399	$-32 + \sqrt{d}$
0	3	791	$-88 + 3\sqrt{d}$
0	5	791	$88 - 3\sqrt{d}$
0	7	399	$32 - \sqrt{d}$
4	1	1023	$292 + 9\sqrt{d}$
4	3	1239	$388 + 11\sqrt{d}$
4	5	1239	$-388 - 11\sqrt{d}$
4	7	1023	$-292 - 9\sqrt{d}$
1	0	799	$1585 + 56\sqrt{d}$
7	0	799	$-1585 - 56\sqrt{d}$
1	4	399	$241 + 12\sqrt{d}$
7	4	399	$-241 - 12\sqrt{d}$

Table A.7: Examples of $\gamma = a + b\sqrt{d}$ with $(\gamma) = I^4$ for some ideal I of order 4 in $\mathcal{O}_K$ for $d \equiv 7 \bmod 8$

a mod 8	b mod 8	d	ε_0
0	1	31	$1520 + 273\sqrt{d}$
0	3	7	$8 + 3\sqrt{d}$
0	5	23	$24 + 5\sqrt{d}$
0	7	47	$48 + 7\sqrt{d}$
4	1	15	$4 + \sqrt{d}$
4	3	87	$28 + 3\sqrt{d}$
4	5	231	$76 + 5\sqrt{d}$
4	7	447	$148 + 7\sqrt{d}$
1	0	791	$225 + 8\sqrt{d}$
7	0	1271	$32799 + 920\sqrt{d}$
1	4	39	$25 + 4\sqrt{d}$
7	4	95	$39 + 4\sqrt{d}$

Table A.8: Examples of $\varepsilon_0 = a + b\sqrt{d}$, the fundamental unit in $\mathcal{O}_K$ for $d \equiv 7 \bmod 8$

Bibliography

[1] D. Hubbard and L. Washington. Kummer generators and lambda invariants. *J. Number Theory*, 130(1):61–81, January 2010.

[2] S. Lang. *Algebra*. Addison-Wesley, 2nd edition, 1984.

[3] L. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, 2nd edition, 1997.