ABSTRACT

Title of Dissertation: ON THE DIVISIBILITY OF CLASS NUMBERS IN FAMILIES OF NUMBER FIELDS

David Lev Pincus
Doctor of Philosophy, 2021

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

We adapt techniques used to investigate the divisibility of class numbers in families of algebraic number fields to study related topics in three particular families of number fields. Let r be a positive integer. We prove that the quartic family contains infinitely many distinct fields whose class group contains a cyclic subgroup of order r. We further show that when r is odd, an ideal class generating this subgroup does not come from the field's unique quadratic subfield. When r is odd, we show that the family of sextics contains infinitely many distinct fields whose class group contains a cyclic subgroup of order r generated by an ideal class which does not come from either the quadratic or cubic subfields of the sextic field. Finally, we extend and modify the techniques to handle a family of non-Galois cubic extensions of $\mathbb{Q}$. We prove that here too the result holds; this family contains infinitely many distinct fields whose class group contains a cyclic subgroup of order r.

ON THE DIVISIBILITY OF CLASS NUMBERS IN FAMILIES OF NUMBER FIELDS

by

David Lev Pincus

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
2021

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

Dedication

For Ari and Daphna,

and to the memory of Uncle Michael z″l.

Acknowledgments

I am indebted to many people for affording me this graduate experience, for making it such a pleasant one, and for their help in bringing this work to light. Thank you to my advisor Professor Lawrence C. Washington who first suggested this project, who took significant time every week to review and discuss my work, make suggestions, and who is such a good friend. Thank you to the University of Maryland Mathematics Department, both faculty and staff, for providing me with tremendous support in many ways for many years. In particular, I would like to extend a very big thank you to Professor James A. Schafer, Professor Jonathan M. Rosenberg, Professor Thomas J. Haines, and Professor William M. Goldman, who not only provided me with significant portions of my mathematical background but without whom this experience would not have been possible or successful.

My wife Yvonne and my parents Ruth and Roger have always encouraged me to pursue my dreams and have made all of this possible with their love and support. Indeed, the same is true of my entire family. Thank You!

Last, but in no way least, thank you to all of my friends for always being so good to me. I can always feel your love and support and it is invaluable to me.

Table of Contents

List of Tables

List of Figures

List of Symbols

f_n, $f_n(X)$	Polynomial whose roots generate the extension of interest
K_n	Splitting field of f_n
k_2	Quadratic subfield of K_n
k_3	A cubic subfield of K_n
$\mathcal{O}_{K_n}$, $\mathcal{O}_{k_3}$	Ring of integers
$\mathcal{O}_{K_n}^{\times}$, $\mathcal{O}_{k_3}^{\times}$	Group of Units
U, U_χ	Subgroups of $\mathcal{O}_{K_n}^{\times}$ or $\mathcal{O}_{k_3}^{\times}$
ρ, ρ_i	Roots of f_n; a unit
μ, μ_i	Units
ε	Fundamental unit of quadratic subfield
Cl_{K_n}	Class group of K_n
h_{K_n}	Class number of K_n

Chapter 1: Background and Introduction

The construction of the class group Cl_K of an algebraic number field K is well known; take the group of nonzero fractional ideals of K and mod out by those which are principal (i.e., generated by a single element of K.) It is equally well known that Cl_K is a finite group; its order is the class number of K and is denoted h_K. Since every ideal class has an integral representative, h_K gives a measure of how distant the ring of integers $\mathcal{O}_K$ is from a PID or, since $\mathcal{O}_K$ is a Dedekind domain, how distant the ring is from a UFD.

It is generally difficult to calculate the class group of a number field, although fields with small discriminant may be tackled using Minkowski's bound. Class numbers may be calculated using Dirichlet's analytic formula, but the calculation requires the knowledge of quantities, such as the regulator of the field, which may themselves be difficult to calculate.

Let $\mathcal{F}$ be a family of algebraic number fields. If $r > 1$ is an otherwise arbitrary integer one may ask the following question: Does there exist a field $K \in \mathcal{F}$ such that $r \mid h_K$? It is well known that the answer is affirmative in the case that $\mathcal{F}$ is the family of imaginary quadratic fields. In 1970 Yamamoto [16] showed that that the same is true when $\mathcal{F}$ is the

family of real quadratic fields and this was independently proved by Weinberger [15] in 1973.

In 1973 Uchida [13] asked and answered the same question for the following family of cubics: $\{K_n\}$, where K_n is the cyclic cubic field generated by adjoining to $\mathbb{Q}$ a zero of

$$f_n(X) = X^3 + nX^2 + 2nX + n.$$

He showed that for any positive integer r there is a cyclic cubic field in this family with class number a multiple of r. In 1987 Washington [14] proved a similar result by studying the family of simplest cubic fields $\{K_n\}$, where K_n is the cyclic cubic field generated by adjoining to $\mathbb{Q}$ a zero of

$$f_n(X) = X^3 + nX^2 - (n+3)X + 1.$$

In this work we mimic the techniques used by Washington [14] and others to answer the same question (and related questions) for families of cyclic quartics, cyclic sextics, and even for a family of non-Galois cubics; a family to which the techniques would appear, at first glance, not applicable.

In Chapter 2 we study the quartic case. Each such field is generated over $\mathbb{Q}$ by a zero of

$$f_n(X) = X^4 - nX^3 - 6X^2 + nX + 1.$$

Our main result shows that the resulting family contains infinitely many distinct fields, K_n, whose class group contains a cyclic subgroup of order r and further that this subgroup is generated by a class that does not come from an ideal class of the unique quadratic subfield of K_n.

In Chapter 3 we shift focus to the sextic case. Each such field is generated over $\mathbb{Q}$ by a zero of

$$f_n(X) = X^6 - 2nX^5 - (5n + 15)X^4 - 20X^3 + 5nX^2 + (2n + 6)X + 1.$$

Let $r \geq 1$ be an odd but otherwise arbitrary integer. Our main result shows that this family of sextics contains infinitely many distinct fields, K_n, whose class group contains a cyclic subgroup of order r generated by an ideal class that does not come from either the quadratic or cubic subfield of K_n.

Finally, in Chapter 4, we turn our attention to a non-Galois cubic family. Each field in the family is generated over $\mathbb{Q}$ by a zero of

$$f_n(X) := X^3 + nX^2 + nX - 1.$$

Let $r \geq 1$ be an otherwise arbitrary integer. Once again our main result shows that this family contains infinitely many distinct fields, K_n, whose class group contains a cyclic subgroup of order r.

The interest is that we are actually able to modify the techniques of the previous two chapters to apply to this family of non-Galois number fields. What makes this slightly surprising is that the techniques, as applied in Chapters 2 and 3, make regular use of the Galois group of K_n. But applying the Galois group of the sextic splitting field of the cubic polynomial $f_n(X)$ in this situation has the undesirable effect of moving us out of the cubic extension we are studying (and into an isomorphic cubic extension.) Nevertheless, by applying the splitting field's Galois group and then taking products of the resulting expressions, we find that the proofs emerge unscathed.

Chapter 2: A Family of Quartic Extensions of $\mathbb{Q}$.

We restrict attention in this chapter to the family of splitting fields, K_n, of polynomials of the form

$$f_n(X) = X^4 - nX^3 - 6X^2 + nX + 1,$$

where n is a nonzero integer not equal to ± 3. This family of quartic extensions was investigated by M.-N. Gras in [6]. Beginning with Remark 2.3 we will, without any loss of generality, restrict our attention to positive values of n.

Let $r \geq 1$ be an otherwise arbitrary integer. Our main result shows that this family of quartics contains infinitely many distinct fields, K_n, whose class group contains a cyclic subgroup of order r and further that this subgroup is generated by a class which does not come from an ideal class of the unique quadratic subfield of K_n.

2.1 Irreducibility of f_n.

Proposition 2.1. *$f_n(X)$ is irreducible over $\mathbb{Q}$.*

Proof. We begin by noting that n a nonzero integer and $n \neq \pm 3$ imply that $n^2 + 16$ is not a square.

To dispatch with the possibility that f_n has a linear factor, we note that the only possible roots of $f_n = 0$ in $\mathbb{Q}$ are ± 1, but $f_n(1) = f_n(-1) = -4 \neq 0$, and so f has no roots in $\mathbb{Q}$ and hence no linear factors.

To dispatch with the possibility that f_n splits as a product of two irreducible quadratics, we suppose that

$$f_n(X) = g(X)h(X),$$

where

$$g(X) = X^2 + aX + b, \text{ and}$$
$$h(X) = X^2 + cX + d,$$

with $g(X)$ and $h(X)$ irreducible over $\mathbb{Q}$ and $a, b, c, d \in \mathbb{Z}$. This gives us the following system:

$$bd = 1,\ (ad + bc) = n,\ (b + ac + d) = -6,\ (a + c) = -n$$

The first equation implies that $b = d = \pm 1$. If $b = d = 1$, then $n = 0$ and $n^2 + 16 = 16$ is a square. If $b = d = -1$, then the third equation says that $ac = -4$ and so there are six cases $(a, c) = (\pm 1, \mp 4), (\pm 2, \mp 2), (\pm 4, \mp 1)$, each of which leads to $n^2 + 16$ being either 25 or 16 and hence a square.

Since f_n does not have a linear factor and does not split into irreducible quadratics it is irreducible over $\mathbb{Q}$. □

2.2 Roots of f_n.

Lemma 2.2. *ρ is a root of $f_n(X) = 0$ if and only if $-\rho$ is a root of $f_{-n}(X) = 0$.*

Proof.

$$\begin{aligned} f_n(x) &= x^4 - nx^3 - 6x^2 + nx + 1 \\ &= (-x)^4 + n(-x)^3 - 6(-x)^2 - n(-x) + 1 \\ &= f_{-n}(-x). \end{aligned}$$

□

Remark 2.3. *Lemma 2.2 implies that $K_n = K_{-n}$, and so for this reason we will restrict our attention to positive values of the parameter n.*

Proposition 2.4. *The roots of $f_n(X) = 0$ are real. They are explicitly given by the*

formulae:

$$\begin{aligned}
\rho_0 &= \frac{1}{4}\left(n + \sqrt{\delta} + \sqrt{2}\sqrt{\delta + n\sqrt{\delta}}\right) \\
\rho_1 &= \frac{1}{4}\left(n - \sqrt{\delta} + \sqrt{2}\sqrt{\delta - n\sqrt{\delta}}\right) \\
\rho_2 &= \frac{1}{4}\left(n + \sqrt{\delta} - \sqrt{2}\sqrt{\delta + n\sqrt{\delta}}\right) \\
\rho_3 &= \frac{1}{4}\left(n - \sqrt{\delta} - \sqrt{2}\sqrt{\delta - n\sqrt{\delta}}\right),
\end{aligned}$$

where $\delta := n^2 + 16$.

Proof. The reality of the roots follows from the explicit formulae. To establish these formulae, divide each side of $f_n(\rho) = 0$ by ρ^2 to find that

$$\begin{aligned}
0 &= \rho^2 - n\rho - 6 + \frac{n}{\rho} + \frac{1}{\rho^2} \\
&= \left(\rho - \frac{1}{\rho}\right)^2 - n\left(\rho - \frac{1}{\rho}\right) - 4.
\end{aligned}$$

Hence

$$\rho - \frac{1}{\rho} = \frac{n \pm \sqrt{\delta}}{2},$$

and so

$$\rho^2 - \left(\frac{n \pm \sqrt{\delta}}{2}\right)\rho - 1 = 0.$$

Solving this last quadratic yields

$$\rho = \frac{1}{4}\left(n \pm \sqrt{\delta} \pm \sqrt{2}\sqrt{\delta \pm n\sqrt{\delta}}\right),$$

where the choice for the first ambiguous sign should match that of the third. □

Lemma 2.5. *ρ is a zero of f_n if and only if $(\rho-1)/(\rho+1)$ is a zero of f_n.*

Proof. The zeros of f_n coincide with those of the rational function with rule

$$\begin{aligned} g_n(X) &:= f_n(X)/X^2 \\ &= X^2 - nX - 6 + \frac{n}{X} + \frac{1}{X^2} \\ &= \left(X - \frac{1}{X}\right)^2 - n\left(X - \frac{1}{X}\right) - 4. \end{aligned}$$

Since

$$\begin{aligned} g_n\left(\frac{\rho-1}{\rho+1}\right) &= \left(\frac{\rho-1}{\rho+1} - \frac{\rho+1}{\rho-1}\right)^2 - n\left(\frac{\rho-1}{\rho+1} - \frac{\rho+1}{\rho-1}\right) - 4 \\ &= \left(\frac{-4\rho}{\rho^2-1}\right)^2 - n\left(\frac{-4\rho}{\rho^2-1}\right) - 4 \\ &= \frac{16\rho^2 + 4n\rho(\rho^2-1) - 4(\rho^2-1)^2}{(\rho^2-1)^2} \\ &= -4\frac{f_n(\rho)}{(\rho^2-1)^2}, \end{aligned}$$

we conclude that ρ is a zero of f_n if and only if $(\rho-1)/(\rho+1)$ is a zero of g_n if and only if $(\rho-1)/(\rho+1)$ is a zero of f_n. □

Proposition 2.6.

$$\rho_1 = (\rho_0 - 1)/(\rho_0 + 1)$$

$$\rho_2 = -1/\rho_0$$

$$\rho_3 = -1/\rho_1,$$

with $\rho_0 > 1 > \rho_1 > 0 > \rho_2 > -1 > \rho_0$.

Proof. Since ρ_0 is a root of $f_n(X) = 0$, successive applications of Lemma 2.5 imply that so are $(\rho_0 - 1)/(\rho_0 + 1)$, $-1/\rho_0$, and $-(\rho_0 + 1)/(\rho_0 - 1)$. Since $\rho_0 > 1$ (Proposition 2.4), we have

$$\rho_0 > 1 > (\rho_0 - 1)/(\rho_0 + 1) > 0 > -1/\rho_0 > -1 > -(\rho_0 + 1)/(\rho_0 - 1).$$

The explicit formulae of Proposition 2.4 show that $\rho_0\rho_2 = -1$. Hence $\rho_2 = -1/\rho_0$. Since $-(\rho_0+1)/(\rho_0-1)$ is the only remaining negative root and since ρ_3 is negative (Proposition 2.4), we conclude that $\rho_3 = -(\rho_0 + 1)/(\rho_0 - 1)$, and $\rho_1 = (\rho_0 - 1)/(\rho_0 + 1)$. □

Lemma 2.7. *For all* $n > 0$, $1/e < \rho_1(n) < e$, *while for* $n > 7$, $\rho_0(n) < n + 1$.

Proof. Since $\rho_0 = (n+\sqrt{n^2+16}+\sqrt{2}\sqrt{n^2+16+n\sqrt{n^2+16}})$ (Proposition 2.4), $\rho_0 \geq 9/4$ for $n \geq 1$. Hence $2/(\rho_0 - 1) \leq 8/5$ and so

$$e > 1 > \rho_1 = \frac{\rho_0 - 1}{\rho_0 + 1} = \frac{1}{1 + \frac{2}{\rho_0 - 1}} \geq \frac{1}{1 + 8/5} = \frac{5}{13} > 1/e,$$

for $n \geq 1$.

When $n > 7$, $n^2 + 16 < (n+1)^2$. Hence when $n > 7$,

$$\begin{aligned}
\rho_0(n) &= \left(n + \sqrt{n^2+16} + \sqrt{2}\sqrt{n^2+16+n\sqrt{n^2+16}}\right)/4 \\
&< \left(n + n + 1 + \sqrt{2}\sqrt{(n+1)^2 + n(n+1)}\right)/4 \\
&= \left(2n + 1 + \sqrt{2}\sqrt{(2n+1)(n+1)}\right)/4 \\
&= \left(2n + 1 + 2\sqrt{(n+1/2)(n+1)}\right)/4 \\
&< (2n + 1 + 2n + 2)/4 \\
&< n + 1.
\end{aligned}$$

□

2.3 $\mathrm{Gal}(f_n)$ and structure of the splitting field K_n.

Proposition 2.8. *Let K_n denote the splitting field of f_n. Then $K_n = \mathbb{Q}(\rho_0)$ and $\mathrm{Gal}(K_n/\mathbb{Q})$ is a cyclic group of order 4.*

Proof. Since $\rho_0 \in K_n$, $\mathbb{Q}(\rho_0) \subseteq K_n$. On the other hand, adjoining ρ_0 to $\mathbb{Q}$ adjoins the three remaining roots as well (Proposition 2.6) and so $f_n(X)$ splits into linear factors over $\mathbb{Q}(\rho_0)$. Hence $K_n = \mathbb{Q}(\rho_0)$ and $[K_n : \mathbb{Q}] = 4$. In particular, $|\mathrm{Gal}(K_n/\mathbb{Q})| = 4$. Since $\mathrm{Gal}(K_n/\mathbb{Q})$ acts transitively on the roots of f_n, there is an automorphism $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ for which

$$\sigma(\rho_0) = \rho_1 = (\rho_0 - 1)/(\rho_0 + 1).$$

Hence

$$\sigma^2(\rho_0) = \sigma(\rho_1) = \sigma(\rho_0 - 1)\sigma(\rho_0 + 1)^{-1} = (-2/(\rho_0 + 1))(2\rho_0/(\rho_0 + 1))^{-1} = -1/\rho_0 = \rho_2$$

$$\sigma^3(\rho_0) = \sigma(\rho_2) = -\sigma(\rho_0)^{-1} = -1/\rho_1 = \rho_3,$$

$$\sigma^4(\rho_0) = \sigma(\rho_3) = -\sigma(\rho_1)^{-1} = -1/\rho_2 = \rho_0,$$

and we conclude that $\mathrm{Gal}(K_n/\mathbb{Q})$ is cyclic generated by σ. □

Remark 2.9. *Let $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ denote the generator of the previous proposition. Then $\sigma^i(\rho_0) = \rho_i$, where the i should be read mod 4. Similarly, $\sigma(\rho_i) = \rho_{i+1}$, where the subscripts should be read mod 4.*

Corollary 2.10. *The splitting field K_n has a unique quadratic subfield $k_{2,n} = \mathbb{Q}(\sqrt{n^2+16})$.*

Proof. For the existence and uniqueness of the quadratic subfield note that $\mathbb{Z}/4\mathbb{Z}$ has a unique subgroup of order 2 and apply the Fundamental Theorem of Galois Theory. Since $2(\rho_0 + \rho_2) - n = \sqrt{n^2+16}$ (Proposition 2.4) and since the elements of the order two subgroup $\{1, \sigma^2\}$ each fix the element $2(\rho_0 + \rho_2) - n$ on the left hand side, we conclude that the right hand side $\sqrt{n^2+16} \in k_{2,n}$. Since $n^2 + 16$ is not a square when $n = 0, \pm 3$, we conclude that $\sqrt{n^2+16}$ is a primitive element for the quadratic extension $k_{2,n}/\mathbb{Q}$. □

Let $\sigma = (0123)$ as above. Then the lattice of subfields of K_n and the corresponding lattice of subgroups of $\mathbb{Z}/4\mathbb{Z} = \langle\sigma\rangle$ are given by the following diagrams:

Lemma 2.11. *When $n^2 + 16$ is square-free, $\mathrm{disc}(\mathcal{O}_{k_2}/\mathbb{Z}) = n^2 + 16$ and $\mathrm{disc}(\mathcal{O}_{K_n}/\mathbb{Z}) =$*

$$\begin{array}{ccc} K_n & & \langle 1 \rangle \\ | & & | \\ k_{2,n} = \mathbb{Q}(\sqrt{n^2+16}) & & \langle \sigma^2 \rangle \\ | & & | \\ \mathbb{Q} & & \langle \sigma \rangle = \mathbb{Z}/4\mathbb{Z} \end{array}$$

$(n^2+16)^3$.

Proof. If n^2+16 is square-free, then $n^2+16 \equiv 1 \mod 4$. Hence $\operatorname{disc}(\mathcal{O}_{k_2}/\mathbb{Z}) = n^2+16$. Since $\operatorname{disc}(\mathcal{O}_{K_n}/\mathbb{Z}) = \operatorname{disc}(\mathcal{O}_{k_2}/\mathbb{Z})^2 \cdot \mathfrak{N}_{k_2|\mathbb{Q}}(\operatorname{disc}(\mathcal{O}_{K_n}/\mathcal{O}_{k_2}))$ [12], we conclude that $(n^2+16)^2$ divides $\operatorname{disc}(\mathcal{O}_{K_n}/\mathbb{Z})$. But $\operatorname{disc}(f_n(X)) = (n^2+16)^3$ and since $\operatorname{disc}(f_n(X)) = [\mathcal{O}_{K_n} : \mathbb{Z}[\rho]]^2 \operatorname{disc}(\mathcal{O}_{K_n}/\mathbb{Z})$ and n^2+16 is square-free, we conclude that $\operatorname{disc}(\mathcal{O}_{K_n}/\mathbb{Z}) = (n^2+16)^3$. □

2.4 Units.

Since there are four real embeddings of K into $\mathbb{C}$ and no complex embeddings, Dirichlet's Unit Theorem implies that the rank of the unit group $\mathcal{O}_K^\times$ is 3. We already have three units: ρ_0, ρ_1, and the fundamental unit of the quadratic subfield ε. This section gives sufficient conditions for these units to form a fundamental set of units. It provides additional information about the units when the index of the subgroup they generate along with the torsion units ± 1 in the full group of units $\mathcal{O}_{K_n}^\times$ is even.

2.4.1 Regulator of $\{\varepsilon, \rho_0, \rho_1\}$

Proposition 2.12. *Let R' denote the regulator of $\{\varepsilon, \rho_0, \rho_1\}$. $R' = 2\log\varepsilon(\log^2\rho_0 + \log^2\rho_1)$, and $\{\varepsilon, \rho_0, \rho_1\}$ form a multiplicatively independent subset of $\mathcal{O}_{K_n}^\times$.*

Proof.

$$R' = \left| \det \begin{pmatrix} \log \rho_0 & \log \rho_1 & \log \varepsilon \\ \log \rho_1 & -\log \rho_0 & \log |\varepsilon^\sigma| \\ -\log \rho_0 & -\log \rho_1 & \log \varepsilon \end{pmatrix} \right|$$

$$= 2 \log \varepsilon \, (\log^2 \rho_0 + \log^2 \rho_1).$$

Since $\varepsilon > 1$ and $\rho_0 > 1$, we conclude that $R' > 0$. Hence $\{\varepsilon, \rho_0, \rho_1\}$ form a multiplicatively independent subset of the group of units. □

Lemma 2.13. *Let* $U := \langle -1, \varepsilon, \rho_0, \rho_1 \rangle \leq \mathcal{O}_K^\times$. *When* n^2+16 *is square-free,* $[\mathcal{O}_K^\times : U] \leq 2$.

Proof. The regulator of $\{\varepsilon, \rho_0, \rho_1\}$ is $2 \log \varepsilon \, (\log^2 \rho_0 + \log^2 \rho_1)$ (Proposition 2.12). Since we are assuming that $n^2 + 16$ is square-free, we know that $d_k := \operatorname{disc}(\mathcal{O}_k/\mathbb{Z}) = n^2 + 16$ and $d_K := \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = (n^2 + 16)^3$ (Lemma 2.11).

Letting R denote the regulator of K, we know from the work of Balady and Washington (Proposition 8) [1] that

$$\frac{R}{2 \log \varepsilon} > \frac{1}{8} \log^2 \left(\frac{D_K}{4.84 \, d_k^2} \right) = \frac{1}{8} \log^2 \left(\frac{n^2 + 16}{4.84} \right),$$

whenever $n > 11$. Since $[\mathcal{O}_K^\times : U] = R'/R$, we conclude that

$$\frac{1}{8} \log^2 \left(\frac{n^2 + 16}{4.84} \right) < \frac{R}{2 \log \varepsilon} = \frac{\log^2 \rho_0 + \log^2 \rho_1}{[\mathcal{O}_K^\times : U]},$$

or

$$[\mathcal{O}_K^\times : U] < 8\,\frac{\log^2 \rho_0 + \log^2 \rho_1}{\log^2\left(\frac{n^2+16}{4.84}\right)},$$

when $n > 11$. Since $\rho_0(n) < n+1$ for such n (Lemma 2.7) and since $e > \rho_1(n) > 1/e$ for such n (Lemma 2.7), we find that $\log^2 \rho_0(n) < \log^2(n+1)$ and that $\log^2 \rho_1(n) < 1$, whenever $n \geq 11$.

We conclude that for sufficiently large n,

$$\begin{aligned}
[\mathcal{O}_K^\times : U] &< 8\,\frac{\log^2 \rho_0 + \log^2 \rho_1}{\log^2\left(\frac{n^2+16}{4.84}\right)} \\
&< 8\frac{\log^2(n+1)+1}{\log^2\left(\frac{n^2+16}{4.84}\right)} \\
&< 8\frac{\log^2(n+1)+1}{\log^2\left(\frac{n}{2.2}\right)^2} \\
&= 2\frac{\log^2(n+1)+1}{\log^2\left(\frac{n}{2.2}\right)}.
\end{aligned}$$

Since $\frac{\log^2(n+1)+1}{\log^2\left(\frac{n}{2.2}\right)}$ is monotone decreasing for $n \geq 120$ and less than $3/2$ when $n = 121$, we conclude that $[\mathcal{O}_K^\times : U] \leq 2$ whenever $n \geq 120$. There are now only a finite number of cases remaining to check. We have used PARI to do so and present the results in the following table. $\square$

Table 2.1: Table of $[\mathcal{O}_K^\times : U]$ for $n \leq 121$ and $n^2 + 16$ square-free.

n	$[\mathcal{O}_K^\times : U]$	Prime factors of $\delta = n^2 + 16$	n	$[\mathcal{O}_K^\times : U]$	Prime factors of $\delta = n^2 + 16$
1	2	$17 = 17^1$	63	1	$3985 = 5^1 \times 797^1$
5	2	$41 = 41^1$	65	2	$4241 = 4241^1$
7	1	$65 = 5^1 \times 13^1$	67	1	$4505 = 5^1 \times 17^1 \times 53^1$
9	2	$97 = 97^1$	69	1	$4777 = 17^1 \times 281^1$
11	2	$137 = 137^1$	71	1	$5057 = 13^1 \times 389^1$
13	1	$185 = 5^1 \times 37^1$	73	1	$5345 = 5^1 \times 1069^1$
15	2	$241 = 241^1$	75	2	$5641 = 5641^1$
17	1	$305 = 5^1 \times 61^1$	77	1	$5945 = 5^1 \times 29^1 \times 41^1$
19	1	$377 = 13^1 \times 29^1$	79	2	$6257 = 6257^1$
21	2	$457 = 457^1$	81	2	$6577 = 6577^1$
23	1	$545 = 5^1 \times 109^1$	83	1	$6905 = 5^1 \times 1381^1$
25	2	$641 = 641^1$	85	1	$7241 = 13^1 \times 557^1$
27	1	$745 = 5^1 \times 149^1$	87	1	$7585 = 5^1 \times 37^1 \times 41^1$
29	2	$857 = 857^1$	89	2	$7937 = 7937^1$
31	2	$977 = 977^1$	91	2	$8297 = 8297^1$
33	1	$1105 = 5^1 \times 13^1 \times 17^1$	93	1	$8665 = 5^1 \times 1733^1$
35	2	$1241 = 17^1 \times 73^1$	95	2	$9041 = 9041^1$
37	1	$1385 = 5^1 \times 277^1$	99	2	$9817 = 9817^1$
39	1	$1537 = 29^1 \times 53^1$	101	2	$10217 = 17^1 \times 601^1$
41	2	$1697 = 1697^1$	105	1	$11041 = 61^1 \times 181^1$
43	1	$1865 = 5^1 \times 373^1$	107	1	$11465 = 5^1 \times 2293^1$
45	1	$2041 = 13^1 \times 157^1$	109	2	$11897 = 11897^1$
49	2	$2417 = 2417^1$	113	1	$12785 = 5^1 \times 2557^1$
51	2	$2617 = 2617^1$	115	2	$13241 = 13241^1$
55	2	$3041 = 3041^1$	117	1	$13705 = 5^1 \times 2741^1$
57	1	$3265 = 5^1 \times 653^1$	119	2	$14177 = 14177^1$
59	1	$3497 = 13^1 \times 269^1$	121	2	$14657 = 14657^1$
61	1	$3737 = 37^1 \times 101^1$			

2.4.2 Divisibility of the index $[\mathcal{O}_K^\times : U]$

Henceforth, let $n \geq 1$, $n \neq 3$ be otherwise arbitrary integers.

Lemma 2.14. *If* 2 *divides the index* $[\mathcal{O}_K^\times : U]$, *then*

1. $N_{k_2|\mathbb{Q}}(\varepsilon) = -1$

2. $\varepsilon\rho_0\rho_1 = \vartheta^2$ *for some unit* ϑ *of* K

3. $\vartheta^{1+\sigma^2} = \pm\varepsilon$

Proof. If $2 \mid [\mathcal{O}_K^\times : U]$, then there is a unit $u \in \mathcal{O}_K^\times \smallsetminus U$ such that

$$u^2 = \pm\varepsilon^a\rho_0^b\rho_1^c,$$

and without loss of generality we may take $a, b, c \in \{0, 1\}$. Since ε, ρ_0, and ρ_1 are all positive quantities, we see that we must choose the plus sign. Applying the four elements of the Galois group, we arrive at the following four equations:

$$u^2 = \varepsilon^a\rho_0^b\rho_1^c \quad (i)$$

$$(u^\sigma)^2 = (\varepsilon^\sigma)^a\rho_1^b\rho_2^c \quad (ii)$$

$$(u^{\sigma^2})^2 = \varepsilon^a\rho_2^b\rho_3^c \quad (iii)$$

$$(u^{\sigma^3})^2 = (\varepsilon^\sigma)^a\rho_3^b\rho_0^c \quad (iv)$$

If $N_{k_2|\mathbb{Q}}(\varepsilon) = 1$, then $\varepsilon\varepsilon^\sigma = 1$, and ε and ε^σ are both positive. Hence (ii) implies that $c = 0$, and (iii) then implies that $b = 0$. So $u^2 = \varepsilon^a$. If $a = 0$, then $u^2 = 1$ and we would reach the contradiction that $u = \pm 1 \in U$. Hence $a = 1$, and we conclude that ε is the square of a unit of K; say $\varepsilon = \vartheta^2$.

Applying σ we find that $(\vartheta^\sigma)^2 = \varepsilon^\sigma$. Hence

$$(\vartheta\vartheta^\sigma)^2 = \vartheta^2(\vartheta^\sigma)^2 = \varepsilon\varepsilon^\sigma = N_{k_2|\mathbb{Q}}(\varepsilon) = 1,$$

and so

$$\vartheta\vartheta^\sigma = \pm 1.$$

Note further that this last result implies that $\vartheta^{\sigma^2} = \vartheta$ and hence that $\vartheta \in k_2$. But ε is the fundamental unit of k_2. Hence $\vartheta = \varepsilon^a$ for some $a \in \mathbb{Z}$, and so $\varepsilon = \vartheta^2 = \varepsilon^{2a}$ for some $a \in \mathbb{Z}$; an obvious contradiction. We conclude that $N_{k_2|\mathbb{Q}}(\varepsilon) \neq 1$ and hence that $N_{k_2|\mathbb{Q}}(\varepsilon) = -1$.

Since $N_{k_2|\mathbb{Q}}(\varepsilon) = -1$, ε and ε^σ have opposite signs and $\varepsilon^\sigma < 0$. From (ii) $a = c$ and from (iii) $b = c$. Hence $a = b = c$. If $a = b = c = 0$, then $a = 0$, and we reach the contradiction that $u = \pm 1 \in U$. We conclude $a = b = c = 1$ and hence that

$$u^2 = \varepsilon\rho_0\rho_1.$$

In other words, $\varepsilon\rho_0\rho_1$ is the square of a unit of K; say $\varepsilon\rho_0\rho_1 = \vartheta^2$, where ϑ is a unit of K.

Taking norms down to the quadratic subfield of both sides of the equation $\varepsilon\rho_0\rho_1 = \vartheta^2$ leads us to conclude that $(N_{K|k_2}(\vartheta))^2 = \varepsilon^2$. Hence

$$N_{K|k_2}(\vartheta) = \pm\varepsilon.$$

□

Corollary 2.15. *Suppose that $d_k = n^2 + 16$ is square-free. If $N_{k_2|\mathbb{Q}}(\varepsilon) = 1$ or if $\varepsilon\rho_0\rho_1$ is not the square of a unit of K, then $\{\varepsilon, \rho_0, \rho_1\}$ forms a fundamental system of units for K.*

Proof. Almost immediate. From the contrapositive of Lemma 2.14, 2 does not divide the index $[\mathcal{O}_K^\times : U]$. But when $d_k = n^2 + 16$ is square-free $[\mathcal{O}_K^\times : U] \leq 2$ (Lemma 2.13). Hence $[\mathcal{O}_K^\times : U] = 1$. □

Lemma 2.16. *The greatest power of 2 that may divide the index $[\mathcal{O}_K^\times : U]$ is 2.*

Proof. Let $U_\chi := \{u \in \mathcal{O}_K \mid N_{K|k_2}(u) = \pm 1\}$ denote the group of relative units of K and let $U_2 := \mathcal{O}_{k_2}$ denote the units of the quadratic subfield. Let $Q := [\mathcal{O}_K^\times : U_\chi U_2]$, so that

$$\begin{aligned}[\mathcal{O}_K^\times : U] &= [\mathcal{O}_K^\times : U_\chi U_2][U_\chi U_2 : U] \\ &= Q\,[U_\chi U_2 : U]\,.\end{aligned}$$

By a theorem of Hasse [8, 11] we know that $Q \leq 2$ for any real cyclic quartic field K. We now show that $[U_\chi U_2 : U]$ is odd. There is a group homomorphism $U_\chi \to U_\chi U_2/U$ sending $u \mapsto (u \cdot 1)U$. Since $U_2 \subset U$, this homomorphism is surjective. Finally, since $\langle -1, \rho_0, \rho_1\rangle \subset U$, it is clear that this epimorphism factors through the quotient $U_\chi/\langle -1, \rho_0, \rho_1\rangle$. By way of contradiction, suppose that 2 divides $[U_\chi : \langle -1, \rho_0, \rho_1\rangle]$. Then there is $v \in U_\chi \smallsetminus \langle -1, \rho_0, \rho_1\rangle$ such that

$$v^2 = \pm\rho_0^a\rho_1^b,$$

for some integers a, b. Since ρ_0 and ρ_1 are positive, it is clear that we must choose the plus sign and, without loss of generality, we may take $a, b \in \{0, 1\}$. Applying σ and σ^2 we find that

$$(v^{\sigma})^2 = \rho_1^a \rho_2^b$$

$$(v^{\sigma^2})^2 = \rho_2^a \rho_3^b.$$

Since $\rho_1 > 0$, while $\rho_2, \rho_3 < 0$, these equations imply that $a = b = 0$. We conclude that $v^2 = 1$. Hence $v = \pm 1 \in \langle -1, \rho_0, \rho_1 \rangle$ and we have arrived at a conclusion which contradicts our choice of v. Thus $[U_\chi : \langle -1, \rho_0, \rho_1 \rangle]$ is odd. The epimorphism form $U_\chi / \langle -1, \rho_0, \rho_1 \rangle$ onto $U_\chi U_2 / U$, implies that $[U_\chi U_2 : U]$ divides $[U_\chi : \langle -1, \rho_0, \rho_1 \rangle$ and hence that $[U_\chi U_2 : U]$ is also odd. Since $Q \leq 2$, we conclude that $[\mathcal{O}_k^\times : U] \not\equiv 0 \mod 4$. □

2.5 Conditions sufficient to conclude that $r \mid h_K$ for a given $r > 1$.

A method for showing that r divides the class number of K is to show that the class group contains an element of order r. A straightforward method for doing so is to begin with a principal ideal of K, show that it factors as an rth power of an ideal $\mathfrak{a}$, and then show that no lesser power of $\mathfrak{a}$ is principal.

In Washington's work on class numbers of the simplest cubic fields [14], the principal ideal which factors as an rth power is $(x - \rho)$, where ρ is a root of the cubic polynomial $X^3 + nX^2 - (n + 3)X + 1$, and (x, y) is a rational point on the curve $Y^r =$

$X^3 + nX^2 - (n+3)X + 1$. To show that no smaller power of the resulting ideal is principal x is fixed to be equal to -1, so that $y^r = 2n + 3$.

The analogous situation here would be to look at $(x - \rho_0)$ where (x, y) is a rational point on the curve $Y^r = f_n(X)$. Unfortunately we encountered difficulty when we fixed x and searched for y such that $y^r = f_n(x)$. For example, when we fixed $x = -2$, we found that $y^r = 6n - 7$; an equation which has no solutions when r is even since -1 is not a square mod 3.

We were thus led to consider other primitive elements α for the extension $K_n/\mathbb{Q}$ along with their minimal polynomials $m_\alpha(X)$ and to consider factoring $(x - \alpha)$ and finding solutions to $Y^r = m_\alpha(X)$.

2.5.1 Candidate for a representative of a class of order r

Lemma 2.17. *Let $\alpha := a\rho_0 + b\rho_1$ with $a, b \in \mathbb{Z}$. If $a \neq 0$ or $b \neq 0$, then α is a primitive element for $K/\mathbb{Q}$ with minimal polynomial*

$$\begin{aligned} m_{a,b}(X) = X^4 - (a+b)nX^3 + (abn^2 + (-6a^2 + 4ab - 6b^2))X^2 \\ + ((-a^2b + ab^2)n^2 + (a^3 + 3a^2b + 3ab^2 + b^3)n + (-16a^2b + 16ab^2))X \\ + (-a^2b^2n^2 + (a^4 + 4a^3b - 10a^2b^2 + 4ab^3 + b^4)). \end{aligned} \tag{2.1}$$

Proof. Suppose, by way of contradiction, that α is not a primitive element for $K/\mathbb{Q}$. Then

$\alpha \in k$ and is fixed by σ^2. Since $\sigma^2(\alpha) = a\rho_2 + b\rho_3$, we conclude that $a(\rho_0 - \rho_2) + b(\rho_1 - \rho_3) = 0$. Therefore $a = 0$ if and only if $b = 0$ (since $\rho_i - \rho_{i+2} > 0$ when $i = 1, 2$.) Since we are assuming that either a or b is nonzero, we are forced to conclude that each is nonzero. Hence $(\rho_0 - \rho_2)/(\rho_1 - \rho_3) = -b/a \in \mathbb{Q}$ and so is fixed by σ. But then this quantity equals its negative reciprocal which leads to the conclusion that $(\rho_0 - \rho_2)/(\rho_1 - \rho_3)$ is a solution to $X^2 + 1 = 0$. Since $(\rho_0 - \rho_2)/(\rho_1 - \rho_3) \in \mathbb{R}$ this is an impossibility. We conclude that $K = \mathbb{Q}(\alpha)$.

Using the fact that $\rho_0^4 = n\rho_0^3 + 6\rho_0^2 - n\rho_0 - 1$, the matrix representing multiplication by $a\rho_0$ with respect to the ordered power basis $\{1, \rho_0, \rho_0^2, \rho_0^3\}$ for $K/\mathbb{Q}$ is

$$M := \begin{pmatrix} 0 & 0 & 0 & -a \\ a & 0 & 0 & -na \\ 0 & a & 0 & 6a \\ 0 & 0 & a & na \end{pmatrix}.$$

Since

$$
\begin{aligned}
4 &= 4 + 0\rho_0 + 0\rho_0^2 + 0\rho_0^3 \\
4\rho_1 &= 4\left(\frac{\rho_0 - 1}{\rho_0 + 1}\right) \\
&= (\rho_0 - 1)(\rho_0^3 - (n+1)\rho_0^2 + (n-5)\rho_0 + 5) \\
&= -6 + (10 - 2n)\rho_0 + (2n+2)\rho_0^2 - 2\rho_0^3 \\
4\rho_1^2 &= (-2n + 12) + (-2n^2 + 10n - 28)\rho_0 + (2n^2 - 2n)\rho_0^2 + (4 - 2n)\rho_0^3 \\
4\rho_1^3 &= (-2n^2 + 8n - 30) + (-2n^3 + 10n^2 - 38n + 70)\rho_0 \\
&\quad + (2n^3 - 2n^2 + 14n + 10)\rho_0^2 + (-2n^2 + 4n - 14)\rho_0^3,
\end{aligned}
$$

the matrix representing the change of coordinates from those based on powers of ρ_1 to those based on powers of ρ_0 is given by

$$
C := \frac{1}{4}\begin{pmatrix}
4 & -6 & -2n + 12 & -2n^2 + 8n - 30 \\
0 & 10 - 2n & -2n^2 + 10n - 28 & -2n^3 + 10n^2 - 38n + 70 \\
0 & 2n + 2 & 2n^2 - 2n & 2n^3 - 2n^2 + 14n + 10 \\
0 & -2 & 4 - 2n & -2n^2 + 4n - 14
\end{pmatrix}.
$$

Its inverse is

$$C^{-1} = \begin{pmatrix} 1 & 3/2 & n/2+3 & n^2/2+2n+15/2 \\ 0 & n/2+5/2 & n^2/2+5n/2+7 & n^3/2+5n^2/2+19n/2+35/2 \\ 0 & n/2-1/2 & n^2/2+n/2 & n^3/2+n^2/2+7n/2-5/2 \\ 0 & -1/2 & -n/2-1 & -n^2/2-n-7/2. \end{pmatrix}$$

Thus the matrix representing multiplication by $b\rho_1$ with respect to the basis consisting of powers of ρ_0 is

$$\begin{aligned} N &= C \begin{pmatrix} 0 & 0 & 0 & -b \\ b & 0 & 0 & -nb \\ 0 & b & 0 & 6b \\ 0 & 0 & b & nb \end{pmatrix} C^{-1} \\ &= \frac{b}{2} \begin{pmatrix} -3 & 1 & -1 & 1 \\ 5-n & n-3 & 1-n & n-1 \\ n+1 & -n-1 & n+3 & -n-5 \\ -1 & 1 & -1 & 3 \end{pmatrix}, \end{aligned}$$

and so the matrix representing multiplication by $a\rho_0 + b\rho_1$ with respect to our ordered ρ_0

power basis is

$$M+N=\begin{pmatrix} -3b/2 & b/2 & -b/2 & -a+b/2 \\ a+(5-n)b/2 & (n-3)b/2 & (1-n)b/2 & -na+(n-1)b/2 \\ (n+1)b/2 & a+(-n-1)b/2 & (n+3)b/2 & 6a+(-n-5)b/2 \\ -b/2 & b/2 & a-b/2 & na+3b/2 \end{pmatrix}.$$

Since $m_{a,b}(X)$ is of degree 4 and divides the characteristic polynomial of $M+N$, we calculate the latter and conclude that

$$\begin{aligned} m_{a,b}(X) = X^4 &- (a+b)nX^3 + (abn^2 + (-6a^2+4ab-6b^2))X^2 \\ &+ ((-a^2b+ab^2)n^2 + (a^3+3a^2b+3ab^2+b^3)n + (-16a^2b+16ab^2))X \\ &+ (-a^2b^2n^2 + (a^4+4a^3b-10a^2b^2+4ab^3+b^4)). \end{aligned}$$

□

Remark 2.18. *The coefficient of n^2 in $m_{a,b}(X)$ is $abX^2+(-a^2b+ab^2)X-a^2b^2$. Therefore setting $X=-b$ or $X=a$ in $m_{a,b}(X)$ yields a linear expression in n.*

Lemma 2.19. *Suppose that $(-b,y)$ is a solution in integers to $Y^r = m_{a,b}(X)$. Assume that any prime factor of y splits completely in K and that no such factor divides the discriminant of $m_{a,b}(X)$. Then $(-b-\alpha)$ is the rth power of an ideal of K.*

Proof. From the hypotheses we have that

$$y^r = m_{a,b}(-b) = (-b-\alpha)(-b-\alpha^{\sigma})(-b-\alpha^{\sigma^2})(-b-\alpha^{\sigma^3}).$$

Let

$$(-b-\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}},$$

be the unique factorization of the integral ideal $(-b-\alpha)$ into a product of positive integer powers of prime ideals and let p be the rational prime below $\mathfrak{p}$.

Write $(p) = \mathfrak{p}\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$. Each of these four prime ideals over p must contain exactly one of the conjugates of $-b-\alpha$, since otherwise one of these prime ideals would contain $\mathrm{disc}(m_{a,b}(X))$ and p would divide $\mathrm{disc}(m_{a,b}(X))$; a contradiction to our hypothesis on primes dividing y. Hence $p^{\nu_{\mathfrak{p}}}$ exactly divides y^r, and so $r \mid \nu_{\mathfrak{p}}$.

Thus $(-b-\alpha)$ is the rth power of the ideal

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}/r}.$$

□

2.5.2 The behavior of primes revisited.

Henceforth we set $a = 1$ and $b = -3$, so that

$$\alpha = \rho_0 - 3\rho_1.$$

We also let $m_\alpha(X)$ denote the minimal polynomial of α over $\mathbb{Q}$.

Lemma 2.20. *Let* $(3, y)$ *be a solution in integers to* $Y^r = m_\alpha(X)$. *Then* $\gcd(30, y) = 1$ *and the only possible prime common divisors of* y *and* $\mathrm{disc}(m_\alpha(X))$ *are* $7, 13$, *and* 41.

Proof. Substitute into $a = 1, b = -3$, into Equation (2.1) to find that

$$m_\alpha(X) = X^4 + 2nX^3 + (-3n^2 - 72)X^2 + (12n^2 - 8n + 192)X + (-9n^2 - 128),$$

and note that

$$\mathrm{disc}(m_\alpha(X)) = 16(3n - 16)^2(6n - 7)^2(n^2 + 16)^3.$$

Substitute $X = 3$ into $m_\alpha(X)$ to find that

$$y^{2r} = 30n - 119.$$

If $q = 2, 3$, or 5 divides y, then $1 \equiv 0 \mod q$; an impossibility. Hence $\gcd(30, y) = 1$. We see that any prime common divisor, q, of $\mathrm{disc}(m_\alpha(X))$ and y^r yields a pair of

congruences

$$16(3n-16)^2(6n-7)^2(n^2+16)^3 \equiv 0 \mod q$$
$$30n - 119 \equiv 0 \mod q.$$

Since $\gcd(30, q) = 1$ the linear congruence has the unique solution $n \equiv 119/30 \mod q$. Substituting into the first congruence then reveals that $q = 7, 13,$ or 41. We conclude that the only possible prime common divisors of y and $\mathrm{disc}(m_\alpha(X))$ are $7, 13,$ and 41. □

Lemma 2.21. *Let $(3, y)$ be a solution in integers to $Y^r = m_\alpha(X)$. Any prime divisor $q \neq 13$ of y splits completely in K.*

Proof. Let q be a prime divisor of $y^r = (3-\alpha)(3-\alpha^\sigma)(3-\alpha^{\sigma^2})(3-\alpha^{\sigma^3})$. Choose a prime $\mathfrak{q}$ over q such that $3 \equiv \alpha \mod \mathfrak{q}$. Then

$$\rho_0 \equiv 3(1+\rho_1) \equiv 3\left(1 + \frac{\rho_0 - 1}{\rho_0 + 1}\right) \equiv 3\left(\frac{2\rho_0}{\rho_0+1}\right) \mod \mathfrak{q}.$$

Hence

$$\rho_0 \equiv 5 \mod \mathfrak{q},$$

and

$$\begin{aligned} \rho_1 &= \frac{\rho_0 - 1}{\rho_0 + 1} \equiv \frac{2}{3} \mod \mathfrak{q} \\ \rho_2 &= -\frac{1}{\rho_0} \equiv -\frac{1}{5} \mod \mathfrak{q} \\ \rho_3 &= -\frac{1}{\rho_1} \equiv -\frac{3}{2} \mod \mathfrak{q}. \end{aligned} \tag{2.2}$$

The Galois group acts on the set of primes over q. If σ^2 stabilized $\mathfrak{q}$, then $\alpha \equiv \alpha^{\sigma^2} \mod \mathfrak{q}$, and so

$$5 + \frac{1}{5} - 3\left(\frac{2}{3} + \frac{3}{2}\right) \equiv 0 \mod \mathfrak{q}.$$

Since this implies that

$$13 \equiv 0 \mod q,$$

we conclude that any prime divisor $q \neq 13$ of y splits completely in K. □

2.5.3 Divisibility of the index $[\mathcal{O}_K^\times : U]$ redux.

Lemma 2.22. *Let ℓ be an odd prime and q a prime for which exactly two elements of the set $\{2, 3, 5\}$ are ℓth power residues mod q, while the third is an ℓth power nonresidue mod q. Assume that $\mathfrak{q}$ is a prime over q such that $\rho_0 \equiv 5 \mod \mathfrak{q}$, and that q splits completely in K. Then ℓ does not divide $[\mathcal{O}_K^\times : U]$, where $U = \langle -1, \varepsilon, \rho_0, \rho_1 \rangle$.*

Proof. As in Equation (2.2), $\rho_1 \equiv 2/3$, $\rho_2 \equiv -1/5$, and $\rho_3 \equiv -3/2 \mod \mathfrak{q}$.

If ℓ is an odd prime and divides $[\mathcal{O}_K^\times : U]$, then there is a unit $u \in \mathcal{O}_K^\times \smallsetminus U$ such that

$$u^\ell = \pm \varepsilon^a \rho_0^b \rho_1^c.$$

Without loss of generality we may take each integer exponent $0 \leq a, b, c < \ell$ and, since ℓ is odd, take

$$u^\ell = \varepsilon^a \rho_0^b \rho_1^c. \quad (**)$$

Applying $1+\sigma \in \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ to both sides of $(**)$ we conclude that

$$\begin{aligned}(uu^{\sigma})^{\ell} &= (\varepsilon\varepsilon^{\sigma})^{a}(\rho_0\rho_1)^{b}(\rho_1\rho_2)^{c} \\ &= (\pm 1)^{a}(\rho_0\rho_1)^{b}(\rho_1\rho_2)^{c} \\ &\equiv (\pm 1)^{a}(-1)^{c}5^{b-c}2^{b+c}3^{-(b+c)} \mod \mathfrak{q}.\end{aligned}$$

Similarly, by applying $\sigma(1+\sigma) \in \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ to both sides of $(**)$, we find that

$$\begin{aligned}(u^{\sigma}u^{\sigma^2})^{\ell} &= (\pm 1)^{a}(\rho_1\rho_2)^{b}(\rho_2\rho_3)^{c} \\ &\equiv (\pm 1)^{a}(-1)^{c}2^{b-c}3^{-(b-c)}5^{-(b+c)} \mod \mathfrak{q}.\end{aligned}$$

Using our power residue hypotheses, one of these congruences implies that $b \equiv -c \mod \ell$, while the other implies that $b \equiv c \mod \ell$. Hence $b \equiv c \equiv 0 \bmod \ell$, and so $b = c = 0$. Thus $u^{\ell} = \varepsilon^{a}$. If $u^{\sigma^2} \neq u$ then, noting that $u, u^{\sigma^2} \in \mathbb{R}$ and that ℓ is odd, we conclude that $(u^{\sigma^2})^{\ell} \neq u^{\ell}$. Hence $\varepsilon^{a} = u^{\ell} \neq (u^{\ell})^{\sigma^2} = (\varepsilon^{a})^{\sigma^2} = \varepsilon^{a}$; a contradiction. We conclude that $u^{\sigma^2} = u$, and hence that $u \in \mathcal{O}_K^{\times} \cap k_2 \subset U$. This result contradicts the fact that $u \notin U$, and so we conclude that ℓ is relatively prime to $[\mathcal{O}_K^{\times} : U]$. □

2.5.4 A class of order r

Proposition 2.23. *Let $n > 3$. Then $(3-\alpha)$ is not the square of a principal ideal.*

Proof. Arguing by contradiction, suppose that $(3-\alpha) = (\beta)^2$, so that $-\rho_0 + 3(1+\rho_1) = u\beta^2$, where u is a unit of K. We consider the two cases in which $[\mathcal{O}_K^{\times} : U]$ is even or odd separately.

If $[\mathcal{O}_K^\times : U]$ is odd, then there are integers s and t such that $u = u^{s[\mathcal{O}_K^\times:U]}u^{2t}$. Hence $-\rho_0 + 3(1+\rho_1) = \pm\varepsilon^a\rho_0^b\rho_1^c\beta_1^2$, where $\beta_1 = u^t\beta$. Since $n > 3$, the left hand side is negative and we see that we must choose the negative sign on the right hand side. By absorbing any squares into β_1, we may assume without loss of generality that $a, b, c \in \{0, 1\}$. Thus we arrive at the equation

$$\rho_0 - 3\rho_1 - 3 = \varepsilon^a\rho_0^b\rho_1^c\beta_2^2.$$

Taking norms down to $\mathbb{Q}$ of both sides of this equation, we arrive at the contradiction that $-9n^2 - 128 = N_{K|\mathbb{Q}}(\beta_2)^2$; i.e., that $-128 - 9n^2 < 0$ is the square of a rational number.

If $[\mathcal{O}_K^\times : U]$ is even, then we know from Lemma 2.14 that $N_{k_2|\mathbb{Q}}(\varepsilon) = -1$ and that $\varepsilon\rho_0\rho_1$ is the square of a unit of K, say $\varepsilon\rho_0\rho_1 = \vartheta^2$. The subgroup $U' = \langle -1, \vartheta, \rho_0, \rho_1\rangle \subset \mathcal{O}_K^\times$ properly contains the subgroup $U = \langle -1, \varepsilon, \rho_0, \rho_1\rangle$, and the quotient U'/U is generated by the class of ϑ; an element of order 2. Hence $[U' : U] = 2$. Since we know from Lemma 2.16 that the greatest power of 2 which may divide

$$[\mathcal{O}_K^\times : U] = [\mathcal{O}_K^\times : U'][U' : U] = 2[\mathcal{O}_K^\times : U']$$

is 2, we conclude that $[\mathcal{O}_K^\times : U']$ is odd.

Thus, working as above, $-\rho_0 + 3\rho_1 + 3 = u\beta^2$ implies that $-\rho_0 + 3\rho_1 + 3 = \pm\vartheta^a\rho_0^b\rho_1^c\beta_1^2$. Without loss of generality, we may assume that $\vartheta > 0$. (We require only that ϑ is a square

root of $\varepsilon\rho_0\rho_1$, so choose the positive square root.) Since $-\rho_0 + 3\rho_1 + 3 < 0$, we see that we must choose the negative sign on the right. By absorbing any squares into β_1, we may take $a, b, c \in \{0, 1\}$, and upon applying the elements of the Galois group we now arrive at the four equations:

$$\rho_0 - 3\rho_1 - 3 = \vartheta^a \rho_0^b \rho_1^c \beta_2^2 \tag{2.3}$$

$$\rho_1 - 3\rho_2 - 3 = (\vartheta^\sigma)^a \rho_1^b \rho_2^c (\beta_2^\sigma)^2 \tag{2.4}$$

$$\rho_2 - 3\rho_3 - 3 = (\vartheta^{\sigma^2})^a \rho_2^b \rho_3^c (\beta_2^{\sigma^2})^2 \tag{2.5}$$

$$\rho_3 - 3\rho_0 - 3 = (\vartheta^{\sigma^3})^a \rho_3^b \rho_0^c (\beta_2^{\sigma^3})^2. \tag{2.6}$$

Since $\vartheta^2 = \varepsilon\rho_0\rho_1$, $(\vartheta^\sigma)^2 = \varepsilon^\sigma \rho_1\rho_2$. Noting that $\varepsilon\varepsilon^\sigma = N_{k_2|\mathbb{Q}}(\varepsilon) = -1$ (Lemma 2.14), we find that $(\vartheta\vartheta^\sigma)^2 = -\rho_0\rho_1^2\rho_2 = \rho_1^2$, and so

$$\vartheta\vartheta^\sigma = \pm\rho_1.$$

If $\vartheta\vartheta^\sigma = +\rho_1$, then Galois conjugating:

$$\vartheta\vartheta^\sigma = \rho_1$$

$$\vartheta^\sigma\vartheta^{\sigma^2} = \rho_2$$

$$\vartheta^{\sigma^2}\vartheta^{\sigma^3} = \rho_3$$

$$\vartheta^{\sigma^3}\vartheta = \rho_0$$

Since ϑ and ρ_1 are both positive, we conclude from the first equation that so is ϑ^σ. Then

the second equation implies that $\vartheta^{\sigma^2} < 0$, and the third equation implies that $\vartheta^{\sigma^3} > 0$. Noting that (when $n > 3$)

$$\rho_0 - 3\rho_1 - 3 > 0$$

$$\rho_1 - 3\rho_2 - 3 < 0$$

$$\rho_2 - 3\rho_3 - 3 > 0$$

$$\rho_3 - 3\rho_0 - 3 < 0$$

Equations (2.4) and (2.6) now reveal that $b = c = 1$. If $a = 1$, then the left hand side of Equation (2.5) would be positive while the right hand side is negative. Hence $a = 0$ and we may write

$$\rho_0 - 3\rho_1 - 3 = \rho_0^b \rho_1^c \beta_2^2.$$

Taking norms down to $\mathbb{Q}$, we again arrive at the contradiction that $-128-9n^2 = N_{K|\mathbb{Q}}(\beta_2)^2$; i.e., that $-9n^2 - 128 < 0$ is the square of a rational number.

On the other hand, if $\vartheta\vartheta^\sigma = -\rho_1$, then Galois conjugating:

$$\vartheta\vartheta^\sigma = -\rho_1$$

$$\vartheta^\sigma\vartheta^{\sigma^2} = -\rho_2$$

$$\vartheta^{\sigma^2}\vartheta^{\sigma^3} = -\rho_3$$

$$\vartheta^{\sigma^3}\vartheta = -\rho_0,$$

and we conclude that $\vartheta^{\sigma} < 0$, $\vartheta^{\sigma^2} < 0$, and $\vartheta^{\sigma^3} < 0$. If $a = 0$, then by taking norms down to $\mathbb{Q}$ we run into the same contradiction that we've already encountered twice above. Hence $a = 1$. But then equation (2.4) implies that $c = 0$ and equation (2.6) implies that $b = 0$. Hence from Equation (2.5), $\rho_2 - 3\rho_3 - 3 = \vartheta^{\sigma^2}(\beta_2^{\sigma^2})^2$. Since the left hand side of this equation is positive, while the right hand side is negative, we've reached a contradiction.

We have exhausted the possibilities and so are forced to conclude that our initial assumption was false and hence that $(3 - \alpha)$ is not the square of a principal ideal. □

Proposition 2.24. *Let r be a positive integer and let $(3, y)$ be a solution in integers to $Y^r = m_\alpha(X)$. Let ℓ be an odd prime divisor of r and let q, q_2 be prime divisors of y not equal to $7, 13,$ or 41 and satisfying the following conditions:*

1. *Exactly two of the primes $2, 3, 5$ are ℓth power residues mod q, while the third is a ℓth power nonresidue mod q.*
2. *All three of the primes $2, 3, 5$ are ℓth power residues mod q_2, while 13 is an ℓth power nonresidue mod q_2.*

Then $(3 - \alpha)$ is not the ℓth power of a principal ideal.

Proof. Again we proceed by contradiction and suppose that $(3 - \alpha) = (\beta)^\ell$, so that $-\rho_0 + 3(1 + \rho_1) = u\beta^\ell$, where u is a unit of K.

The primes q, q_2 totally split in K (Lemma 2.21) and neither divides $\mathrm{disc}(m_\alpha(X))$ (Lemma 2.20). Hence we choose primes $\mathfrak{q}$ (resp. $\mathfrak{q}_2$) over q (resp. q_2) such that $3 \equiv \alpha \mod \mathfrak{q}, \mathfrak{q}_2$.

Then $\rho_0 \equiv 5$, $\rho_1 \equiv 2/3$, $\rho_2 \equiv -1/5$, $\rho_3 \equiv -3/2 \mod \mathfrak{q}, \mathfrak{q}_2$ (Equation (2.2)).

Since ℓ is odd, we know from Lemma 2.22 above that $\gcd([\mathcal{O}_K^\times : U], \ell) = 1$. Hence there are integers s and t such that $u = (u^s)^{[\mathcal{O}_K^\times : U]}(u^t)^\ell$ and hence such that

$$-\rho_0 + 3(1 + \rho_1) = \pm\varepsilon^a \rho_0^b \rho_1^c \beta_1^\ell,$$

where ε is the fundamental unit of the quadratic subfield and where $\beta_1 = \beta u^t$.

If $-N_{K|\mathbb{Q}}(\rho_0 - 3(1 + \rho_1)) = n^2 + 128$ is not an ℓth power in $\mathbb{Z}$, then we are done and may conclude that $(3 - \alpha) \neq (\beta)^\ell$.

If not, then by applying σ and σ^2 to both sides of these equations we find that

$$-\rho_1 + 3(1 + \rho_2) = \pm(\varepsilon^\sigma)^a \rho_1^b \rho_2^c (\beta_1^\sigma)^\ell$$
$$-\rho_2 + 3(1 + \rho_3) = \pm\varepsilon^a \rho_2^b \rho_3^c (\beta_1^{\sigma^2})^\ell,$$

and upon multiplying these two equations and using the congruences above, we find that

$$-\frac{169}{75} \equiv (\pm 1)^a (-1)^c (2/3)^{b-c} (-1/5)^{b+c} (\beta_1^\sigma \beta_1^{\sigma^2})^\ell \mod \mathfrak{q}_2,$$

or that

$$13^2 \equiv (\pm 1)^a (-1)^{1+b} 2^{b-c} 3^{1-b+c} 5^{2-b-c} (\beta_1^\sigma \beta_1^{\sigma^2})^\ell \mod \mathfrak{q}_2.$$

By absorbing any factors of -1 into the ℓth power and applying our assumptions regarding ℓth power residues, we conclude that 13^2 is an ℓth power mod $\mathfrak{q}_2$. Since q_2 splits completely in K, the degree of the residue field $[\mathcal{O}_K/\mathfrak{q}_2 : \mathbb{Z}/q_2\mathbb{Z}] = 1$. So 13^2 is an ℓth power residue mod $\mathfrak{q}_2$ if and only if it is an ℓth power residue mod q_2; say $\gamma^\ell \equiv 13^2 \bmod q_2$. Since ℓ is odd, there are integers s and t such that $2s + \ell t = 1$ and hence such that

$$13 = 13^{2s+\ell t} = 13^{2s}13^{\ell t} \equiv \gamma^{\ell s}13^{\ell t} \mod q_2 = (\gamma^s 13^t)^\ell \mod q_2.$$

By hypothesis 13 is an ℓth power nonresidue mod q_2; contradiction. □

Corollary 2.25. *Let $n > 3$, let r be a positive integer, and let $(3, y)$ be a solution in integers to $Y^r = m_\alpha(X)$. Assume that $7, 13$, and 41 do not divide y. Assume further that for each odd prime divisor ℓ of r there are corresponding prime divisors q, q_2 of y that satisfy:*

1. *Exactly two of the primes $2, 3, 5$ are ℓth power residues mod q, while the third is a ℓth power nonresidue mod q.*
2. *All three of the primes $2, 3, 5$ are ℓth power residues mod q_2, while 13 is an ℓth power nonresidue mod q_2.*

Then $(3 - \alpha) = \mathfrak{a}^r$, where $\mathfrak{a}$ is a representative of a class of order r in the class group of K.

Proof. According to Lemma 2.20 none of the prime factors of y divide $\operatorname{disc}(m_\alpha(X))$, and according to Lemma 2.21 any prime factor of y splits completely in K. The hypotheses of Lemma 2.19 are satisfied and allow us to conclude that $(3 - \alpha) = \mathfrak{a}^r$, for some ideal

$\mathfrak{a}$ of K. To show that $\mathfrak{a}$ has order r upon passing to the class group, we must show that no smaller positive power of $\mathfrak{a}$ is principal. If this was not the case, and some smaller positive power of $\mathfrak{a}$ was principal, then we would conclude that $(3-\alpha)$ is the ℓth power of a principal ideal for some $\ell > 1$ dividing r. Since a power of a principal ideal is principal we may, without loss of generality, take ℓ to be prime. Since the hypotheses of Propositions 2.23 and 2.24 are satisfied, $(3-\alpha)$ is not the ℓth power of principal ideal for any prime ℓ dividing r. Hence $\mathfrak{a}$ is a representative of a class of order r. □

2.6 On the origin of the ideal classes.

Y. Yamamoto [16] proved the existence of infinitely many real quadratic fields with class number divisible by any integer $r > 1$. Later, P.J. Weinberger [15] independently showed that the class number of the real quadratic field $\mathbb{Q}(\sqrt{a^{2r}+4})$ with a prime is divisible by r for odd r and by $r/2$ for even r if a satisfies some additional r-dependent conditions. This result was extended to show that for every integer $r \geq 2$ and every odd integer $a \geq 3$, the ideal class number of the field $\mathbb{Q}(\sqrt{a^{2r}+4})$ is divisible by r.

Based on these results, one might wonder if the ideal classes detected by our method are not, in fact, simply coming from ideal classes of the real quadratic subfield. We now show that this is not the case for infinitely many distinct fields K_n.

Lemma 2.26. *Let $r > 1$ be a rational integer. Let ρ be a root of the polynomial $f_{956}(X) := X^4 - 956X^3 - 6X^2 + 956X + 1$. Then $X^r - \rho$ is irreducible in $K_{956}[X]$.*

Proof. Let ρ denote a root of $f_{956}(X)$. We use PARI to compute a set of fundamental units for $K_{956} := K$:

$$u_1 = (1/338)\rho^3 - (478/169)\rho^2 - (5/338)\rho + 408/169$$

$$u_2 = (7/8788)\rho^3 - (6709/8788)\rho^2 + (16203/8788)\rho + 15531/8788$$

$$u_3 = (17/8788)\rho^3 - (16245/8788)\rho^2 - (6811/8788)\rho + 25019/8788.$$

It is then straightforward (but tedious) to check that

$$\rho = -\frac{1}{u_1 u_2^5 u_3^3}.$$

Hence $u_1 = -1/(\rho u_2^5 u_3^3)$ and we conclude that $\{\rho, u_2, u_3\}$ is also a set of fundamental units for K. But a result found in Lang's Algebra [10] says that $X^r - \rho$ is irreducible over a field K if $\rho \notin (K^\times)^\ell$ for any prime ℓ dividing r and $\rho \notin -4(K^\times)^4$ when $4 \mid r$. Since ρ belongs to a set of fundamental units, we conclude that $\rho \notin (K^\times)^\ell$ for every prime $\ell \mid r$. Computer calculation confirms that $f_{956}(X^4)$ is irreducible over $\mathbb{Q}$; hence $X^4 - \rho$ is irreducible in $K[X]$.

It is easy to see that the converse of the above result is also true: if $\rho \in (K^\times)^\ell$, then $X^r - \rho$ factors. If $\rho = -4b^4$ (with $b \in K^\times$), then $X^4 - \rho = X^4 + 4b^4 = (X^2 + 2bX + 2b^2)(X^2 - 2bX + 2b^2)$.

Hence, since $X^4 - \rho$ is irreducible in $K[X]$, we conclude that $\rho \notin (K^\times)^2$ and $\rho \notin$

$-4(K^\times)^4$. Thus Lang's result allows us to conclude that $X^r - \rho$ is irreducible for all integers $r \geq 1$. □

Definition 2.27. *A relative ideal class is an ideal class with trivial norm down to k_2.*

Remark 2.28. *The next theorem relies on the existence of primes satisfying a set of congruence conditions. This is established in the section immediately following this one.*

Theorem 2.29. *Let $r \geq 3$ be an odd rational integer. Let $(3, c_r(30dy + 1))$ be a solution in integers to $Y^r = m_\alpha(X)$, where $d = 3731 = 7 \times 13 \times 41$, and where $c_r \equiv 1 \mod 30$ is a constant which is not divisible by $7, 13$, and 41, and is chosen such that for each prime divisor ℓ of r there are corresponding prime divisors q_2, q_3, q_4, of c_r for which*

1. *All three of the primes $2, 3, 5$ are ℓth power residues mod q_2, while 13 is an ℓth power nonresidue mod q_2.*
2. *$2, 3$ are rth power residues mod q_3 and 5 is an ℓ-th power nonresidue mod q_3.*
3. *$3, 5$ are rth power residues mod q_4 and 2 is an ℓ-th power nonresidue mod q_4.*

Then there are infinitely many distinct fields in the family $\{K_n\}$ for which

$$\left(\frac{3 - \alpha_1}{3 - \alpha_3}\right) = \mathfrak{c}^r,$$

where $[\mathfrak{c}] \in \mathrm{Cl}_K$ is a relative ideal class of order r.

Proof. Apply Corollary 2.25 to conclude that $(3 - \alpha) = \mathfrak{a}^r$, where $[\mathfrak{a}]$ has order r in Cl_K .

It follows that

$$\left(\frac{3-\alpha_1}{3-\alpha_3}\right) = \mathfrak{c}^r,$$

for some ideal $\mathfrak{c}$. If $[\mathfrak{c}]$ does not have order r then there is a prime ℓ dividing r such that $\mathfrak{c}^{r/\ell}$ is principal. Hence

$$w := \frac{3-\alpha_1}{3-\alpha_3} = uz^\ell,$$

with u a unit of K and $z \in K^\times$. Our assumptions imply that $[\mathcal{O}_K^\times : \langle -1, \varepsilon, \rho_0, \rho_1 \rangle]$ is not divisible by ℓ. So we may assume that $u \in \langle -1, \varepsilon, \rho_0, \rho_1 \rangle$. Write

$$w = \varepsilon^a \rho_0^b \rho_1^c z^\ell.$$

with $a, b, c \in \mathbb{Z}$. Taking norms $K \to k_2$ we find that $\varepsilon^{2a} = N_{K|k_2}(u) = N_{K|k_2}(z)^{-\ell}$. Hence $\ell \mid a$ and we can absorb ε^a into z^ℓ. By Lemmas 2.20 and 2.21 the primes q_3 and q_4 split completely in K and do not divide disc $m_\alpha(X)$. Hence we may choose primes $\mathfrak{q}_3$ and $\mathfrak{q}_4$ of K lying over them such the $3 \equiv \alpha \mod \mathfrak{q}_3,\ \mathfrak{q}_4$. Applying Congruences (2.2), we find that

$$z^\ell \equiv 2^{2-c} 3^{c-2} 5^{-1-b} \mod \mathfrak{q}_3, \mathfrak{q}_4.$$

Applying conditions (2) and (3) above and absorbing ℓth powers into z, we may take $c = 2$ and $b = -1$. Hence

$$w\rho_0\rho_1^{-2} = z^\ell.$$

It will suffice to show that $Z^r - w\rho_0\rho_1^{-2}$ is irreducible in $K[Z]$, since this guarantees that $w\rho_0\rho_1^{-2} \notin (K^\times)^\ell$ for any prime ℓ dividing r. The minimal polynomial over $\mathbb{Q}$ of $w\rho_0\rho_1^{-2}$

is

$$Z^4 - \left(\frac{119n+480}{30n-119}\right) Z^3 - 6Z^2 + \left(\frac{119n+480}{30n-119}\right) Z + 1.$$

Clearing denominators and replacing Z with Z^r we obtain the polynomial

$$p_n(Z) := (30n-119)Z^{4r} - (119n+480)Z^{3r} - 6(30n-119)Z^{2r} + (119n+480)Z^r + (30n-119).$$

When $p_n(Z)$ is irreducible over $\mathbb{Q}$, $Z^r - w\rho_0\rho_1^{-2}$ is irreducible in $K[Z]$ and we reach the contradiction that $z \notin K^\times$. We are then forced to conclude that the ideal class of $\mathfrak{c}$ has order r.

To see that $p_n(Z)$ is irreducible for infinitely many fields in our family $\{K_n\}$, consider first the case $n = 4$. In this case

$$p_4(Z) = Z^{4r} - 956Z^{3r} - 6Z^{2r} + 956Z^r + 1.$$

If v is a zero of $p_4(Z)$, then the minimal polynomial (over $\mathbb{Q}$) of v divides $p_4(Z)$. But then v^r is a root of $f_{956}(Z)$. Hence by Lemma 2.35, the minimal polynomial (over $\mathbb{Q}$) of v must be of degree $\geq 4r$. Hence $p_4(Z)$ is the minimal polynomial (over $\mathbb{Q}$) of the zero v.

For infinitely many primes q, the polynomial

$$(X^r + 119 - 30\sqrt{-16})(X^r + 119 + 30\sqrt{-16}) \in \mathbb{Z}[X]$$

splits into linear factors mod q. Let q be such a prime. If b is a root mod q, then

$$b^r \equiv -119 \pm 30\sqrt{-16} \mod q.$$

So, choose $n_0 \equiv \pm\sqrt{-16} \mod q$. Then $n_0^2 + 16 \equiv 0 \mod q$. By perhaps adding q to n_0, we may take n_0 to be such that $n_0^2 + 16 \equiv 0 \mod q$, but $n_0^2 + 16 \not\equiv 0 \mod q^2$.

Furthermore, because there are infinitely many such q, we may take q to not divide r, $30c_r d$ and $119^2 + 30^2 \cdot 16$. Then $q \nmid b$ and

$$b^r \equiv 30n_0 - 119 \mod q.$$

By Hensel's Lemma, there exists $b_0 \equiv b \mod q$, with

$$b_0^r \equiv -119 + 30n_0 \mod q^2.$$

Now choose y_0 such that

$$c_r(30dy_0 + 1) \equiv b_0 \mod q^2.$$

Let $m \in \mathbb{Z}$. Then

$$c_r(30d(y_0 + mq^2) + 1) \equiv b_0 \mod q^2.$$

Hence

$$[c_r(30d(y_0 + mq^2) + 1)]^r \equiv -119 + 30n_0 \mod q^2.$$

Noting that

$$[c_r(30d(y_0 + mq^2) + 1)]^r \equiv 1 \mod 30,$$

we may write

$$[c_r(30d(y_0 + mq^2) + 1)]^r = 30n - 119,$$

for some $n \in \mathbb{Z}$. Furthermore, since $30n \equiv 30n_0 \mod q^2$, we see that $n \equiv n_0 \mod q^2$. Hence $n^2 + 16$ is divisible by q but not by q^2. Solving for n in this last equation, we conclude that $p_n(Z) = g(m, Z)$, where

$$\begin{aligned} g(X, Z) := {} & [c_r(30d(y_0 + q^2X) + 1)]^r Z^{4r} \\ & - \left(\frac{119\left([c_r(30d(y_0 + q^2X) + 1)]^r + 119\right) + 14400}{30} \right) Z^{3r} \\ & - 6[c_r(30d(y_0 + q^2X) + 1)]^r Z^{2r} \\ & + \left(\frac{119\left([c_r(30d(y_0 + q^2X) + 1)]^r + 119\right) + 14400}{30} \right) Z^r \\ & + [c_r(30d(y_0 + q^2X) + 1)]^r. \end{aligned}$$

The polynomial $g(X, Z)$ is irreducible in $\mathbb{Q}[X, Z]$. Indeed, if not, then any specialization $g(m, Z) \in \mathbb{Q}[Z]$ would be reducible. But, for example, choosing $X = x \in \mathbb{Q}$ such that $[c_r(30d(y_0 + q^2X) + 1)]^r = 1$ (corresponding to $n = 4$), we obtain the irreducible polynomial $p_4(Z)$. Hilbert's Irreducibility Theorem [9] states that if $g(X, Z)$ is an irreducible polynomial in X and Z with coefficients in $\mathbb{Z}$, then there are infinitely many integers m

for which $g(m, Z)$ is an irreducible polynomial in $\mathbb{Z}[Z]$. Hence there are infinitely many parameter values n for which

$$\left(\frac{3-\alpha_1}{3-\alpha_3}\right) = \mathfrak{c}^r,$$

where $\mathfrak{c}$ represents a class of order r in Cl_K . Furthermore, by allowing the prime q to vary we see that we obtain infinitely many distinct fields for which this is true, because q ramifies in the quadratic subfield $\mathbb{Q}(\sqrt{n^2+16})$.

Since $N_{K|k_2}(w) = 1$, we conclude that $N_{K|k_2}(\mathfrak{c}) = \mathcal{O}_{k_2}$. Hence $[\mathfrak{c}] \in \mathrm{Cl}_K$ is mapped to the trivial element of Cl_{k_2} and is a relative ideal class. □

Remark 2.30. *The only relative ideal classes that possibly admit a representative from k_2 are those of order 1 or 2. Hence the construction of Theorem 2.29 yields ideal class which do not come from the quadratic subfield.*

2.7 Existence of infinitely many fields of the family with $r \mid h_K$ for arbitrary integer $r > 1$.

In this section we show that there are infinitely many distinct fields of the family $\{K_n\}$ with class number a multiple of r. Proving the existence of a field K_n of our family with class number divisible by r is the essential step; once existence is established the existence of infinitely many distinct fields of our family with class number divisible by r follows. Existence requires demonstrating that there are infinitely many primes satisfying the congruence conditions sufficient to guarantee the existence of a class of order r and showing that there are infinitely many primes satisfying similar congruence conditions

was needed in Theorem 2.29. Both can be accomplished with an appeal to Bauer's Theorem in the following Lemmas and Remark.

Lemma 2.31. *Let ℓ be a prime. There are infinitely many primes q for which, for example, 2 and 3 are ℓth power residues mod q, but for which 5 is an ℓth power nonresidue mod q.*

Proof. Let

$$L = \mathbb{Q}(\zeta_\ell, 2^{1/\ell}, 3^{1/\ell})$$

$$L' = \mathbb{Q}(\zeta_{2\ell}, 5^{1/\ell})$$

ζ_ℓ (resp. $\zeta_{2\ell}$) denotes a primitive ℓth (resp. 2ℓth) root of unity. A rational prime q splits completely in L if and only if $q \equiv 1 \bmod \ell$ and $2, 3$ are ℓth power residues mod q. A rational prime q splits completely in L' if and only if $q \equiv 1 \bmod 2\ell$ and 5 is an ℓth power residue mod q. Since $L' \not\subset L$, we may apply Bauer's Theorem [2] to conclude that there are infinitely many primes that split in L and do not split in L'. Hence there are infinitely many primes q for which 2 and 3 are ℓth power residues mod q but for which 5 is an ℓth power nonresidue mod q. □

Remark 2.32. *The previous lemma makes clear that there are infinitely many primes q for which exactly two elements of the set $\{2, 3, 5\}$ are rth (hence ℓth as well) power residues mod q, while the third is an ℓth power nonresidue mod q.*

Lemma 2.33. *Let ℓ be a prime. There are infinitely many primes q_2 for which $2, 3$, and*

5 *are* ℓ*th power residues modulo* q_2*, but for which* 13 *is an* ℓ*th power nonresidue modulo* q_2.

Proof. The proof is extremely similar to that used in Lemma 2.31. □

Theorem 2.34. *Let* r *be an arbitrary positive integer* > 1*. This family contains infinitely many members with class number divisible by* r *and there is a procedure for producing arbitrarily many distinct quartic fields of this family whose class group contains a cyclic subgroup of order* r.

Proof. Let ℓ be a prime dividing r. Choose a pair of primes $(q_\ell, q_{2,\ell})$ satisfying the power residue hypotheses of Corollary 2.25 for each odd prime ℓ dividing r. For $\ell = 2$, choose a prime $q_\ell \equiv 1 \bmod 30$ (by Dirichlet's Theorem on primes in arithmetical progressions there are infinitely many choices for q_ℓ) and set $q_{2,\ell} = 1$. Make sure never to choose $2, 3, 5, 7, 13$, or 41, for either of the primes. (This presents no problem since, by Remark 2.32 and Lemma 2.33, there are infinitely many pairs of primes satisfying the power residue hypotheses of Corollary 2.25.) Choose s such that

$$\left(s \prod_{\ell | m} q_\ell q_{2,\ell} \right)^r \equiv -119 \mod 30.$$

Thus the pair $(3, s \prod_{\ell|m} q_\ell q_{2,\ell})$ is a solution in integers to $Y^r = m_\alpha(X)$ for some n and from Corollary 2.25 we conclude that $r \mid h_n$. Thus for an arbitrary $r > 1$, there is an element, K_n, of this family of quartics which has class number divisible by r.

This result now implies that there are infinitely many members of this family of quar-

tics whose class number is divisible by r. Indeed, suppose that K_n is such that $r \mid h_n$. Let r^ω be the greatest power of r dividing h_n. From the previous paragraph we know that there is a quartic field $K_{n'}$ in this family for which $r^{\omega+1}$ divides $h_{n'}$. But $K_{n'} \neq K_n$, since they have different class numbers. Thus given any finite number of quartic fields with class number divisible by r, we can find an additional one. We conclude that this family of quartic fields contains infinitely many members with class number divisible by r. $\square$

2.8 Figures h_K vs. n.

Figure 2.1 displays average class number versus parameter. The class number of K_n for each value of the parameter n was calculated using PARI. The raw data was then averaged using the Matlab function movmean. For any particular n, this took the corresponding h_{K_n} along with the 500 preceding class numbers and 500 succeeding class numbers and averaged these 1001 data points. The averages at the endpoints are taken over the available data points. We note that the average class number appears to increase with parameter, as expected, but that despite the averaging the plot still contains significant noise.

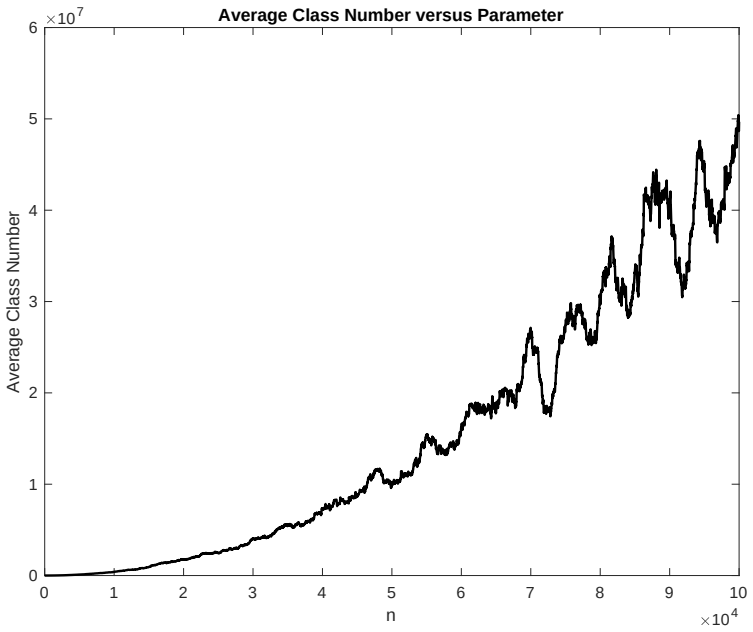


Figure 2.1: Average Class Number vs. Parameter

Figure 2.2 displays average relative class number versus parameter. The class number of the quadratic subfield k_2 for each value of the parameter n was calculated using PARI. The ratio of h_{K_n}/h_{k_2} was then calculated for each n and the raw data was then averaged using the same Matlab function and process outlined above (with the same size averaging window.) Comparing this plot with that in Figure 2.1 suggests that much of the noise in Figure 2.1 comes from the class number of the quadratic subfield and hence that the new ideal classes produced when going from k_2 up to K_n have a much simpler dependence on the parameter n.

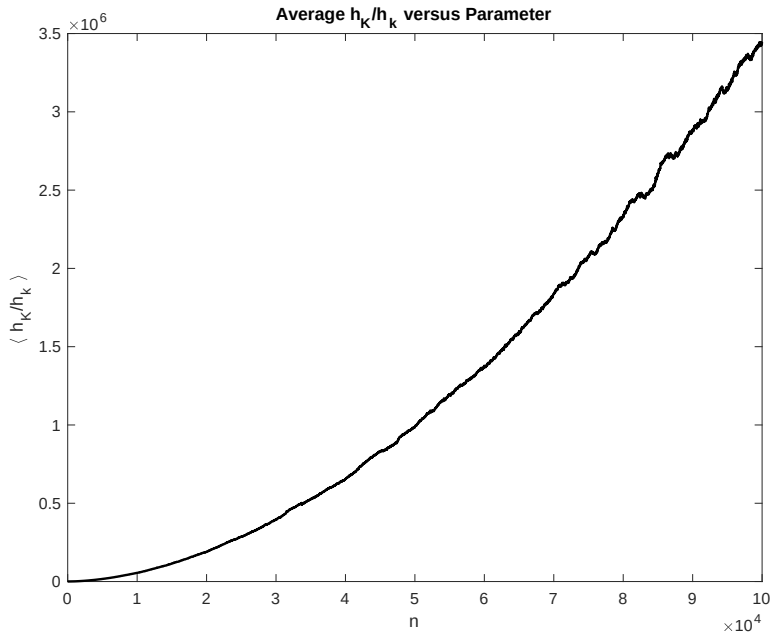


Figure 2.2: Average Relative Class Number vs. Parameter

2.9 Examples.

Example 2.35. *Let* $r = 2$ *and* $y = 31$, *so that* $n = 30788$. *The previous theorem predicts that* $(3 - \alpha) = (3 - \rho_0 + 3\rho_1) = \mathfrak{a}^2$, *where* $\mathfrak{a}$ *is a representative of a class of order* 2 *in the class group. A quick PARI calculation shows that* $h_{30788} = 231735296 = 2^{20} \times 13 \times 17$.

Example 2.36. *Let* $r = 3$. *We now follow the proof of Theorem 2.34 to find a parameter value* n *for which* h_{K_n} *is a multiple of* 3. *The first prime* q *for which two elements of the set* $\{2, 3, 5\}$ *are cubic residues mod* q *while the third is a cubic nonresidue mod* q *is* $q = 67$. *The first prime* q_2 *for which all elements of the set* $\{2, 3, 5\}$ *are cubic residues mod* q_2 *while* 13 *is a cubic nonresidue mod* q_2 *is* $q_2 = 643$. *Since* $qq_2 = 43081 \equiv 1 \mod 30$, *we may choose* $s = 1$. *Solving the equation* $(sq_1q_2)^6 = 30n - 119$ *for* n *we find that* $n = 213104881995293580657999820$. *Corollary 2.25 predicts that* $3 \mid h_{K_n}$. *The results of a PARI computation are not available for such a large value of the parameter* n.

Remark 2.37. *Since* $h_{K_n} \equiv 0 \mod 3$, *when* $n = 30, 54, 56, 62, 64, 65, 70, 74, 75, 83, 91, 94, 108, \ldots$, *Example 2.36 suggests that the algorithm presented in the proof of Theorem 2.34 produces a rather sparse subset of the collection of all fields of the family with class number divisible by* 3.

Chapter 3: A Family of Sextic Number Fields.

We restrict attention in this chapter to the family of splitting fields, K_n, of polynomials of the form

$$f_n(X) = X^6 - 2nX^5 - (5n+15)X^4 - 20X^3 + 5nX^2 + (2n+6)X + 1, \qquad (3.1)$$

where n is a nonzero integer not equal to $-8, -3$, or 5.

Let $r \geq 1$ be an odd but otherwise arbitrary integer. Our main result shows that this family of sextics contains infinitely many distinct fields, K_n, whose class group contains a cyclic subgroup of order r generated by an ideal class which does not come from either the quadratic or cubic subfield of K_n.

Remark 3.1. *Adjoing a root ρ of $f_n(X)$ to $\mathbb{Q}$ yields a real sextic extension of $\mathbb{Q}$ with cyclic Galois group generated by $\sigma : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho)$, $\rho \mapsto (\rho-1)/(\rho+2)$. To see this, let $t = 4n+6$, so that*

$$f_n(X) = X^6 - \left(\frac{t-6}{2}\right)X^5 - 5\left(\frac{t-6}{4}\right)X^4 - 20X^3 + 5\left(\frac{t-6}{4}\right)X^2 + \left(\frac{t+6}{2}\right)X + 1. \qquad (3.2)$$

The splitting fields K_t of polynomials of the form on the right hand side of Equation (3.2) were studied by M.-N. Gras [7] and shown to be real sextic extensions of $\mathbb{Q}$ with cyclic Galois group generated by $\sigma : \mathbb{Q}(\rho) \to \mathbb{Q}(\rho)$, $\rho \mapsto (\rho - 1)/(\rho + 2)$ whenever $t \neq 0, \pm 6, \pm 26$ is a rational integer. Gras also showed in this work that $K_t = K_{-t}$ and so we may restrict our attention to integer parameter values $n \geq -1$ and $n \neq 0, 5$. The form of the polynomial we are using (3.1) is that employed by Gaál and Remete [5] in their recent work on integral bases for these fields.

Remark 3.2. *Let ρ denote a root of $f_n(X) = 0$. Then by applying the elements of the Galois group to ρ we find that the other five zeros of $f_n(X)$ are*

$$\begin{aligned} &\rho_1 = (\rho - 1)/(\rho + 2), \quad \rho_2 = -1/(\rho + 1), \\ &\rho_3 = -(\rho + 2)/(2\rho + 1), \quad \rho_4 = -(\rho + 1)/\rho, \quad \rho_5 = -(2\rho + 1)/(\rho - 1). \end{aligned} \tag{3.3}$$

3.1 More on the zeros of f_n.

Proposition 3.3. *Let ρ_0 denote the greatest root of $f_n(X)$. When $n \geq 8$,*

$$\begin{aligned} &2n + 2 < \rho_0 < 2n + 3, \quad \frac{2n+1}{2n+5} < \rho_1 < \frac{n+1}{n+2}, \quad -\frac{1}{2n+3} < \rho_2 < -\frac{1}{2n+4}, \\ &-\frac{2n+5}{4n+5} < \rho_3 < -\frac{2n+4}{4n+7}, \quad -\frac{n+2}{n+1} < \rho_4 < -1, \quad -\frac{4n+7}{2n+1} < \rho_5 < -\frac{4n+5}{2n+2}. \end{aligned} \tag{3.4}$$

Proof. Since $f_n(1) = -27 < 0$ and since $f_n(x) \to \infty$ as $x \to \infty$ we see that f_n has a real root greater than one. In particular, $\rho_0 > 1$. Letting $\rho = \rho_0$ in Equations (3.3) we

see that ρ_1 is positive but less than 1 and that all of the remaining zeros are negative. For $n \geq 0$, $f_n(2n+2) < 0$, while for $n \geq 8$, $f_n(2n+3) > 0$. Applying the Intermediate Value Theorem we conclude that $2n+2 < \rho_0 < 2n+3$, when $n \geq 8$. The remaining inequalities now follow from Equations (3.3). □

3.2 Structure of the splitting field K_n.

Remark 3.4. *The splitting field K_n contains a unique cubic subfield which we denote by $k_{3,n}$ or k_3 and a unique quadratic subfield which we denote by $k_{2,n}$ or k_2. The quadratic extension is generated by a root of $h(X) = X^2 - (n^2+3n+9)$, while the cubic extension is a simplest cubic field generated by a root of $g_n(X) = X^3 - nX^2 - (n+3)X - 1$ (as detailed in [7], [5]). In terms of the roots ρ_i of $f_n(X) = 0$, the roots of $g_n(X) = 0$ are*

$$\mu = -(1+\rho_0\rho_3), \quad \mu^\sigma = \frac{1}{\rho_0\rho_3}, \text{ and } \mu^{\sigma^2} = -\frac{\rho_0\rho_3}{1+\rho_0\rho_3}.$$

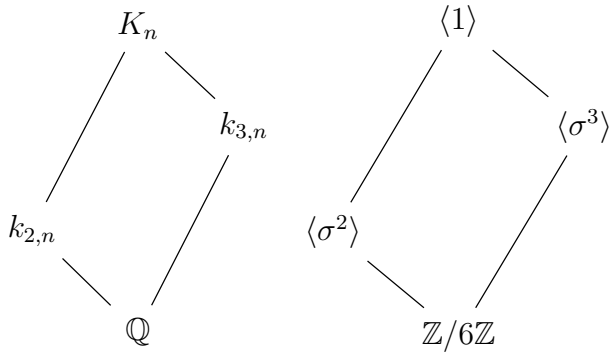
Let $\mu_i = \mu^{\sigma^i}$, $i = 0, 1, 2$. Use the relation $\rho_3 = -(\rho_0+2)/(2\rho_0+1)$ (Equation 3.3) to find that $\mu = (\rho_0^2 - 1)/(2\rho_0 + 1)$ along with the fact that $2n+2 < \rho_0 < 2n+3$ (Proposition 3.3) to conclude that

$$n+2 > \mu_0 > n > 0 > \mu_1 > -1 > \mu_2 > -2,$$

when $n \geq 8$.

Let $\sigma = (012345)$ denote the generator of $\mathrm{Gal}(K_n/\mathbb{Q})$ of Remark 3.1. The lattice of

subfields of K_n and the corresponding lattice of subgroups of $\mathbb{Z}/6\mathbb{Z} = \langle\sigma\rangle$ are given by the following diagrams:



3.3 Units.

Since there are six real embeddings of K into $\mathbb{C}$ and no complex embeddings, Dirichlet's Unit Theorem implies that the rank of the unit group $\mathcal{O}_K^\times$ is 5. That the ρ_i and μ_i are units is evident from their minimal equations of integral dependence (over $\mathbb{Q}$.) Hence it makes sense to study the subgroup U of $\mathcal{O}_K^\times$ generated by $\{-1, \mu_0, \mu_1, \rho_0, \rho_1, \varepsilon\}$. This section gives sufficient conditions to conclude that this set (excluding -1) forms a fundamental set or nearly fundamental set of units. It also provides a proof of the fact that the index $[\mathcal{O}_K^\times : U]$ is odd.

3.3.1 Multiplicative independence of $\{\mu_0, \mu_1, \rho_0, \rho_1, \varepsilon\}$

Proposition 3.5. *If* $n \geq 8$, *then* $\log^2 |\rho_2/\rho_5| - \log |\rho_1/\rho_4| \log |\rho_3/\rho_0| > 0$.

Proof. Using Equations (3.3) and Inequalities (3.4) above, $|\rho_2/\rho_5| < (2n+2)/((4n+5)(2n+3)) < 1/(4n+5)$. Hence $\log |\rho_2/\rho_5| < -\log(4n+5)$, and $\log^2(4n+5) < \log^2 |\rho_2/\rho_5|$. A similar argument shows that $\log((n+1)/(n+2)) - 1 < \log |\rho_1/\rho_4| < 0$, and that $-\log(4n+7) < \log |\rho_3/\rho_0| < 0$. Hence $\log^2 |\rho_2/\rho_5| - \log |\rho_1/\rho_4| \log |\rho_3/\rho_0| > \log^2(4n+5) - \log(4n+7)(\log((n+1)/(n+2)) - 1) > \log^2(4n+5) + \log(4n+7) > 0$.

□

Lemma 3.6. *The set* $\{\mu_0, \mu_1, \rho_0, \rho_1, \varepsilon\}$ *is a multiplicatively independent subset of* $\mathcal{O}_K^\times$.

Proof. Let R denote the regulator of $\{\mu_0, \mu_1, \rho_0, \rho_1, \varepsilon\}$. Then R is the absolute value of

$$\det \begin{pmatrix} \log|\mu_0| & \log|\mu_1| & \log|\rho_0| & \log|\rho_1| & \log|\varepsilon| \\ \log|\mu_1| & \log|\mu_2| & \log|\rho_1| & \log|\rho_2| & \log|\varepsilon^\sigma| \\ \log|\mu_2| & \log|\mu_0| & \log|\rho_2| & \log|\rho_3| & \log|\varepsilon| \\ \log|\mu| & \log|\mu_1| & \log|\rho_3| & \log|\rho_4| & \log|\varepsilon^\sigma| \\ \log|\mu_1| & \log|\mu_2| & \log|\rho_4| & \log|\rho_5| & \log|\varepsilon| \end{pmatrix} \tag{3.5}$$

$$= \det \begin{pmatrix} \log|\mu_0| & \log|\mu_1| & \log|\rho_0| & \log|\rho_1| & \log|\varepsilon| \\ \log|\mu_1| & \log|\mu_2| & \log|\rho_1| & \log|\rho_2| & \log|\varepsilon^\sigma| \\ 0 & 0 & \log|\rho_1/\rho_4| & \log|\rho_2/\rho_5| & \log|\varepsilon| \\ 0 & 0 & \log|\rho_2/\rho_5| & \log|\rho_3/\rho_0| & \log|\varepsilon^\sigma| \\ 0 & 0 & 0 & 0 & 3\log|\varepsilon| \end{pmatrix},$$

where the second matrix is obtained from the first by the following sequence of row operations: add rows 1 and 3 to row 5, add rows 2 and 3 to row 4, and finally add rows 1 and 2 to row 3. It is clear that

$$\det \begin{pmatrix} \log|\mu_0| & \log|\mu_1| \\ \log|\mu_1| & \log|\mu_2| \end{pmatrix} \neq 0,$$

because up to sign this is the regulator of $\{\mu_0, \mu_1\}$; a multiplicatively independent subset of k_3. It is equally clear that $3\log|\varepsilon| \neq 0$, because $\varepsilon > 1$. Finally, applying Proposition

3.5, we conclude that

$$\left| \det \begin{pmatrix} \log|\rho_1/\rho_4| & \log|\rho_2/\rho_5| \\ \log|\rho_2/\rho_5| & \log|\rho_3/\rho_0| \end{pmatrix} \right| = |\log^2|\rho_2/\rho_5| - \log|\rho_1/\rho_4| \log|\rho_3/\rho_0||$$

$$> 0,$$

whenever $n > 8$ and hence that $R \neq 0$ for such n. The remaining values of $-1 \leq n \leq 8$, $n \neq 0, 5$ may be checked by hand (or computer) to conclude that $R \neq 0$ for these cases too. Since $R \neq 0$, we conclude that $\{\mu_0, \mu_1, \rho_0, \rho_1, \varepsilon\}$ is a multiplicatively independent subset of $\mathcal{O}_K^\times$. □

3.3.2 The index $[\mathcal{O}_K^\times : U]$

The following information, prerequisite for Proposition 3.7, can be found in M.N. Gras [7]. Let $U_\chi := \{u \in \mathcal{O}_K^\times \mid N_{K|k_2}(u) = \pm 1 \text{ and } N_{K|k_3}(u) = \pm 1\}$ denote the group of relative units. Note that if $u \in U_\chi$, then $u^{1+\sigma^2+\sigma^4} = \pm 1$ and $u^{1+\sigma^3} = \pm 1$. Hence

$$u^{1+\sigma^2+\sigma^4} = \pm u^{1+\sigma^3} \implies u^{\sigma^2+\sigma^4} = \pm u^{\sigma^3} \implies u^{1+\sigma^2} = \pm u^{\sigma} \implies u^{1-\sigma+\sigma^2} = \pm 1.$$

Conversely, if u is a unit for which $u^{1-\sigma+\sigma^2} = \pm 1$, then

$$u^{1+\sigma^2} = \pm u^{\sigma} \implies u^{\sigma^2+\sigma^4} = \pm u^{\sigma^3} \implies N_{K|k_2}(u) = u^{1+\sigma^2+\sigma^4} = \pm u^{1+\sigma^3} = \pm N_{K|k_3}(u).$$

Since the units of k_2 and k_3 meet in $\{\pm 1\}$, we conclude that $N_{K|k_2}(u) = \pm 1$ and $N_{K|k_3}(u) = \pm 1$ and hence that $u \in U_\chi$. Thus $U_\chi = \{u \in \mathcal{O}_K^\times \mid u^{1-\sigma+\sigma^2} = \pm 1\}$. Let G

denote $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ and note that U_χ is $\mathbb{Z}[G]$-module. Let U_* denote the submodule $\{u \in U_\chi \mid u^{1-\sigma+\sigma^2} = 1\}$, so that $U_\chi = \{\pm 1\} \times U_*$. Then U_* is a free $\mathbb{Z}[G]/(1-\sigma+\sigma^2)$-module of rank 1, and so if $\{u\}$ is a basis for this free-module, then every element of U_χ may be written uniquely in the form $\pm u^a (u^\sigma)^b$ with $a, b \in \mathbb{Z}$. M.N. Gras has shown (see [7] Théorème 4.18) that when n^2+3n+9 is, apart from powers of 3, square-free, and $n \neq 1, 12$, ρ_0/ρ_3 generates U_* as a $\mathbb{Z}[G]/(1-\sigma+\sigma^2)$-module. In other words, under these hypotheses every element of U_χ may be written uniquely in the form $\pm(\rho_0/\rho_3)^a(\rho_1/\rho_4)^b$ with $a, b \in \mathbb{Z}$. This is sufficient to establish the following:

Proposition 3.7. *If n^2+3n+9 is, apart from powers of 3, square-free, and $n \neq 1, 12$, then $[\mathcal{O}_K^\times : U] = 1$ or 3.*

Proof. Note that U contains the subgroup U' generated by $\{-1, \mu_0, \mu_1, \rho_0/\rho_3, \rho_1/\rho_4, \varepsilon\}$. Indeed, $\rho_0^{-1}(\mu_1)^{-1} = \rho_0\rho_3/\rho_0 = \rho_3$. Hence U contains ρ_3, and since it also contains ρ_0, it contains ρ_0/ρ_3. Similarly, $\rho_1^{-1}(\mu_2)^{-1} = \rho_4$. Since $(\mu_2)^{-1} = \mu_0\mu_1$ and since U contains ρ_1, we conclude that U contains ρ_4. Hence U also contains ρ_1/ρ_4. Since U contains the generators of U' it contains U'.

Let R' denote the regulator of $\{\mu_0, \mu_1, \rho_0/\rho_3, \rho_1/\rho_4, \varepsilon\}$. Then R' is the absolute value

of

$$\det \begin{pmatrix} \log|\mu_0| & \log|\mu_1| & \log|\rho_0/\rho_3| & \log|\rho_1/\rho_4| & \log|\epsilon| \\ \log|\mu_1| & \log|\mu_2| & \log|\rho_1/\rho_4| & \log|\rho_2/\rho_5| & \log|\epsilon^\sigma| \\ \log|\mu_2| & \log|\mu_0| & \log|\rho_2/\rho_5| & \log|\rho_3/\rho_0| & \log|\epsilon| \\ \log|\mu_0| & \log|\mu_1| & \log|\rho_3/\rho_0| & \log|\rho_4/\rho_1| & \log|\epsilon^\sigma| \\ \log|\mu_1| & \log|\mu_2| & \log|\rho_4/\rho_1| & \log|\rho_5/\rho_2| & \log|\epsilon| \end{pmatrix} \tag{3.6}$$

$$= \det \begin{pmatrix} \log|\mu_0| & \log|\mu_1| & \log|\rho_0/\rho_3| & \log|\rho_1/\rho_4| & \log|\epsilon| \\ \log|\mu_1| & \log|\mu_2| & \log|\rho_1/\rho_4| & \log|\rho_2/\rho_5| & \log|\epsilon^\sigma| \\ 0 & 0 & 2\log|\rho_1/\rho_4| & 2\log|\rho_2/\rho_5| & \log|\epsilon| \\ 0 & 0 & 2\log|\rho_2/\rho_5| & 2\log|\rho_3/\rho_0| & \log|\epsilon^\sigma| \\ 0 & 0 & 0 & 0 & 3\log|\epsilon| \end{pmatrix},$$

where we have used the same sequence of row operations as used in Lemma 3.6 to bring the first matrix into the row equivalent form of the second matrix. Comparing the right hand sides of Equations (3.5) and (3.6), we conclude that $R' = 4R$. Hence

$$[\mathcal{O}_K^\times : U] = \frac{[\mathcal{O}_K^\times : U']}{[U : U']} = \frac{[\mathcal{O}_K^\times : U']}{R'/R} = \frac{[\mathcal{O}_K^\times : U']}{4}.$$

The paragraph preceding this proposition, allows us to conclude that U' is the subgroup $U_2U_3U_R \leq \mathcal{O}_K^\times$ of Ennola, Maki, and Turunen [4] and hence that $[\mathcal{O}_K^\times : U'] = 1, 3, 4,$ or 12. Hence we conclude that $[\mathcal{O}_K^\times : U] = 1$ or 3. □

Lemma 3.8. *The index* $[\mathcal{O}_K^\times : U]$ *is odd.*

Proof. If 2 divides $[\mathcal{O}_K^\times : U]$, then there is a unit $u \in \mathcal{O}_K^\times \smallsetminus U$ such that

$$u^2 = \pm\varepsilon^a \mu_0^b \mu_1^c \rho_0^d \rho_1^e, \tag{3.7}$$

and with each integer exponent $a, b, c, d, e \in \{0, 1\}$. Taking norms $K \to k_2$ of both sides of Equation (3.7), we find that

$$(N_{K|k_2}(u))^2 = \pm\varepsilon^{3a}.$$

If $a = 1$, then we conclude that $\pm\varepsilon$ is a square in k_2. But $-\varepsilon$ cannot be a square in k_2, because $K/\mathbb{Q}$ is a real and ε cannot be a square in k_2, because it is the fundamental unit of k_2. We conclude that $a = 0$, and so

$$u^2 = \pm\mu_0^b \mu_1^c \rho_0^d \rho_1^e. \tag{3.8}$$

Taking norms $K \to k_3$ of both sides of Equation (3.8), we find that

$$(N_{K|k_3}(u))^2 = \mu_0^{2b-e} \mu_1^{2c-d-e}.$$

Recall that $\mu_0\mu_1 = 1/\mu_2$. If $d \neq 0$ or $e \neq 0$, then either μ_2/μ_1, μ_2, or μ_1 is a square in k_3. Since none of these units is totally positive, we've reached a contradiction. Hence

$d = e = 0$, and Equation (3.8) becomes

$$u^2 = \pm\mu_0^b \mu_1^c.$$

If $b \neq 0$ or $c \neq 0$, we again reach the contradiction that the left hand side is totally positive, while the right hand side is not totally positive. Hence $b = c = 0$ and $u^2 = \pm 1$. We conclude that $u = \pm 1 \in U$. Since this contradicts our hypothesis that $u \notin U$, the proof is complete. □

3.4 Conditions sufficient to conclude that $r \mid h_K$ for arbitrary odd integer $r > 1$.

As in the quartic case, we show that r divides the class number of K by showing that the class group contains an element of order r. We begin again with a principal ideal of K, show that it factors as an rth power of an ideal $\mathfrak{a}$, and then show that no lesser power of $\mathfrak{a}$ is principal.

In the quartic case we were led to consider other primitive elements for the extension K_n/Q in order to ensure that an arbitrary integer r divided the class number of a field in our family. We pursued the same method here, but without success. Hence we factor $(x - \rho_0)$ and find solutions to $Y^r = f_n(X)$ as in the original work of [14], but our results only detect classes of odd but otherwise arbitrary order.

3.4.1 Candidate for a representative of a class of odd order r

Lemma 3.9. *Let $(-3, y)$ be a solution in integers to $Y^r = f_n(X)$. Assume that any prime factor of y which splits in K does not divide the discriminant of $f_n(X)$. If $\gcd(r, 3) = 1$, then $(-3 - \rho_0)$ is the rth power of an ideal of K. If $r \equiv 0 \mod 3$, then $(-3 - \rho_0)$ is the $r/3$-th power of an ideal of K.*

Proof. Since $f_n(-3) = 120n + 37$, the hypothesis that $y^r = f_n(-3)$ implies that 37 is an r-th power residue mod 5. Since $37 \equiv 2 \mod 5$ is a quadratic nonresidue mod 5, it is clear that r must be odd. From the same hypotheses we have that

$$y^r = f_n(-3) = \prod_{i=0}^{5}(-3 - \rho_0).$$

Let

$$(-3 - \rho_0) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}},$$

be the unique factorization of the integral ideal $(-3 - \rho_0)$ into a product of (only finitely many) positive integer powers of prime ideals and let p be the rational prime below $\mathfrak{p}$.

If $\mathfrak{p}$ is totally ramified in K, then it equals its Galois conjugates, so $\mathfrak{p}^{\nu_\mathfrak{p}}$ is the exact power of $\mathfrak{p}$ dividing each of the $(-3 - \rho_i)$. Hence $\mathfrak{p}^{6\nu_\mathfrak{p}} = p^{\nu_\mathfrak{p}}$ exactly divides y^r and $r \mid \nu_\mathfrak{p}$.

If p does not split in K, but $\mathfrak{p}$ is not totally ramified, then (p) factors as $\mathfrak{p} = (p)$, $\mathfrak{p}^2 = (p)$, or $\mathfrak{p}^3 = (p)$. No matter which factorization holds, $\mathfrak{p}$ still equals its Galois conjugates and

so $\mathfrak{p}^{\nu_\mathfrak{p}}$ is the exact power of $\mathfrak{p}$ dividing the conjugates of $(-3-\rho_0)$. Hence $\mathfrak{p}^{6\nu_\mathfrak{p}}$ exactly divides y^r. If $\mathfrak{p}=(p)$, then $r \mid 6\nu_\mathfrak{p} \implies r \mid 3\nu_\mathfrak{p}$. If $\mathfrak{p}^2=(p)$, then $r \mid 3\nu_\mathfrak{p}$, and if $\mathfrak{p}^3=(p)$, then $r \mid 2\nu_\mathfrak{p} \implies r \mid \nu_\mathfrak{p}$.

Finally, if p splits in K, then either it splits completely or it splits into two or three prime ideals. Suppose that p splits into two primes and let $\mathfrak{p}_2$ denote the other prime over p. Since $\mathrm{Gal}(K/\mathbb{Q})=\langle\sigma\rangle$ acts transitively on the set $\{\mathfrak{p},\mathfrak{p}_2\}$, the stabilizer of any prime under this action is the unique subgroup of order 3, $\langle\sigma^2\rangle$. Since $-3-\rho_0 \in \mathfrak{p}$, we now conclude that $-3-\rho_2 \in \mathfrak{p}$. Hence $\mathfrak{p}$ contains $\rho_0-\rho_2$ and so contains $\mathrm{disc}(f_n(X))$. Similarly p splitting into three prime ideals implies that $\mathfrak{p}$ contains $\mathrm{disc}(f_n(X))$. Since this contradicts our hypothesis on primes dividing y which split in K, we conclude that p splits completely in K: $(p)=\mathfrak{p}\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$. Each of these six prime ideals over p must contain exactly one of the conjugates of $-3-\rho_0$, since otherwise one of these prime ideals would contain $\mathrm{disc}(f_n(X))$ and p would divide $\mathrm{disc}(f_n(X))$; again a contradiction to our hypothesis on primes dividing y which split in K. Hence $p^{\nu_\mathfrak{p}}$ exactly divides y^r, and so $r \mid \nu_\mathfrak{p}$.

We have now shown that if $\gcd(r,3)=1$, then $(-3-\rho_0)$ is the rth power of the ideal

$$\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{\nu_\mathfrak{p}/r}.$$

We have also shown that if $r \equiv 0 \mod 3$, then $(-3-\rho_0)$ is the $r/3$-th power of the ideal

$$\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{3\nu_{\mathfrak{p}}/r}.$$

□

3.4.2 The behavior of primes revisited

Lemma 3.10. *Let $(-3, y)$ be a solution in integers to $Y^r = f_n(X)$. Then $\gcd(120, y) = 1$ and the only possible prime common divisor of y and $\mathrm{disc}(f_n(X))$ is 7.*

Proof. Note that $\mathrm{disc}(f_n(X)) = 6^6(n^2+3n+9)^5$ and that

$$y^r = f_n(-3) = 120n + 37.$$

If $q = 2, 3$, or 5 divides y, then $37 \equiv 0 \mod q$; an absurdity. Hence $\gcd(120, y) = 1$. We see that any prime common divisor, q, of $\mathrm{disc}(f_n(X))$ and y^r yields a pair of congruences

$$6^6(n^2+3n+9)^5 \equiv 0 \mod q$$

$$120n + 37 \equiv 0 \mod q.$$

Since $\gcd(q, 120) = 1$, the linear congruence has the unique solution $n \equiv -37/120 \mod q$. Substituting into the first congruence reveals that $q = 7$, and so we conclude that 7 is the only possible prime common divisor of y and $\mathrm{disc}(f_n(X))$. □

Lemma 3.11. *Let $(-3, y)$ be a solution in integers to $Y^r = f_n(X)$. If $q \neq 7$ is a prime*

divisor of y, then q splits completely in K.

Proof. Let q be a prime divisor of $y^r = \prod_{i=0}^{5}(-3-\rho_i)$. Choose a prime $\mathfrak{q}$ over q such that

$$\rho_0 \equiv -3 \mod \mathfrak{q}.$$

Apply equations (3.3) to conclude that

$$\rho_1 \equiv 4, \quad \rho_2 \equiv \frac{1}{2}, \quad \rho_3 \equiv -\frac{1}{5}, \quad \rho_4 \equiv -\frac{2}{3}, \quad \rho_5 \equiv -\frac{5}{4} \mod \mathfrak{q}. \tag{3.9}$$

The Galois group acts on the set of primes over q. If σ^2 stabilized $\mathfrak{q}$, then $\rho_0 \equiv \rho_2 \equiv \rho_4 \mod \mathfrak{q}$. Each of these congruences implies that $q = 7$. If σ^3 stabilized $\mathfrak{q}$, then $\rho_0 \equiv \rho_3 \mod \mathfrak{q}$. This implies that $q = 2$ or 7. Since $y^r = f_n(-3) = 120n + 37$, we know that 2 does not divide y. We conclude that any prime divisor q of y not equal 7, splits completely in K. □

3.4.3 Divisibility of the index $[\mathcal{O}_K^\times : U]$ redux.

Lemma 3.12. *Let $\ell \neq 3$ be an odd prime. Let $\mathfrak{q}$ be a prime of K such that $\rho_0 \equiv -3 \mod \mathfrak{q}$ and let q be the rational prime under $\mathfrak{q}$. Assume that q totally splits in K and that exactly two elements of the set $\{2,3,5\}$ are ℓ-th power residues mod q, while the third is an ℓ-th power non-residue mod q. Then $[\mathcal{O}_K^\times : U] \not\equiv 0 \mod \ell$.*

Proof. If ℓ divides $[\mathcal{O}_K^\times : U]$, then there is a unit $u \in \mathcal{O}_K^\times \setminus U$ such that $u^\ell = \pm\varepsilon^a\mu_0^b\mu_1^c\rho_0^d\rho_1^e$, with $a, b, c, d, e \in \{0, \ldots, \ell-1\}$. Since ℓ is odd we may, without loss of generality, assume

that u is such that

$$u^\ell = \varepsilon^a \mu_0^b \mu_1^c \rho_0^d \rho_1^e. \tag{3.10}$$

Upon taking norms $K \to k_2$ we find that $(N_{K|k_2}(u))^\ell = \varepsilon^{3a}$. If $a \neq 0$, use $\gcd(3a, \ell) = 1$ to write $\varepsilon = \varepsilon^{3as+\ell t} = (N_{K|k_2}(u^s)\varepsilon^t)^\ell$ for some $s, t \in \mathbb{Z}$. This contradicts the fact ε is the fundamental unit for k_2. We conclude that $a = 0$ and Equation (3.10) becomes

$$u^\ell = \mu_0^b \mu_1^c \rho_0^d \rho_1^e. \tag{3.11}$$

Taking norms $K \to k_3$, we find that $(N_{K|k_3}(u))^\ell = \mu_0^f \mu_1^g$, where $f = 2b + e$ and $g = 2c - d + e$. By absorbing any ℓth powers into the left hand side of this last equation, we may take it to have the form $v^\ell = \mu_0^f \mu_1^g$, with v a unit of k_3 and $f, g \in \{0, \ldots, \ell - 1\}$. Hence $(v^\sigma)^\ell = \mu_1^f \mu_2^g = \mu_0^{-g} \mu_1^{f-g}$. Since $\mu_0 \equiv -8/5 \mod \mathfrak{q}$ and $\mu_1 \equiv 5/3 \mod \mathfrak{q}$, we conclude that

$$v^\ell \equiv (-1)^f 2^{3f} 3^{-g} 5^{g-f} \mod \mathfrak{q},$$
$$(v^\sigma)^\ell \equiv (-1)^g 2^{-3g} 3^{g-f} 5^f \mod \mathfrak{q},$$

Since exactly two of the primes $\{2, 3, 5\}$ are ℓth power residues mod q while the third is an ℓth power nonresidue we conclude that $f \equiv g \equiv 0 \mod \ell$. Hence, up to a power of ℓ, we may replace e in Equation (3.11) with $-2b$ and d with $2(c - b)$ and so conclude that

there is a unit $w \in \mathcal{O}_K^\times \smallsetminus U$ such that

$$\begin{aligned} w^\ell &= (\mu_0/(\rho_0\rho_1)^2)^b(\mu_1\rho_0^2)^c \\ (w^\sigma)^\ell &= (\mu_1/(\rho_1\rho_2)^2)^b(\rho_1^2/(\mu_0\mu_1))^c. \end{aligned} \tag{3.12}$$

Applying Congruences (3.9) along with the congruences $\mu_0 \equiv -8/5 \mod \mathfrak{q}$ and $\mu_1 \equiv 5/3 \mod \mathfrak{q}$, we find that

$$\begin{aligned} w^\ell &\equiv (-1)^b 2^{-b} 3^{c-2b} 5^{c-b} \mod \mathfrak{q}, \\ (w^\sigma)^\ell &\equiv (-1)^c 2^{c-2b} 3^{c-b} 5^b \mod \mathfrak{q}. \end{aligned}$$

Since exactly two of the primes $\{2,3,5\}$ are ℓth power residues mod q while the third is an ℓth power nonresidue we conclude that $b \equiv c \equiv 0 \mod \ell$. Since $0 \leq b, c < \ell$, we conclude that $b = c = 0$. Hence $e \equiv -2b = 0 \mod \ell$ and so $e = 0$. Similarly $d \equiv 2(c-b) = 0 \mod \ell$ and so $d = 0$. Since $a = b = c = d = e = 0$, Equation (3.11) reduces to $u^\ell = 1$ and implies that $u = 1 \in U$. Since this contradicts our choice of u, we conclude that $[\mathcal{O}_K^\times : U] \not\equiv 0 \mod \ell$. □

Lemma 3.13. *Let $\mathfrak{q}$, $\mathfrak{q}_2$ be primes of K lying over the rational primes q, q_2 and such that $\rho_0 \equiv -3 \mod \mathfrak{q}, \mathfrak{q}_2$. Assume that these rational primes totally split in K. Assume further that 2 is a cubic residue mod q and exactly one element of the set $\{3,5\}$ is a ninth power residue mod q, while the other is a cubic non-residue mod q. Finally, assume that exactly two elements of the set $\{2,3,5\}$ are 9th power residues mod q_2, while the remaining element is a cubic non-residue mod q_2. Then the quotient $\mathcal{O}_K^\times/U$ does not contain an*

element of order 9.

Proof. Suppose the contrary. Then there is a unit $u \in \mathcal{O}_K^\times \smallsetminus U$ with $u^9 \in U$, but $u^i \notin U$ for $0 \leq i \leq 8$. Without loss of generality, we may take u to be such that

$$u^9 = \varepsilon^a \mu_0^b \mu_1^c \rho_0^d \rho_1^e, \tag{3.13}$$

with $a, b, c, d, e \in \{0, \ldots, 8\}$. Taking norms $K \to k_3$, we find that $(N_{K|k_3}(u))^9 = \pm\mu_0^f \mu_1^g$, where $f = 2b+e$ and $g = 2c-d+e$. By absorbing any ninth powers and factors of -1 into the left hand side of this last equation, we may take it to have the form $v^9 = \mu_0^f \mu_1^g$, with v a unit of k_3 and $f, g \in \{0, \ldots, 8\}$. Hence $(v^\sigma)^9 = \mu_1^f \mu_2^g = \mu_0^{-g} \mu_1^{f-g}$. Since $\mu_0 \equiv -8/5 \mod \mathfrak{q}$ and $\mu_1 \equiv 5/3 \mod \mathfrak{q}$, we conclude that

$$\begin{aligned} v^9 &\equiv (-1)^f 2^{3f} 3^{-g} 5^{g-f} \mod \mathfrak{q}, \\ (v^\sigma)^9 &\equiv (-1)^g 2^{-3g} 3^{g-f} 5^f \mod \mathfrak{q}, \end{aligned}$$

Since exactly one of the primes $\{3, 5\}$ is a ninth power residue mod q while the other is a cubic nonresidue we conclude that $f \equiv g \equiv 0 \mod 9$. Hence, up to a power of 9, we may replace e in Equation (3.13) with $-2b$ and d with $2(c-b)$ and so conclude that there is a unit $w \in \mathcal{O}_K^\times \smallsetminus U$ such that $w^9 = \varepsilon^a (\mu_0/(\rho_0\rho_1)^2)^b (\mu_1\rho_0^2)^c$ and $(w^\sigma)^9 = (\varepsilon^\sigma)^a (\mu_1/(\rho_1\rho_2)^2)^b (\rho_1^2/(\mu_0\mu_1))^c$. The product of these two units is a unit ϑ satisfying

$$\begin{aligned} \vartheta^9 &= \pm(\mu_0\mu_1/(\rho_0\rho_1^2\rho_2)^2)^b (\rho_0^2\rho_1^2/\mu_0)^c \\ (\vartheta^\sigma)^9 &= \pm(\mu_1\mu_2/(\rho_1\rho_2^2\rho_3)^2)^b (\rho_1^2\rho_2^2/\mu_1)^c \end{aligned} \tag{3.14}$$

Applying Congruences (3.9) along with the congruences $\mu_0 \equiv -8/5 \mod \mathfrak{q}$ and $\mu_1 \equiv 5/3 \mod \mathfrak{q}$, we find that

$$\vartheta^3 \equiv (-1)^{b+c} 2^{c-3b} 3^{2c-3b} 5^c \mod \mathfrak{q}_2,$$
$$(\vartheta^\sigma)^3 \equiv (-1)^b 2^{2c-3b} 3^c 5^{3b-c} \mod \mathfrak{q}_2.$$

Since exactly two of the primes $\{2, 3, 5\}$ are ninth power residues mod q_2 while the third is a cubic nonresidue we conclude that $c \equiv 0 \mod 9$ and $b \equiv 0 \mod 3$. Hence $e \equiv -2b = 0 \mod 3$ and $d \equiv 2(c-b) \equiv 0 \mod 3$. Since $b \equiv c \equiv d \equiv e \equiv 0 \mod 3$, we conclude via Equation (3.13) that there is a unit $\eta \in \mathcal{O}_K^\times$ such that $\eta^3 = \varepsilon^j$, $j \in \{0, 1, 2\}$ ($j \equiv a \mod 3$.) If $j \neq 0$, then $\varepsilon = \kappa^3$ for some $\kappa \in \mathcal{O}_K^\times$. Applying σ we conclude that $(\kappa\kappa^\sigma)^3 = \varepsilon\varepsilon^\sigma = \pm 1$. Hence $\kappa\kappa^\sigma = \pm 1$. Apply σ^5 to both sides of this last equation to conclude that $\kappa^{\sigma^5}\kappa = \pm 1$. Hence $\kappa^{\sigma^5} = \kappa^\sigma$ and so $\kappa^{\sigma^2} = \kappa$. But this means that $\kappa \in k_2$. Since ε cannot have a cube root in k_2 (because ε is its fundamental unit), we are forced to conclude that $j = 0$ and that $a \equiv 0 \mod 3$. Since $a \equiv b \equiv c \equiv d \equiv e \equiv 0 \mod 3$, we conclude from Equation (3.13) that $u^3 \in U$. Since this contradicts our choice of u, we conclude that $\mathcal{O}_K^\times / U$ does not contain an element of order 9. □

3.4.4 A class of odd order r

Proposition 3.14. *Let $(-3, y)$ be a solution to $Y^r = f_n(X)$. Assume that for every prime divisor $\ell \neq 3$ of r there are prime divisors $q, q_2 \neq 7$ of y such that*

1. *Exactly two elements of the set $\{2, 3, 5\}$ are ℓ-th power residues mod q, while the third is an ℓ-th power non-residue mod q.*

2. *The numbers* $2, 3,$ *and* 5 *are each* ℓ*-th power residues mod* q_2*, but* 7 *is an* ℓ*-th power non-residue.*

Then $(-3-\rho_0) \neq (\alpha)^\ell$ *for any prime divisor* $\ell \neq 3$ *of* r.

Proof. Note that $r \equiv 0 \mod 2$ and $y^r = f_n(-3) = 120n + 37$ imply that $120n + 37$ is a square and hence that 2 is a quadratic residue mod 5. Since this is impossible, r is odd. If $(-3-\rho_0) = (\alpha)^\ell$, then $-3-\rho_0 = u\alpha^\ell$, where u is a unit. The primes q and q_2 split completely in K by Lemma 3.11. Let $\mathfrak{q}$ and $\mathfrak{q}_2$ denote primes of K above q and q_2 which contain $-3-\rho_0$. Since the hypotheses of (Lemma 3.12) are satisfied, ℓ does not divide $[\mathcal{O}_K^\times : U]$. Hence we may write

$$-3-\rho_0 = \pm\varepsilon^a \mu_0^b \mu_1^c \rho_0^d \rho_1^e \alpha_1^\ell.$$

Apply σ and σ^4 to find that

$$-3-\rho_1 = \pm(\varepsilon^\sigma)^a \mu_0^{-c} \mu_1^{b-c} \rho_1^d \rho_2^e (\alpha_1^\sigma)^\ell$$

$$-3-\rho_4 = \pm\varepsilon^a \mu_0^{-c} \mu_1^{b-c} \rho_4^d \rho_5^e (\alpha_1^{\sigma^4})^\ell.$$

Multiply these equations to find that

$$(-3-\rho_1)(-3-\rho_4) = (\varepsilon\varepsilon^\sigma)^a \mu_0^{-2c+d-e} \mu_1^{2(b-c)+d} (\alpha_1^{\sigma+\sigma^4})^\ell.$$

Apply Congruences (3.9) to both sides of this equation to conclude that

$$7^2 \equiv \pm 2^{-6c+3(d-e)} 3^{2(c-b)-d} 5^{e+2b} (\alpha_1^{\sigma+\sigma^4})^\ell \bmod \mathfrak{q}_2.$$

We conclude that 7^2 and hence 7 is an ℓth power residue mod q_2, and since this contradicts one of our hypotheses, we conclude that $(-3-\rho_0)$ is not the ℓth power of a principal ideal. □

Proposition 3.15. *Let $(-3, y)$ be a solution to $Y^r = f_n(X)$, with $r \equiv 0 \mod 3$. Assume that there are prime divisors $q, q_2, q_3 \neq 7$ of y such that $q_3 \equiv 1 \mod 9$ and*

1. *2 is a cubic residue mod q and exactly one element of the set $\{3, 5\}$ is a ninth power residue mod q, while the other is a cubic non-residue mod q.*
2. *Exactly two elements of the set $\{2, 3, 5\}$ are 9th power residues mod q_2, while the remaining element is a cubic non-residue mod q_2.*
3. *2 is a cubic residue mod q_3, 3 and 5 are each 9th power residues mod q_3, and 7 is a cubic non-residue mod q_3.*

Then $(-3-\rho_0)$ is not the cube of a principal ideal.

Proof. If $(-3-\rho_0) = (\alpha)^3$, then $-3-\rho_0 = u\alpha^3$, where u is a unit. The primes q and q_2 split completely in K by Lemma 3.11. Let $\mathfrak{q}$ and $\mathfrak{q}_2$ denote primes of K above q and q_2 which contain $-3-\rho_0$. Since the hypotheses of (Lemma 3.13) are satisfied, $\mathcal{O}_K^\times/U$ does not contain an element of order 9. Hence we may write

$$-(3+\rho_0)^3 = \pm\varepsilon^a \mu_0^b \mu_1^c \rho_0^d \rho_1^e \alpha_1^9.$$

Apply σ and σ^4 to find that

$$-(3+\rho_1)^3 = \pm(\varepsilon^\sigma)^a \mu_0^{-c} \mu_1^{b-c} \rho_1^d \rho_2^e (\alpha_1^\sigma)^9$$
$$-(3+\rho_4)^3 = \pm\varepsilon^a \mu_0^{-c} \mu_1^{b-c} \rho_4^d \rho_5^e (\alpha_1^{\sigma^4})^9.$$

Multiply these equations to find that

$$(3+\rho_1)^3(3+\rho_4)^3 = (\varepsilon\varepsilon^\sigma)^a \mu_0^{-2c+d-e} \mu_1^{2(b-c)+d} (\alpha_1^{\sigma+\sigma^4})^9.$$

Apply Congruences (3.9) to both sides of this equation to conclude that

$$7^6 \equiv \pm 2^{-6c+3(d-e)} 3^{2(c-b)-d+3} 5^{e+2b} (\alpha_1^{\sigma+\sigma^4})^9 \bmod \mathfrak{q}_3.$$

We conclude that 7^6 is a ninth power residue mod q_3; say $7^6 \equiv z^9 \mod q_3$. Let ζ be a generator for $(\mathbb{Z}/q_3\mathbb{Z})^\times$ and write $z \equiv \zeta^s \mod q_3$ and $7 \equiv \zeta^t \mod q_3$ for integers s and t. Then $\zeta^{9s-6t} \equiv 1 \mod q_3$ and since $q_3 \equiv 1 \mod 9$, we conclude that $t \equiv 0 \mod 3$. But this implies that 7 is a cubic residue mod q_3; a contradiction to one of our hypotheses. We conclude that $(-3-\rho_0)$ is not the cube of a principal ideal. □

Corollary 3.16. *Let $(-3, y)$ be a solution in integers to $Y^r = f_n(X)$. Assume that for every prime divisor of r not equal to 3 there are corresponding primes q, q_2 satisfying the hypotheses of Proposition 3.14 and that if $r \equiv 0 \mod 3$, that there are corresponding primes q, q_2, q_3 satisfying the hypotheses of Proposition 3.15. Then $(-3-\rho_0) = \mathfrak{a}^r$, where $\mathfrak{a}$ is a representative of a class of order r in Cl_K.*

Proof. According to Lemma 3.10 none of the prime factors of y divide $\mathrm{disc}(f_n(X))$, and according to Lemma 3.11 any prime factor of y splits completely in K. The hypotheses of Lemma 3.9 are satisfied and allow us to conclude that $(-3-\rho_0) = \mathfrak{a}^r$, for some ideal $\mathfrak{a}$ of K. To show that $\mathfrak{a}$ has order r upon passing to the class group, we must show that no smaller positive power of $\mathfrak{a}$ is principal. If this was not the case, and some smaller positive power of $\mathfrak{a}$ was principal, then we would conclude that $(-3-\rho_0)$ is the ℓth power of a principal ideal for some $\ell > 1$ dividing r. Since a power of a principal ideal is principal we may, without loss of generality, take ℓ to be prime. Since the hypotheses of Propositions 3.14 and 3.15 are satisfied, $(-3-\rho_0)$ is not the ℓth power of principal ideal for any prime ℓ dividing r. Hence $\mathfrak{a}$ is a representative of a class of order r. □

3.5 On the origin of the ideal classes.

Under sufficient conditions the ideal classes of order r that we detect are not coming from ideal classes of the quadratic or cubic subfields.

Definition 3.17. *A relative ideal class is an ideal class with trivial norm down to both the quadratic and cubic subfields.*

Remark 3.18. *The next theorem relies on the existence of primes satisfying a set of congruence conditions. This is established in the section immediately following this one.*

Theorem 3.19. *Let $r \not\equiv 0 \mod 3$ be an odd positive integer and let $(-3, c_r(120(7)y +$*

37)) *be a solution in integers to* $Y^r = f_n(X)$, *where* c_r *is a constant which is not divisible by* 7 *and is chosen such that* $(37c_r)^r \equiv 37 \mod 120$ *and such that for each prime divisor* ℓ *of* r *there are corresponding prime divisors* q_2, q_3, q_4 *of* c_r *for which*

1. *All three of the primes* $2, 3, 5$ *are* ℓ*th power residues mod* q_2, *while* 7 *is an* ℓ*th power non-residue mod* q_2.
2. 2 *and* 3 *are* r*th power residues mod* q_3, *while* 5 *is an* ℓ*th power non-residue mod* q_3.
3. 3 *and* 5 *are* r*th power residues mod* q_4, *while* 2 *is an* ℓ*th power non-residue mod* q_4.

Then there are infinitely many distinct fields in the family $\{K_n\}$ *for which*

$$\left(\frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)}\right) = \mathfrak{c}^r,$$

where $[\mathfrak{c}] \in \mathrm{Cl}_K$ *is a relative ideal class of order* r.

Proof. That $(-3-\rho_0) = \mathfrak{a}^r$, for some ideal $[\mathfrak{a}]$, is Corollary 3.16. It follows that

$$\left(\frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)}\right) = \mathfrak{c}^r,$$

for some ideal $\mathfrak{c}$. If $[\mathfrak{c}]$ does not have order r, then there is a prime $\ell \mid r$ such that $\mathfrak{c}^{r/\ell}$ is principal. Hence

$$w := \frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)} = uz^\ell,$$

for some $u \in \mathcal{O}_K^\times$ and some $z \in K^\times$. Our hypotheses ensure that ℓ doesn't divide the index $[\mathcal{O}_K^\times : \langle -1, \varepsilon, \mu_0, \mu_1, \rho_0, \rho_1\rangle]$, so we may assume $u \in \langle -1, \varepsilon, \mu_0, \mu_1, \rho_0, \rho_1\rangle$. Since w has norm one down to k_2 and k_3, we conclude that the norm of u down to both subfields is an ℓth power. We now proceed in the same manner as we did to produce Equations (3.10)

and (3.11). Since ℓ is odd, we may ignore -1 and write

$$u = \varepsilon^a \mu_0^b \mu_1^c \rho_0^d \rho_1^e.$$

Taking norms $K \to k_2$, we find that

$$\varepsilon^{3a} = N_{K|k_2}(u) = N_{K|k_2}(z)^{-\ell}$$

Hence $\ell \mid a$ and we can absorb ε^a into z^ℓ.

Taking norms $K \to k_3$, we find that

$$N_{K|k_3}(z)^{-\ell} = N_{K|k_3}(u) = (\pm 1)^a \mu_0^{2b+e} \mu_1^{2c-d+e}.$$

Since $\ell \nmid [\mathcal{O}_K^\times : \langle -1, \varepsilon, \mu_0, \mu_1, \rho_0, \rho_1 \rangle]$, we conclude that

$$2b + e \equiv 0 \mod \ell$$

$$2c - d + e \equiv 0 \mod \ell.$$

Hence, $e \equiv -2b$ and $d \equiv 2c - 2b \mod \ell$. Thus

$$w = \frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)} = \mu_0^b \mu_1^c \rho_0^{2c-2b} \rho_1^{-2b} z_1^\ell,$$

for some $z_1 \in K^\times$. Applying Congruences (3.9) we find that

$$6 \equiv 2^{-b}3^{c-2b}5^{c-b} \times (\ell\text{th power}) \mod q_3,\ q_4.$$

Our power residue hypotheses then imply that $c \equiv b \equiv -1 \mod \ell$. Hence $e \equiv 2$ and $d \equiv 0 \mod \ell$. Thus there exists $z_2 \in K^\times$ such that

$$\begin{aligned} w &= \mu_0^{-1}\mu_1^{-1}\rho_1^2 z_2^\ell \\ &= (\rho_1\rho_4)^{-1}\rho_1^2 z_2^\ell \\ &= \frac{\rho_1}{\rho_4} z_2^\ell, \end{aligned}$$

or

$$\frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)}\rho_4\rho_1^{-1} = z_2^\ell.$$

It will suffice to show that the polynomial $Z^r - w\rho_4\rho_1^{-1}$ is irreducible in $K[Z]$, since this guarantees that $w\rho_4\rho_1^{-1} \notin (K^\times)^\ell$ for any prime ℓ dividing r. Toward this end we note that the minimal polynomial over $\mathbb{Q}$ of $\frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)}\rho_4\rho_1^{-1}$ is

$$Z^6 + a_5Z^5 + a_4Z^4 + a_3Z^3 + a_2Z^2 + a_1Z + 1,$$

where

$$a_1 = a_5 = -6$$
$$a_2 = a_4 = \frac{-1666384n^2 - 5513952n - 16920921}{(120n+37)^2}$$
$$a_3 = \frac{-4052768n^2 - 11471904n - 33910292}{(120n+37)^2}.$$

Clearing denominators and replacing Z with Z^r, we obtain the polynomial

$$p_n(Z) := b_6 Z^{6r} + b_5 Z^{5r} + b_4 Z^{4r} + b_3 Z^{3r} + b_2 Z^{2r} + b_1 Z^r + b_0,$$

where

$$b_0 = b_6 = (120n+37)^2$$
$$b_1 = b_5 = -6(120n+37)^2$$
$$b_2 = b_4 = -1666384n^2 - 5513952n - 16920921$$
$$b_3 = -4052768n^2 - 11471904n - 33910292.$$

When $p_n(Z)$ is irreducible over $\mathbb{Q}$, $Z^r - w\rho_4\rho_1^{-1}$ is irreducible in $K[Z]$ and we reach the contradiction that $z_2 \notin K$. We are then forced to conclude that the ideal class of $\mathfrak{c}$ has order r.

For infinitely many primes q, the polynomial

$$(X^r - 37 - 120(-3 - \sqrt{-27})/2)(X^r - 37 - 120(-3 + \sqrt{-27})/2) \in \mathbb{Z}[X]$$

splits into linear factors mod q. Let q be such a prime. If b is a zero mod q, then

$$b^r \equiv 37 + 120(-3 \pm \sqrt{-27})/2 \mod q.$$

So, choose $n_0 \equiv (-3 \pm \sqrt{-27})/2 \mod q$. Then $n_0^2 + 3n_0 + 9 \equiv 0 \mod q$. By perhaps adding q to n_0, we may take n_0 to be such that $n_0^2 + 3n_0 + 9 \equiv 0 \mod q$, but $n_0^2 + 3n_0 + 9 \not\equiv 0 \mod q^2$.

Furthermore, because there are infinitely many such q, we may take q to not divide r, $840c_r$ and $|37 + 120(-3 \pm \sqrt{-27})/2|^2$. Then $q \nmid b$ and

$$b^r \equiv 120n_0 + 37 \mod q.$$

By Hensel's Lemma, there exists $b_0 \equiv b \mod q$, with

$$b_0^r \equiv 37 + 120n_0 \mod q^2.$$

Now choose y_0 such that

$$c_r(840y_0 + 37) \equiv b_0 \mod q^2.$$

Let $m \in \mathbb{Z}$. Then

$$c_r(840(y_0 + mq^2) + 37) \equiv b_0 \mod q^2.$$

Hence

$$[c_r(840(y_0 + mq^2) + 37)]^r \equiv 37 + 120n_0 \mod q^2.$$

Noting that

$$[c_r(840(y_0 + mq^2) + 37)]^r \equiv 37 \mod 120,$$

we may write

$$[c_r(840(y_0 + mq^2) + 37)]^r = 120n + 37,$$

for some $n \in \mathbb{Z}$. Furthermore, since $120n \equiv 120n_0 \mod q^2$, we see that $n \equiv n_0 \mod q^2$. Hence $n^2 + 3n + 9$ is divisible by q but not by q^2. Solving for n in this last equation, we conclude that $p_n(Z) = g(m, Z)$, where

$$g(X, Z) := b_6(X)Z^{6r} + b_5(X)Z^{5r} + \cdots + b_1(X)Z^r + b_0(X),$$

and where, for example,

$$b_0(X) = b_6(X) = [c_r(840(y_0 + Xq^2) + 37)]^{2r}$$

The polynomial $g(X, Z)$ is irreducible in $\mathbb{Q}[X, Z]$. Indeed, if not, then any specialization $g(x, Z) \in \mathbb{Q}[Z]$ would be reducible. But, for example, choosing $X = x \in \mathbb{Q}$ such that $c_r(840(y_0 + Xq^2) + 37) = 1$ (corresponding to $n = -3/10$), we obtain the irreducible

polynomial

$$p_{-3/10}(Z) = Z^{6r} - 6Z^{5r} - \frac{385417749}{25}Z^{4r} - \frac{770836748}{25}Z^{3r} - \frac{385417749}{25}Z^{2r} - 6Z^r + 1.$$

To see that this polynomial is irreducible over $\mathbb{Q}$, consider the polynomial

$$h_1(Z) := Z^6 - 6Z^5 - \frac{385417749}{25}Z^4 - \frac{770836748}{25}Z^3 - \frac{385417749}{25}Z^2 - 6Z + 1,$$

and let v be a zero of $h_1(Z)$. Note that 5 splits completely in the field $\mathbb{Q}(v)$. From the symmetry of h_1 it is clear that $1/v$ is also a zero of h_1. Setting

$$\begin{aligned} h_2(Z) &:= 5^6 h_1(Z/5) \\ &= Z^6 - 30Z^5 - 385417749Z^4 - 3854183740Z^3 \\ &\quad + 9635443725Z^2 - 18750Z + 15625, \end{aligned}$$

we note that $5v$ is a zero of h_2 and so is an algebraic integer in the field $\mathbb{Q}(v)$. Since v isn't an algebraic integer, it has some prime ideals in its denominator. But 5 splits completely and $5v$ is an algebraic integer, so v must have the first power of some prime ideal in its denominator. Hence v cannot be the ℓth power of of some element of $\mathbb{Q}(v)$ for any prime ℓ dividing r. Applying a result found in Lang's Algebra [10], we conclude that $Z^r - v$ is irreducible in $\mathbb{Q}(v)[Z]$. Hence $p_{-3/10}(Z)$ is irreducible over $\mathbb{Q}$. Irreducibility of $g(X, Z)$

and the polynomial obtained upon clearing denominators are equivalent. Hilbert's Irreducibility Theorem [9] states that if $g(X, Z)$ is an irreducible polynomial in X and Z with coefficients in $\mathbb{Z}$, then there are infinitely many integers m for which $g(m, Z)$ is an irreducible polynomial in $\mathbb{Z}[Z]$. We conclude that there are infinitely many parameter values n for which $\frac{(-3-\rho_1)(-3-\rho_2)}{(-3-\rho_4)(-3-\rho_5)} = \mathfrak{c}^r$, where $\mathfrak{c}$ represents a class of order r in Cl_K . Furthermore, by allowing the prime q to vary we see that we obtain infinitely many distinct fields for which this is true, because q ramifies in the quadratic subfield $\mathbb{Q}(\sqrt{n^2+3n+9})$. Since w has norm 1 down to both the cubic and quadratic subfields we conclude that $\mathfrak{c}$ has trivial norm down to both subfields. Hence $[\mathfrak{c}] \in \mathrm{Cl}_K$ is mapped to the trivial element of Cl_{k_2} and Cl_{k_3} and is a relative ideal class. □

3.6 Existence of infinitely many fields of the family with $r \mid h_K$ for arbitrary odd integer $r > 1$.

Our method detects infinitely many distinct fields containing a cyclic subgroup of arbitrary odd order. As in the previous chapter and as in the following chapter, the existence of a field K_n of our family with class number divisible by r is the essential step; once existence is established the existence of infinitely many distinct fields of our family with class number divisible by r follows. Existence requires demonstrating that there are infinitely many primes satisfying the congruence conditions sufficient to guarantee the existence of a class of order r, and this is accomplished with an appeal to Bauer's Theorem in the following Lemmas and Remarks.

Lemma 3.20. *Let ℓ be a prime. There are infinitely many primes q for which, for example, 2 and 3 are ℓth power residues mod q, but for which 5 is an ℓth power nonresidue mod q.*

Proof. Let

$$L = \mathbb{Q}(\zeta_\ell, 2^{1/\ell}, 3^{1/\ell})$$

$$L' = \mathbb{Q}(\zeta_{2\ell}, 5^{1/\ell})$$

ζ_ℓ (resp. $\zeta_{2\ell}$) denotes a primitive ℓth (resp. 2ℓth) root of unity. A rational prime q splits completely in L if and only if $q \equiv 1 \bmod \ell$ and $2, 3$ are ℓth power residues mod q. A rational prime q splits completely in L' if and only if $q \equiv 1 \bmod 2\ell$ and 5 is an ℓth power residue mod q. Since $L' \not\subset L$, we may apply Bauer's Theorem [2] to conclude that there are infinitely many primes that split in L and do not split in L'. Hence there are infinitely many primes q for which 2 and 3 are ℓth power residues mod q but for which 5 is an ℓth power nonresidue mod q. □

Remark 3.21. *The previous lemma makes clear that there are infinitely many primes q for which exactly two elements of the set $\{2, 3, 5\}$ are ℓth power residues mod q, while the third is an ℓth power nonresidue mod q.*

Lemma 3.22. *Let ℓ be a prime. There are infinitely many primes q_2 for which $2, 3$, and 5 are ℓth power residues modulo q_2, but for which 7 is an ℓth power nonresidue modulo q_2.*

Proof. The proof is extremely similar to that used in Lemma 3.20. □

Remark 3.23. *A similar proof may be used to show that there are infinitely many triples*

of primes (q, q_2, q_3) *satisfying the power residue hypotheses of Proposition 3.15.*

Theorem 3.24. *Let* r *be an arbitrary odd positive integer* > 1*. This family of sextic fields contains infinitely many members with class number divisible by* r*.*

Proof. Let ℓ be a prime dividing r. Choose a pair of primes $(q_\ell, q_{2,\ell})$ satisfying the power residue hypotheses of Proposition 3.14 for each odd prime $\ell \neq 3$ dividing r. For $\ell = 3$, choose a triple of primes $(q_\ell, q_{2,\ell}, q_{3,\ell})$ satisfying the power residue hypotheses of Proposition 3.15. Make sure never to choose $2, 3, 5$, or 7, for any of the primes. (This presents no problem since, by the remarks immediately preceding this Theorem, there are infinitely many pairs/triples of primes satisfying these hypotheses.) Let p denote the product of the chosen primes. Note that $|\mathbb{Z}/120\mathbb{Z}^\times| = 32 = 2^5$. Since $\gcd(r, 2) = 1$, 37 is an rth power mod 120. Choose s such that

$$(sp)^r \equiv 37 \mod 120.$$

Then the pair $(-3, sp)$ is a solution in integers to $Y^r = f_n(X)$ for some n and from Corollary 3.16 we conclude that $r \mid h_n$. Thus for an arbitrary odd $r > 1$, there is an element, K_n, of this family of sextics which has class number divisible by r.

This result now implies that there are infinitely many members of this family of degree 6 extensions whose class number is divisible by r. Indeed, suppose that K_n is such that $r \mid h_n$. Let r^ω be the greatest power of r dividing h_n. From the previous paragraph we know that there is a sextic field $K_{n'}$ in this family for which $r^{\omega+1}$ divides $h_{n'}$. But

$K_{n'} \neq K_n$, since they have different class numbers. Thus given any finite number of sextic fields with class number divisible by r, we can find an additional one. We conclude that this family of sextic fields contains infinitely many members with class number divisible by r. $\square$

Chapter 4: A Family of Non-Galois Cubic Extensions of $\mathbb{Q}$.

We restrict attention in this chapter to cubic extensions of the form $\mathbb{Q}(\rho)/\mathbb{Q}$, where ρ is a root of the polynomial

$$f_n(X) := X^3 + nX^2 + nX - 1 \in \mathbb{Z}[X],$$

with $n \in \mathbb{Z}$, $0 \neq n \in \mathbb{Z}$. From Corollary 4.8 onwards, we'll assume n is odd and $n \geq 5$.

Let $r \geq 1$ be an otherwise arbitrary integer. Our main results shows that this family of non-Galois cubic extensions contains infinitely many distinct fields whose class group contains a cyclic subgroup of order r. The non-Galois nature of these extensions prevents us from directly applying the techniques used by us to investigate the families of quartic and sextic extensions above. Indeed, it was the Galois group's action on the roots that allowed us determine what each root was congruent to modulo a prime, that allowed us to show that certain primes did not divide the index of our group of units in the full group of units, and ultimately allowed us to show that our chosen principal ideal was not itself a prime power of a principal ideal. Applying the Galois group of the degree 6 splitting field of $f_n(X)$ in the analogous situation here has the undesirable effect of moving us out of the cubic field we are studying (and into an isomorphic cubic field.) Nevertheless, by

applying the splitting field's Galois group and then taking products of the resulting expressions, we find that much of the same arguments go through and allow us to apply our techniques to a setting in which they would appear, at first glance, not amenable.

4.1 Irreducibility of f_n.

Proposition 4.1. *$f_n(X)$ is irreducible over $\mathbb{Q}$.*

Proof. Note that f is reducible over $\mathbb{Q}$ if and only if it has a root in $\mathbb{Z}$. Any such root would be ± 1. But $f(1) = 2n \neq 0$ and $f(-1) = -2 \neq 0$, so we conclude that f is irreducible over $\mathbb{Q}$. □

4.2 Roots of f_n.

Lemma 4.2. *ρ is a root of $f_n(X) = 0$ if and only if $1/\rho$ is a root of $f_{-n}(X) = 0$.*

Proof. Note that 0 is not a zero of $f_n(X)$. If ρ is a root of $f_n(X) = 0$, then $\rho^3 + n\rho^2 + n\rho - 1 = 0$. Divide both sides of the last equation by $-\rho^3$ to find that $(1/\rho)^3 - n(1/\rho)^2 - n(1/\rho) - 1 = 0$. This argument is reversible. □

Remark 4.3. *Let K_n denote the splitting field of $f_n(X)$. Lemma 4.2 implies that $K_n = K_{-n}$. For this reason we will restrict our attention to positive values of the parameter n.*

Proposition 4.4. *$(1-n, 2-n)$, $(-1-3/n, -1-1/n)$, and $(1/(n+1), 1/n)$.*

Proof. When $n \geq 7$, note that $f(1-n) = -n < 0$, $f(2-n) = n^2 - 6n + 7 > 0$, $f(-1-3/n) = (n^3 - 27n - 27)/n^3 > 0$, $f(-1-1/n) = -(n^3 + 2n^2 + 3n + 1)/n^3 < 0$,

$f(1/(n+1)) = -n/(n^3+3n^2+3n+1) < 0$, and that $f(1/n) = (n^2+1)/n^3 > 0$. Now apply the Intermediate Value Theorem to obtain the result for $n \geq 7$, and check the remaining two cases $n = 5, 6$ by hand. □

Remark 4.5. *When $|n| \leq 4$, some roots are complex.*

Remark 4.6. *We denote the roots of $f_n(X) = 0$ by ρ_i $(i \in \{0,1,2\})$, and we order these roots according to their absolute value with ρ_0 denoting the root of greatest magnitude. Applying Proposition 4.4 we note that when $n \geq 7$,*

$$-(n-1) < \rho_0 < -(n-2),$$

$$-1-3/n < \rho_1 < -1-1/n,$$

$$1/(n+1) < \rho_2 < 1/n.$$

4.3 $\mathrm{Gal}(f_n)$ and structure of the splitting field K_n.

Proposition 4.7. *Let K_n denote the splitting field of f_n. Then $\mathrm{disc}(f_n) = n^4 - 18n^2 - 27$ and the Galois group $\mathrm{Gal}(K_n/\mathbb{Q}) \cong S_3$.*

Proof. The Galois group, $\mathrm{Gal}(K_n/\mathbb{Q})$, is isomorphic to a transitive subgroup of S_3; hence to either A_3 or S_3. If it was isomorphic to A_3, then the discriminant of f_n would be a square in $\mathbb{Q}$. We now show that this is not the case and hence that

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong S_3.$$

First note that $\mathrm{disc}(f_n) = (n')^2 - 2^2 3^3$, where $n' := n^2 - 9$.

By way of contradiction, assume that $\mathrm{disc}(f_n)$ is a square in $\mathbb{Q}$. Then it is a square in $\mathbb{Z}$; say $\mathrm{disc}(f_n) = m^2$. Without loss of generality, we may assume $m > 0$. Then $(n' + m)(n' - m) = 2^2 3^3$. Since $n' + m$ and $n' - m$ have the same parity, we conclude that one of the following possibilities holds:

$$(n' + m, n' - m) = (2 \cdot 3^3, 2)$$

$$(n' + m, n' - m) = (2 \cdot 3^2, 2 \cdot 3)$$

$$(n' + m, n' - m) = (-2, -2 \cdot 3^3)$$

$$(n' + m, n' - m) = (-2 \cdot 3, -2 \cdot 3^2).$$

These possibilities imply that $n' = 28, 12, -28$, or -12, and since none of these are of the form $n^2 - 9$, we conclude that $\mathrm{disc}(f_n)$ is not a square. Hence

$$S_3 \cong \mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2 \rangle,$$

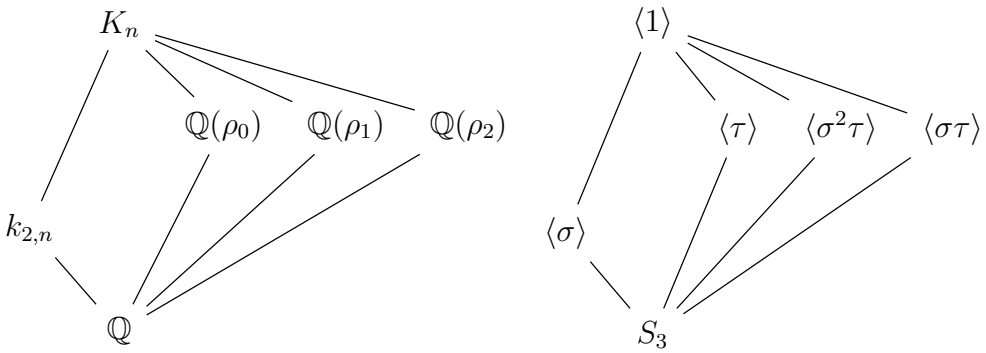
as claimed. □

Corollary 4.8. *The splitting field K_n has a unique quadratic subfield $k_{2,n}$ and three conjugate totally real cubic subfields $k_{3,n} := \mathbb{Q}(\rho_0)$, $k'_{3,n} = \mathbb{Q}(\rho_1)$, and $k''_{3,n} = \mathbb{Q}(\rho_2)$.*

Proof. Each root of $f_n(X)$ is real, so the cubic extensions of $\mathbb{Q}$ are real. Note that S_3 has a unique subgroup of order 3 and 3 conjugate subgroups of order 2 and apply the

Fundamental Theorem of Galois Theory. □

Let $\sigma = (012)$, $\tau = (12)$, $\sigma\tau = (01)$, $\sigma^2\tau = (02)$. Then the lattice of subfields of K_n and the corresponding lattice of subgroups of S_3 are given by the following diagrams:



4.4 Discriminants; behavior of primes.

Let $k_3 = \mathbb{Q}(\rho_0)$, and we continue to assume n is an odd integer.

Lemma 4.9. 2 *totally ramifies in* k_3.

Proof. Define

$$g(X) := f_n(X-1) = X^3 + (n-3)X^2 - (n-3)X - 2.$$

g is Eisenstein at 2. Hence 2 is totally ramified in the extension generated by a root of $g(X)$. Thus 2 is totally ramified in $\mathbb{Q}(\rho_0 + 1) = \mathbb{Q}(\rho_0) = k_3$. □

Lemma 4.10. $\mathrm{disc}(f_n) = n^4 - 18n^2 - 27 \equiv 4 \ \textit{mod}\ 8$.

Proof. We have already shown that $\mathrm{disc}(f_n) = n^4 - 18n^2 - 27$ (Proposition 4.7).

$$\begin{aligned} n^4 - 18n^2 - 27 &\equiv 1 - 18 + 5 \bmod 16 \\ &\equiv -12 \bmod 16 \\ &\equiv 4 \bmod 16. \end{aligned}$$

□

Remark 4.11. *Lemma 4.10 shows that* $\mathrm{disc}(f_n)$ *is never square-free; it is divisible by* 4 *but not by any greater power of* 2.

Definition 4.12. *An integer is said to be odd-square-free if it is not divisible by the square of any odd prime.*

Lemma 4.13. *If* $\mathrm{disc}(f_n)$ *is odd-square free, then* $\mathrm{disc}(\mathcal{O}_{k_3}/\mathbb{Z}) = \mathrm{disc}(f_n) = n^4 - 18n^2 - 27$.

Proof. From the fact that $\mathrm{disc}(f_n)$ is odd-square free and the relation

$$\mathrm{disc}(f_n) = [\mathcal{O}_{k_3} : \mathbb{Z}[\rho]]^2 \, \mathrm{disc}(\mathcal{O}_{k_3}/\mathbb{Z}),$$

we conclude that any odd prime dividing $\mathrm{disc}(f_n)$ also divides $\mathrm{disc}(\mathcal{O}_{k_3}/\mathbb{Z})$. The exact power of 2 dividing $\mathrm{disc}(f_n)$ is 4 (Remark 4.11) and 2 divides $\mathrm{disc}(\mathcal{O}_{k_3}/\mathbb{Z})$ (Lemma 4.9). Hence 4 divides $\mathrm{disc}(\mathcal{O}_{k_3}/\mathbb{Z})$ and $\mathrm{disc}(f_n) \mid \mathrm{disc}(\mathcal{O}_{k_3}/\mathbb{Z})$. □

4.5 Units

Let ρ denote a zero of $f_n(X)$ and let $k_3 = \mathbb{Q}(\rho)$. Dirichlet's Unit Theorem tells us that the rank of the unit group $\mathcal{O}_{k_3}^{\times}$ is 2, and that the rank of the unit group of $\mathcal{O}_K^{\times}$ is 5. Candidates for a multiplicatively independent subset of units were easy to identify in our study of the quartic and sextic families above. ρ is obviously a unit of k_3, but a second unit, μ, of k_3 which is multiplicatively independent of ρ is less obvious. To find such a unit we analyze the norm of an arbitrary element of k_3. We then study their total positivity and regulator, and ultimately provide sufficient conditions for $\{\rho, \mu\}$ to form a fundamental set of units for k_3.

Lemma 4.14. *Let a, b, c be integers. Then*

$$N_{k_3|\mathbb{Q}}(a + b\rho + c\rho^2) = (a^2c + ac^2 - abc)n^2 - (2a^2c + a^2b - 2ac^2 - ab^2 - bc^2 + b^2c)n + (a^3 + b^3 + c^3 - 3abc)$$

Proof. With respect to the ordered basis $\{1, \rho, \rho^2\}$ the $\mathbb{Q}$-endomorphism of k_3 corresponding to multiplication by the element $a + b\rho + c\rho^2$ is represented by the matrix

$$M := \begin{pmatrix} a & c & b - cn \\ b & a - cn & c - bn + cn^2 \\ c & b - cn & a - (b + c)n + cn^2 \end{pmatrix}.$$

Hence

$$\begin{aligned} N_{k_3|\mathbb{Q}}(a+b\rho+c\rho^2) &= \det(M) \\ &= (a^2c+ac^2-abc)n^2-(2a^2c+a^2b-2ac^2-ab^2-bc^2+b^2c)n \\ &\quad +(a^3+b^3+c^3-3abc). \end{aligned}$$

□

Lemma 4.15. *When n is odd,*

$$\mu := \left(\frac{n+3}{2}\right)(1+\rho)+\rho^2 \in \mathcal{O}_{k_3}^{\times}$$

with $N_{k_3|\mathbb{Q}}(\mu)=1$.

Proof. Substitute $a=b=(n+3)/2$ and $c=1$ into the expression for $N_{k_3|\mathbb{Q}}(a+b\rho+c\rho^2)$ in Lemma 4.14 to find that $N_{k_3|\mathbb{Q}}(\mu)=1$. □

 *Unless explicitly stated otherwise, the parameter n will henceforth be assumed to be an odd positive integer not less than 5.*

4.5.1 Signs of ρ and μ; total positivity.

Lemma 4.16. *ρ and μ have differing sign when $\rho<-1$, but have the same sign for $\rho\in(-1,0)\cup(0,\infty)$.*

Proof. Solve the equation $\rho^3+n\rho^2+n\rho-1=0$ for n to find that $n=(1-\rho^3)/(\rho^2+\rho)$.

Hence $(n+3)/2 = -(\rho^3 - 3\rho^2 - 3\rho - 1)/(2(\rho^2+\rho))$, and

$$\begin{aligned}\mu &= \left(\frac{n+3}{2}\right)(1+\rho) + \rho^2 \\ &= \frac{\rho^3 + 3\rho^2 + 3\rho + 1}{2\rho} \\ &= \frac{(\rho+1)^3}{2\rho}\end{aligned} \tag{4.1}$$

It is now clear that when $\rho < -1$, $\mu > 0$ and hence that ρ and μ have different signs. For $\rho \in (-1, 0)$ we find that $\mu < 0$ and hence that ρ and μ have the same sign. For $\rho > 0$, μ is positive and hence ρ and μ have the same sign. □

Corollary 4.17. *ρ_i and μ_i differ in sign for $i = 0, 1$, but have the same sign for $i = 2$.*

Proof. Proposition 4.4 and Remark 4.6 give the intervals in which the ρ_i lie. □

Corollary 4.18. *ρ is not totally positive, but μ is totally positive.*

Proof. That ρ is not totally positive follows from Proposition 4.4 and Remark 4.6. For $n \geq 5$, $\rho_2 > 0$, while $\rho_0, \rho_1 < 0$. So from Corollary 4.17 μ_0, μ_1, and μ_2 are all positive.

□

4.5.2 Regulator of $\{\rho, \mu\}$

Proposition 4.19. *The set $\{\rho, \mu\}$ forms a multiplicatively independent subset of k_3. Let R' denote the regulator of $\{\rho, \mu\}$. For $n \geq 17$,*

$$R' \leq \left(\frac{11}{3}\right)\log(n-1)\log(n+3).$$

Proof.

$$R' = \Big|\log|\mu_0|\log|\rho_1| - \log|\rho_0|\log|\mu_1|\Big|.$$

For $n \geq 7$, $-1-3/n < \rho_1 < -1-1/n$ (Proposition 4.4 and Remark 4.6). Hence $1+1/n < |\rho_1| < 1+3/n$ and $1/n < |\rho_1+1| < 3/n$. Using the relation $\mu = (\rho+1)^3/(2\rho)$ (Equation (4.1)), we conclude that

$$1 > \frac{27}{2n^2(n+1)} = (3/n)^3/(2(1+1/n)) > |\mu_1| = |\rho_1+1|^3/(2|\rho_1|) > \frac{1}{2n^2(n+3)}.$$

Since $1-n < \rho_0 < 2-n$ (Proposition 4.4 and Remark 4.6), $n-2 < |\rho_0| < n-1$ and $n-3 < |\rho_0+1| < n-2$. Using the relation $\mu = (\rho+1)^3/(2\rho)$ again, we conclude that

$$(n-2)^2/2 = (n-2)^3/(2(n-2)) > |\mu_0| = |\rho_0+1|^3/(2|\rho_0|) > (n-3)^3/(2(n-1)) > 1.$$

Hence

$$\begin{aligned} R' &= \log|\mu_0|\log|\rho_1| - \log|\rho_0|\log|\mu_1| \\ &\geq \log\left(\frac{(n-3)^3}{2(n-1)}\right)\log(1+1/n) - \log(n-2)\log\left(\frac{27}{2n^2(n+1)}\right) \\ &\geq \log(n-2)\log\left(\frac{2n^2(n+1)}{27}\right) \\ &> 0, \end{aligned}$$

and we conclude that $\{\rho, \mu\}$ is a multiplicatively independent subset of k_3 for $n \geq 7$. It may be verified by hand that $R' \neq 0$ when $n = 5$, so that $\{\rho, \mu\}$ is a multiplicatively independent subset of k_3 for all n under consideration.

Finally, for an upper bound we find that,

$$\begin{aligned}
R' &= \log|\mu_0|\log|\rho_1| - \log|\rho_0|\log|\mu_1| \\
&\leq \log\left(\frac{(n-2)^2}{2}\right)\log(1+3/n) - \log(n-1)\log\left(\frac{1}{2n^2(n+3)}\right) \\
&= \log\left(\frac{(n-2)^2}{2}\right)\log(1+3/n) + \log(n-1)\left(\log 2 + 2\log n + \log(n+3)\right) \\
&\leq \log\left(\frac{(n-2)^2}{2}\right)\log(1+3/n) + \frac{10}{3}\log(n-1)\log(n+3) \\
&\leq \frac{1}{6}\log\left(\frac{(n-2)^2}{2}\right) + \frac{10}{3}\log(n-1)\log(n+3) \qquad (n \geq 17) \\
&= \frac{1}{3}\log\left(\frac{n-2}{\sqrt{2}}\right) + \frac{10}{3}\log(n-1)\log(n+3) \\
&\leq \left(\frac{11}{3}\right)\log(n-1)\log(n+3).
\end{aligned}$$

□

Remark 4.20. *The upper bound for R' may be improved (at the expense of a greater value of n for which the bound is valid), since asymptotically $\log(n-1)\log(2n^3+6n^2)$ behaves like $3\log^2 n$ as $n \to \infty$.*

4.5.3 Congruences and divisibility of the index $[\mathcal{O}_{k_3}^\times : \langle -1, \rho, \mu\rangle]$

Proposition 4.21. *If $n \geq 5$ and $n \equiv 3$ mod 4, then $[\mathcal{O}_{k_3}^\times : \langle -1, \rho, \mu\rangle]$ is not divisible by 2.*

Proof. By way of contradiction, let $u \in \mathcal{O}^\times_{\mathbb{Q}(\rho_0)} \smallsetminus \langle -1, \rho_0, \mu_0\rangle$, such that $u^2 \in \langle -1, \rho_0, \mu_0\rangle$. Write

$$u^2 = \pm\rho_0^a \mu_0^b.$$

By modifying u, assume $a, b \in \{0, 1\}$. We cannot have $a = b = 0$, since this would imply that either $u^2 = -1$, which has no real solutions, or $u^2 = 1$, which has solutions $u = \pm 1 \in \langle -1, \rho_0, \mu_0 \rangle$. Since ρ_0 is not totally positive, it is impossible for $a = 1$ and $b = 0$, since then the left hand side is totally positive while the right hand side is not. Since, for $n \geq 5$, μ_0 is totally positive, while ρ_0 is not, we see that neither of the units $\pm\rho_0\mu_0$ is totally positive and hence neither is a square in k_3. So, we conclude that $u^2 = \pm\mu_0$. Since u^2 and μ_0 are (totally) positive, it is clear that we must choose the plus sign. The minimal polynomial of μ_0 over $\mathbb{Q}$ is

$$X^3 - \frac{1}{2}(n^2 - 4n + 9)X^2 + \frac{1}{4}(n^3 - n^2 - 13n + 9)X - 1.$$

Hence $\pm\sqrt{\mu_0}$ are zeros of the polynomial

$$\mathcal{P}_n(X) := X^6 - \frac{1}{2}(n^2 - 4n + 9)X^4 + \frac{1}{4}(n^3 - n^2 - 13n + 9)X^2 - 1.$$

We claim that $n \equiv 3 \bmod 4$ implies that $\mathcal{P}_n(X)$ is irreducible over $\mathbb{Q}$. To see this, let $n = 3 + 4t$ for some integer t, so that

$$\mathcal{P}_{n(t)}(X) = X^6 - (8t^2 + 4t + 3)X^4 + (16t^3 + 32t^2 + 8t - 3)X^2 - 1$$

Now define

$$\begin{aligned}\mathcal{Q}_{n(t)}(X) &:= \mathcal{P}_{n(t)}(X+1) \\ &= X^6 + 6X^5 - (8t^2+4t-12)X^4 - (32t^2+16t-8)X^3 \\ &\quad + (16t^3 - 16t^2 - 16t - 6)X^2 + (32t^3 + 32t^2 - 12)X \\ &\quad + (16t^3 + 24t^2 + 4t - 6).\end{aligned}$$

$\mathcal{Q}_{n(t)}(X)$ is Eisenstein at 2; every coefficient except the leading is divisible by 2, and the constant term is not divisible by 4. Since any nontrivial factorization of $\mathcal{P}_{n(t)}(X)$ would imply the existence of a nontrivial factorization of $\mathcal{Q}_{n(t)}(X)$, we conclude that $\mathcal{P}_{n(t)}(X)$ is irreducible over $\mathbb{Q}$, and hence that $\mathcal{P}_n(X)$ is irreducible over $\mathbb{Q}$ when $n \equiv 3 \bmod 4$.

Irreducibility of $\mathcal{P}_n(X)$ implies that a square root of μ_0 generates a degree 6 extension over $\mathbb{Q}$. In particular, we conclude that neither square root may lie in $\mathcal{O}_{k_3} \subset k_3$, and so we have reached a contradiction. □

Proposition 4.22. *If $n \geq 5$ and $n \equiv 2$ or 5 mod 9, then $[\mathcal{O}_{k_3}^\times : \langle -1, \rho, \mu \rangle]$ is not divisible by 3.*

Proof. Assume the contrary and let $u \in \mathcal{O}_{k_3}^\times \smallsetminus \langle -1, \rho_0, \mu_0 \rangle$ such that $u^3 \in \langle -1, \rho_0, \mu_0 \rangle$. Then

$$u^3 = \pm \rho_0^a \mu_0^b,$$

with $a, b \in \{0, 1, 2\}$. Since $\rho_0^a \mu_0^b$ is a cube if and only if $-\rho_0^a \mu_0^b$ is a cube, it is clear that we can ignore the minus sign. It is also clear that we cannot have $a = b = 0$, since this would

imply that $u^3 = 1$ and hence that $u = 1 \in \langle -1, \rho_0, \mu_0 \rangle$ and so contradict our hypothesis that $u \notin \langle -1, \rho_0, \mu_0 \rangle$. We now handle the remaining 8 possibilities by reducing to 4 cases:

Case 1: $u^3 = \rho_0^2 \mu_0^2$

This is equivalent to $\rho_0^1 \mu_0^1$ having a cube root in k_3 and implies that μ_0/ρ_0^2 has a cube root in k_3. The minimal polynomial of μ_0/ρ_0^2 over $\mathbb{Q}$ is

$$X^3 + \frac{1}{2}(n^3 - 6n^2 + 9n - 6)X^2 - \frac{1}{4}(n^3 - 3n^2 - 9n + 15)X - 1,$$

and so any cube root is a zero of the polynomial

$$p_1(X) := X^9 + \frac{1}{2}(n^3 - 6n^2 + 9n - 6)X^6 - \frac{1}{4}(n^3 - 3n^2 - 9n + 15)X^3 - 1.$$

If μ_0/ρ_0^2 has a cube root $\gamma_1 \in k_3$, then γ_1's minimal polynomial over $\mathbb{Q}$ is of degree 3 and divides $p_1(X)$. (It is of degree one or three, but can't be of degree one, because then $\gamma_1 \in \mathbb{Z}$.) So, suppose that

$$p_1(X) = (X^3 + a_2X^2 + a_1X + a_0)(X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0),$$

with $a_i, b_i \in \mathbb{Z}$. Since $(N_{k_3|\mathbb{Q}}(\gamma_1))^3 = N_{k_3|\mathbb{Q}}(\mu_0/\rho_0^2) = 1$, we conclude that $N_{k_3|\mathbb{Q}}(\gamma_1) = 1$

and hence that $a_0 = -1$ and $b_0 = 1$. We claim that the polynomial

$$g_1(X) := X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + 1 \in \mathbb{Z}[X],$$

cannot evenly divide $p_1(X)$. Indeed, we write

$$p_1(X) = g_1(X)q_1(X) + r_1(X),$$

where the quotient

$$q_1(X) = X^3 - b_5X^2 + (b_5^2 - b_4)X + ((n^3 - 6n^2 + 9n - 6)/2 - b_3 + 2b_4b_5 - b_5^3),$$

and the remainder

$$r_1(X) = \sum_{i=0}^{5} c_iX^i,$$

with

$$
\begin{aligned}
c_5 &= 2b_3b_5 + b_5^4 - 3b_4b_5^2 - \frac{1}{2}(n^3 - 6n^2 + 9n - 6)b_5 - b_2 + b_4^2 \\
c_4 &= -b_3b_5^2 + 2b_3b_4 + b_4b_5^3 + b_2b_5 - 2b_4^2b_5 - \frac{1}{2}(n^3 - 6n^2 + 9n - 6)b_4 - b_1 \\
c_3 &= b_3^2 + b_3b_5^3 - 2b_3b_4b_5 - \frac{1}{2}(n^3 - 6n^2 + 9n - 6)b_3 + -b_2b_5^2 + b_1b_5 + b_4b_2 \\
&\quad - \frac{1}{4}(n^3 - 3n^2 - 9n + 15) - 1 \\
c_2 &= b_2b_3 + b_2b_5^3 - b_1b_5^2 - 2b_5b_4b_2 + b_5 - \frac{1}{2}(n^3 - 6n^2 + 9n - 6)b_2 + b_1b_4 \\
c_1 &= b_1b_3 + b_1b_5^3 - b_5^2 - 2b_1b_4b_5 + b_4 - \frac{1}{2}(n^3 - 6n^2 + 9n - 6)b_1 \\
c_0 &= -1 - \frac{1}{2}(n^3 - 6n^2 + 9n - 6) + b_3 - 2b_4b_5 + b_5
\end{aligned}
$$

Noting that $n \equiv 2$ or $5 \bmod 9$ and using PARI to run through a complete system of residues of $\mathbb{Z}/9\mathbb{Z}$ for each of the b_i, we find that $\bar{r}_1(X) \in \mathbb{Z}/9\mathbb{Z}[X]$ is always nonzero. Hence so too is $r_1(X)$. We conclude that $p_1(X)$ does not have a cubic factor. Hence μ_0/ρ_0^2 does not have a cube root in k_3 and so neither do $\rho_0^2\mu_0^2$ and $\rho_0\mu_0$.

Case 2: $u^3 = \rho_0^2\mu_0$

This is equivalent to $\rho_0\mu_0^2$ having a cube roots in k_3 and implies that μ_0/ρ_0 has a cube root in k_3. The minimal polynomial over $\mathbb{Q}$ of μ_0/ρ_0 is

$$
X^3 - \frac{1}{2}(n^2 - 4n + 9)X^2 + \frac{1}{4}(n^3 - n^2 - 13n + 9)X - 1,
$$

and so any cube root is a zero of the polynomial

$$p(X) := X^9 - \frac{1}{2}(n^2 - 4n + 9)X^6 + \frac{1}{4}(n^3 - n^2 - 13n + 9)X^3 - 1.$$

If μ_0/ρ_0 has a cube root $\gamma_2 \in k_3$, then γ_2's minimal polynomial over $\mathbb{Q}$ is of degree 3 and divides $p(X)$. Suppose that

$$p_2(X) = (X^3 + a_2X^2 + a_1X + a_0)(X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0),$$

with $a_i, b_i \in \mathbb{Z}$. Since $(N_{k_3|\mathbb{Q}}(\gamma_2))^3 = N_{k_3|\mathbb{Q}}(\mu_0/\rho_0) = 1$, we conclude that $N_{k_3|\mathbb{Q}}(\gamma_2) = 1$ and hence that $a_0 = -1$ and $b_0 = 1$. We claim that the polynomial

$$g_2(X) := X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + 1 \in \mathbb{Z}[X],$$

cannot evenly divide $p_2(X)$. Indeed, we write

$$p_2(X) = g_2(X)q_2(X) + r_2(X),$$

where the quotient

$$q_2(X) = X^3 - b_5X^2 + (b_5^2 - b_4)X + (-(n^2 - 4n + 9)/2 - b_3 + 2b_4b_5 - b_5^3),$$

and the remainder

$$r_2(X) = \sum_{i=0}^{5} c_i X^i,$$

with

$$\begin{aligned}
c_5 &= 2b_3b_5 + b_5^4 - 3b_4b_5^2 + \frac{1}{2}(n^2 - 4n + 9)b_5 - b_2 + b_4^2 \\
c_4 &= -b_3b_5^2 + 2b_3b_4 + b_4b_5^3 + b_2b_5 - 2b_4^2b_5 + \frac{1}{2}(n^2 - 4n + 9)b_4 - b_1 \\
c_3 &= b_3^2 + b_3b_5^3 - 2b_3b_4b_5 + \frac{1}{2}(n^2 - 4n + 9)b_3 + -b_2b_5^2 + b_1b_5 + b_4b_2 \\
&\quad + \frac{1}{4}(n^3 - n^2 - 13n + 9) - 1 \\
c_2 &= b_2b_3 + b_2b_5^3 - b_1b_5^2 - 2b_5b_4b_2 + b_5 + \frac{1}{2}(n^2 - 4n + 9)b_2 + b_1b_4 \\
c_1 &= b_1b_3 + b_1b_5^3 - b_5^2 - 2b_1b_4b_5 + b_4 + \frac{1}{2}(n^2 - 4n + 9)b_1 \\
c_0 &= -1 + \frac{1}{2}(n^2 - 4n + 9) + b_3 - 2b_4b_5 + b_5
\end{aligned}$$

As in case 1, we note that $n \equiv 2$ or $5 \bmod 9$ and use PARI to run through a complete system of residues of $\mathbb{Z}/9\mathbb{Z}$ for each of the b_i. Again we find that $\bar{r}_2(X) \in \mathbb{Z}/9\mathbb{Z}[X]$ is always nonzero. Hence so too is $r_2(X)$. We conclude that $p_2(X)$ does not have a cubic factor and that μ_0/ρ_0, along with $\rho_0^2\mu_0$ and $\rho_0\mu_0^2$, do not have cube roots in k_3.

Case 3: $u^3 = \rho_0$

This is equivalent to ρ_0^2 having a cube root in k_3. The minimal polynomial of ρ_0 over $\mathbb{Q}$ is

$$f_n(X) = X^3 - nX^2 - nX - 1,$$

and so any cube root is a zero of the polynomial

$$p_3(X) := X^9 - nX^6 - nX^3 - 1.$$

If ρ_0 has a cube root $\gamma_3 \in k_3$, then γ_3's minimal polynomial over $\mathbb{Q}$ is of degree 3 and divides $p_3(X)$. Suppose that

$$p_3(X) = (X^3 + a_2X^2 + a_1X + a_0)(X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0),$$

with $a_i, b_i \in \mathbb{Z}$. Using the same argument made in the first two cases, we may conclude that $a_0 = -1$ and $b_0 = 1$. We claim that the polynomial

$$g_3(X) := X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + 1 \in \mathbb{Z}[X],$$

cannot evenly divide $p_3(X)$. We again write

$$p_3(X) = g_3(X)q_3(X) + r_3(X),$$

where the quotient

$$q_3(X) = X^3 - b_5X^2 + (b_5^2 - b_4)X + (-n - b_3 + 2b_4b_5 - b_5^3),$$

and the remainder

$$r_3(X) = \sum_{i=0}^{5} c_i X^i,$$

with

$$\begin{aligned}
c_5 &= 2b_3b_5 + b_5^4 - 3b_4b_5^2 + nb_5 - b_2 + b_4^2 \\
c_4 &= -b_3b_5^2 + 2b_3b_4 + b_4b_5^3 + b_2b_5 - 2b_4^2b_5 + nb_4 - b_1 \\
c_3 &= b_3^2 + b_3b_5^3 - 2b_3b_4b_5 + nb_3 + -b_2b_5^2 + b_1b_5 + b_4b_2 - n - 1 \\
c_2 &= b_2b_3 + b_2b_5^3 - b_1b_5^2 - 2b_5b_4b_2 + b_5 + nb_2 + b_1b_4 \\
c_1 &= b_1b_3 + b_1b_5^3 - b_5^2 - 2b_1b_4b_5 + b_4 + nb_1 \\
c_0 &= -1 + n + b_3 - 2b_4b_5 + b_5
\end{aligned}$$

Using PARI to run through a complete system of residues of $\mathbb{Z}/9\mathbb{Z}$ for each of the b_i along with the fact that $n \equiv 2$ or $5 \bmod 9$, we find that $\bar{r}_3(X) \in \mathbb{Z}/9\mathbb{Z}[X]$ is always nonzero. Hence so too is $r_3(X)$. We conclude that $p_3(X)$ does not have a cubic factor and that ρ_0 and ρ_0^2 do not have cube roots in k_3.

Case 4: $u^3 = \mu_0$

This is equivalent to μ_0^2 having a cube root in k_3. The minimal polynomial of μ_0 over $\mathbb{Q}$ is

$$X^3 - \frac{1}{2}(n^2 + 4n + 9)X^2 - \frac{1}{4}(n^3 + n^2 - 13n - 9)X - 1,$$

and so any cube root is a zero of the polynomial

$$p_4(X) := X^9 - \frac{1}{2}(n^2 + 4n + 9)X^6 - \frac{1}{4}(n^3 + n^2 - 13n - 9)X^3 - 1,$$

If μ_0 has a cube root $\gamma_4 \in k_3$, then γ_4's minimal polynomial over $\mathbb{Q}$ is of degree 3 and divides $p_4(X)$. Suppose that

$$p_4(X) = (X^3 + a_2X^2 + a_1X + a_0)(X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0),$$

with $a_i, b_i \in \mathbb{Z}$. Using arguments made above, we may conclude that $a_0 = -1$ and $b_0 = 1$. We claim that the polynomial

$$g_4(X) := X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + 1 \in \mathbb{Z}[X],$$

cannot evenly divide $p_4(X)$. One last time we write

$$p_4(X) = g_4(X)q_4(X) + r_4(X),$$

where the quotient

$$q_4(X) = X^3 - b_5X^2 + (b_5^2 - b_4)X + (-(n^2 + 4n + 9)/2 - b_3 + 2b_4b_5 - b_5^3),$$

and the remainder

$$r_4(X) = \sum_{i=0}^{5} c_i X^i,$$

with

$$\begin{aligned}
c_5 &= 2b_3b_5 + b_5^4 - 3b_4b_5^2 + \frac{1}{2}(n^2+4n+9)b_5 - b_2 + b_4^2 \\
c_4 &= -b_3b_5^2 + 2b_3b_4 + b_4b_5^3 + b_2b_5 - 2b_4^2b_5 + \frac{1}{2}(n^2+4n+9)b_4 - b_1 \\
c_3 &= b_3^2 + b_3b_5^3 - 2b_3b_4b_5 + \frac{1}{2}(n^2+4n+9)b_3 + -b_2b_5^2 + b_1b_5 + b_4b_2 \\
&\quad - \frac{1}{4}(n^3+n^2-13n-9) - 1 \\
c_2 &= b_2b_3 + b_2b_5^3 - b_1b_5^2 - 2b_5b_4b_2 + b_5 + \frac{1}{2}(n^2+4n+9)b_2 + b_1b_4 \\
c_1 &= b_1b_3 + b_1b_5^3 - b_5^2 - 2b_1b_4b_5 + b_4 + \frac{1}{2}(n^2+4n+9)b_1 \\
c_0 &= -1 + \frac{1}{2}(n^2+4n+9) + b_3 - 2b_4b_5 + b_5
\end{aligned}$$

Using PARI to run through a complete system of residues of $\mathbb{Z}/9\mathbb{Z}$ for each of the b_i along with the fact that $n \equiv 2$ or $4 \bmod 9$, we find that $\bar{r}_4(X) \in \mathbb{Z}/9\mathbb{Z}[X]$ is always nonzero. Hence so too is $r_4(X)$. We conclude that $p_4(X)$ does not have a cubic factor and that μ_0 and μ_0^2 do not have cube roots in k_3.

The proof is now complete. □

4.5.4 Conditions sufficient to conclude that $\{\rho_0, \mu_0\}$ is a set of fundamental units for k_3

Proposition 4.23. *If $n \geq 5$, $n \equiv 3$ mod 4, and $n^4 - 18n^2 - 27$ is odd square-free, then $[\mathcal{O}_{k_3}^{\times} : \langle -1, \rho_0, \mu_0 \rangle] = 1$ or 3.*

Proof. Cusick's result [3] tells us that the regulator R of a totally real cubic field satisfies the inequality

$$R \geq \frac{1}{16} \log^2(D/4),$$

where D is the discriminant of the number field. Hence, when $n \geq 19$, we find that

$$\begin{aligned}
[\mathcal{O}_{k_3}^{\times} : \langle -1, \rho_0, \mu_0 \rangle] &= R'/R \\
&\leq 16R' / \log^2(D/4) \\
&= 16R' / \log^2(\mathrm{disc}(f)/4) \qquad \text{(Lemma 4.13)} \\
&= 16R' / \log^2((n^4 - 18n^2 - 27)/4) \\
&\leq 16 \left(\frac{11}{3}\right) \frac{\log(n-1)\log(n+3)}{\log^2((n^4 - 18n^2 - 27)/4)} \qquad \text{(Proposition 4.19)} \\
&\leq 16 \left(\frac{11}{3}\right) \frac{\log(n-1)\log(n+3)}{\log^2(\frac{n^2-10}{2})^2} \\
&= \left(\frac{44}{3}\right) \frac{\log(n-1)}{\log(\frac{n^2-10}{2})} \frac{\log(n+3)}{\log(\frac{n^2-10}{2})} \\
&\leq \left(\frac{11}{3}\right) \frac{\log(n-1)}{\log(\frac{n-\sqrt{10}}{\sqrt{2}})} \frac{\log(n+3)}{\log(\frac{n-\sqrt{10}}{\sqrt{2}})}
\end{aligned}$$

Both of the sequences $n \mapsto \log(n-1)/\log((n-\sqrt{10})/\sqrt{2})$ and $n \mapsto \log(n+3)/\log((n-$

$\sqrt{10})/\sqrt{2})$ are monotone decreasing for $n \geq 19$, and hence so too is the sequence

$$\left\{ \left(\frac{11}{3}\right) \frac{\log(n-1)}{\log(\frac{n-\sqrt{10}}{\sqrt{2}})} \frac{\log(n+3)}{\log(\frac{n-\sqrt{10}}{\sqrt{2}})} \right\}_{n \geq 19},$$

with limit $11/3$ as $n \to \infty$. When $n = 31$, $\left(\frac{11}{3}\right) \frac{\log(n-1)}{\log(\frac{n-\sqrt{10}}{\sqrt{2}})} \frac{\log(n+3)}{\log(\frac{n-\sqrt{10}}{\sqrt{2}})}, \approx 4.952795 < 5$. Hence $[\mathcal{O}_{k_3}^{\times} : \langle -1, \rho_0, \mu_0 \rangle] \leq 4$ for $n \geq 31$. For each of the remaining values of n which satisfy all of the hypotheses, i.e., $n \in \{7, 11, 19, 23\}$, it is readily found that the quantity $16R'/\log^2(D/4) < 4$. Hence

$$[\mathcal{O}_{k_3}^{\times} : \langle -1, \rho_0, \mu_0 \rangle] \leq 4$$

for each n satisfying our hypotheses.

Since the index is no greater than 4 and since we know that the index is not divisible by 2 (Proposition 4.21), we conclude that it is either 1 or 3. □

Corollary 4.24. *If $n \geq 5$, $n \equiv 3$ mod 4, $n \equiv 2$ or 5 mod 9, and $n^4 - 18n^2 - 27$ is odd square-free, then $\{\rho_0, \mu_0\}$ is a set of fundamental units for k_3.*

Proof. From Proposition 4.23, $[\mathcal{O}_{k_3}^{\times} : \langle -1, \rho_0, \mu_0 \rangle] = 1$ or 3. From Proposition 4.22, $[\mathcal{O}_{k_3}^{\times} : \langle -1, \rho_0, \mu_0 \rangle]$ is not divisible by 3. □

4.6 Conditions sufficient to conclude that $r \mid h_{k_3}$ for a given $r > 1$.

Let $r \geq 1$ be an integer. We show that r divides the class number of K by proving that the class group contains an element of order r. We accomplish this task as we have before: begin with a principal ideal of K, show that it factors as an rth power of an ideal $\mathfrak{a}$, and finally show that no lesser power of $\mathfrak{a}$ is principal.

4.6.1 Candidate for a representative of a class of order r

Lemma 4.25. *Let $(2, y)$ be a solution in integers to $Y^r = (X - \rho_0)(X - \rho_1)(X - \rho_2)$. If 37 does not divide y, then $(2 - \rho_0)$ is the r-th power of an ideal of $\mathbb{Q}(\rho_0)$.*

Proof. Let $\rho = \rho_0$. Since $(2, y)$ is a solution,

$$y^r = (2 - \rho)(2 - \rho_1)(2 - \rho_2) = 2^3 + 2^2 n + 2n - 1 = 6n + 7.$$

Let

$$(2 - \rho) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

be the unique decomposition of $(2 - \rho)$ into positive integer powers of distinct prime ideals of $\mathbb{Q}(\rho)$, and let p denote the rational prime below $\mathfrak{p}$. Note that $(2 - \rho_1)(2 - \rho_2) = \rho^2 + (2 + n)\rho + (4 + 3n)$. We claim that no prime divisor of $(2 - \rho)$ also divides the ideal $(2 - \rho_1)(2 - \rho_2) = (\rho^2 + (2 + n)\rho + (4 + 3n))$. To the contrary, suppose that $\mathfrak{p} \supseteq (2 - \rho)$

and $\mathfrak{p} \supseteq (\rho^2 + (2+n)\rho + (4+3n))$. Then

$$12 + 5n = (\rho^2 + (2+n)\rho + 4 + 3n) + (2-\rho)(\rho + 4 + n) \in \mathfrak{p},$$

and hence

$$5n \equiv -12 \mod p.$$

Since $p \mid y$, the first equation of this proof yields that $n \equiv -7/6 \mod p$. Hence $37 \equiv 0 \mod p$ and we arrive at the contradiction that $p = 37$ is a prime factor of y.

Thus if $\mathfrak{p}^{\nu_\mathfrak{p}}$ is the exact power of $\mathfrak{p}$ dividing $(2-\rho)$, then it is also the exact power of $\mathfrak{p}$ dividing y^r. Hence $r \mid \nu_\mathfrak{p}$, and we conclude that

$$(2-\rho) = \mathfrak{a}^r,$$

where

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}/r}.$$

□

4.6.2 Ramification revisited

Lemma 4.26. *Let* $(2, y)$ *be a solution in integers to* $Y^r = f_n(X)$. *Then* $\gcd(6, y) = 1$ *and the only prime divisors of* y *that divide* $\mathrm{disc}(f_n(X))$ *are* 37 *and* 47.

Proof. Any prime divisor of y also divides $y^r = f_n(2) = 6n + 7$. Since $\mathrm{disc}(f_n(X)) =$

$n^4 - 18n^2 - 27$, any prime common divisor q of y and $\mathrm{disc}(f_n(X))$ satisfies:

$$n^4 - 18n^2 - 27 \equiv 0 \mod q$$

$$6n + 7 \equiv 0 \mod q.$$

The linear congruence has no solution if $q = 2$ or 3. Hence, $\gcd(6, y) = 1$ and the linear congruence has a unique solution; namely $n \equiv -7/6 \mod q$. Substituting into the first congruence reveals that $q = 37$ or 47. In other words, if q is a prime divisor of $y^r = 6n+7$ and divides $\mathrm{disc}(f_n(X))$, then $q \in \{37, 47\}$. □

4.6.3 Divisibility of the index $[\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle]$ redux.

Remark 4.27. *Let m be an integer and $\mathfrak{p} \subset \mathcal{O}_{k_3}$ a prime ideal lying over the rational prime p for which $\rho \equiv m$ mod $\mathfrak{p}$. From Dirichlet's Factorization Theorem we know that if $p \nmid \mathrm{disc}(f_n(X))$, then the degree of the residue field over its prime subfield $[\mathcal{O}_{k_3}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = 1$.*

Lemma 4.28. *Let $(2, y)$ be a solution to $Y^r = (2-\rho_0)(2-\rho_1)(2-\rho_2) = 6n+7$. Let $\ell \neq 3$ be a prime dividing r and let p and q be primes dividing y not equal to 37 or 47. Assume that 3 is an ℓth power nonresidue mod p and mod q. Assume that 2 is an ℓth power residue mod p and an ℓth power nonresidue mod q. Then ℓ does not divide $[\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle]$.*

Proof. Let $\mathfrak{p}$ (resp. $\mathfrak{q}$) be prime ideals of k_3 over p (resp. q) containing $2 - \rho_0$. We note

that this implies that

$$\rho_0 \equiv 2 \mod \mathfrak{p}, \mathfrak{q}, \tag{4.2}$$

and that

$$\begin{aligned} \mu_0 &= \left(\frac{n+3}{2}\right)(1+\rho_0) + \rho_0^2 \\ &\equiv \left(\frac{-7/6+3}{2}\right)(1+2) + 2^2 \mod \mathfrak{p}, \mathfrak{q} \\ &= 27/4 \mod \mathfrak{p}, \mathfrak{q} \end{aligned} \tag{4.3}$$

Suppose that ℓ is a prime common divisor of r and $[\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle]$. From Lemma 4.26, we know that the only possible prime common divisors of y and $\mathrm{disc}(f_n)$ are 37 and 47. Hence from Remark 4.27 we conclude that $[\mathcal{O}_{k_3}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = [\mathcal{O}_{k_3}/\mathfrak{q} : \mathbb{Z}/q\mathbb{Z}] = 1$. Also, since $\ell \mid [\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle]$, there is a unit $u \in \mathcal{O}_{k_3}^\times \smallsetminus \langle -1, \rho_0, \mu_0 \rangle$ such that

$$u^\ell = \pm \rho_0^a \mu_0^b,$$

with a, b non-negative rational integers strictly less than ℓ.

Case 1: $\ell \neq 2$.

Since ℓ is odd, we may ignore the negative sign and conclude that

$$u^\ell \equiv 2^{a-2b} 3^{3b} \mod \mathfrak{p}, \mathfrak{q}.$$

Since $[\mathcal{O}_{k_3}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = 1$, we conclude that $2^{a-2b}3^{3b}$ is an ℓth power residue modulo the rational primes p, q. Since 2 is an ℓth power residue mod p and 3 is an ℓth power nonresidue mod p, we conclude that $3b \equiv 0 \bmod \ell$, and hence that $b \equiv 0 \bmod \ell$. Since $0 \leq b < \ell$, we conclude that $b = 0$ and

$$u^\ell \equiv 2^a \mod \mathfrak{q}.$$

Since 2 is an ℓth power nonresidue mod $\mathfrak{q}$, we conclude that $a \equiv 0 \mod \ell$. Using the fact that $0 \leq a < \ell$, we find that $a = 0$. Hence $u^\ell = 1$, $u = 1 \in \langle -1, \rho_0, \mu_0 \rangle$, and we've reached a contradiction.

Case 2: $\ell = 2$.

In this case we may proceed as in the proof of Proposition 4.21 to conclude that the only possibility is that

$$u^2 = \mu_0.$$

But then $u^2 \equiv 27/4 \mod \mathfrak{p}$, or, upon rearrangement,

$$(2u/3)^2 \equiv 3 \mod \mathfrak{p},$$

and we conclude that 3 is a quadratic residue mod $\mathfrak{p}$. Since $[\mathcal{O}_{k_3}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = 1$, we are forced to conclude that 3 is a quadratic residue mod p; a conclusion that contradicts one of our assumptions. □

We have the following to handle the case in which r is divisible by 3.

Lemma 4.29. *Let* $(2, y)$ *be a solution in integers to* $Y^r = f_n(2)$, *with* $r \equiv 0 \mod 27$. *Let* $p \equiv 1 \mod 9$ *and* q *be primes dividing* y *with* p, q *not equal to* 37 *or* 47. *Assume that* 3 *is a cubic nonresidue mod* p *and mod* q. *Assume that* 2 *is a* 9*th power residue mod* p *and a cubic nonresidue mod* q. *Then* 27 *does not divide* $[\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle]$.

Proof. Let $\mathfrak{p}$ (resp. $\mathfrak{q}$) be prime ideals of k_3 over p (resp. q) containing $2 - \rho_0$. As in Equations (4.2) and (4.3),

$$\rho_0 \equiv 2 \mod \mathfrak{p}, \mathfrak{q},$$

$$\mu_0 \equiv 27/4 \mod \mathfrak{p}, \mathfrak{q}.$$

If 27 divides $[\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle]$, then $\mathcal{O}_{k_3}^\times / \langle -1, \rho_0, \mu_0 \rangle$ contains a subgroup of order 27. This subgroup can be generated by two elements and so isn't isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Hence this subgroup contains a cyclic subgroup of order 9 and so there is a unit $u \in \mathcal{O}_{k_3}^\times$ such that $u^9 = \pm \rho_0^a \mu_0^b$, with $a, b \in \mathbb{Z}$ and such that $u^i \notin \langle -1, \rho_0, \mu_0 \rangle$ for $0 < i < 9$. We may ignore the negative sign and conclude that there is a unit $u \in \mathcal{O}_{k_3}^\times$ such that

$$u^9 = \rho_0^a \mu_0^b,$$

with $a, b \in \mathbb{Z}$ and such that $u^i \notin \langle -1, \rho_0, \mu_0 \rangle$ for $0 < i < 9$. We now show that this is a contradiction by showing that $u^9 \in \langle -1, \rho_0, \mu_0 \rangle$ implies that $u^3 \in \langle -1, \rho_0, \mu_0 \rangle$.

Applying our congruences we conclude that

$$u^9 \equiv 2^{a-2b}3^{3b} \mod \mathfrak{p}, \mathfrak{q}.$$

Since $[\mathcal{O}_{k_3}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] = [\mathcal{O}_{k_3}/\mathfrak{q} : \mathbb{Z}/q\mathbb{Z}] = 1$ (Lemmas 4.26 and Remark 4.27), we may conclude that $2^{a-2b}3^{3b}$ is a 9th power residue modulo the rational primes p, q. Since 2 is a 9th power residue mod p, we may conclude that there is an integer x such that $3^{3b} \equiv x^9$ mod p. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, we conclude that $b \equiv 0 \mod 3$. Furthermore, since $b \equiv 0$ mod 3, we conclude that $a \equiv 0$ mod 3. Since a and b are divisible by 3, we now conclude that $(u^3)^3 = u^9 = \rho_0^a \mu_0^b = (\rho_0^{a/3}\mu_0^{b/3})^3$. From the injectivity of $x \mapsto x^3$ in K, we conclude that

$$u^3 = \rho_0^{a/3}\mu_0^{b/3} \in \langle -1, \rho_0, \mu_0 \rangle,$$

and have reached a contradiction. □

4.6.4 A class of order r

Proposition 4.30. *Let $(2, y)$ be a solution to $Y^r = (2-\rho_0)(2-\rho_1)(2-\rho_2) = 6n+7$. Assume that for every prime divisor $\ell \neq 3$ of r there are prime divisors p, p_2, p_3 of y not equal to 37 or 47 that satisfy:*

1. *3 is an ℓth power nonresidue mod p, p_2*
2. *2 is an ℓth power residue mod p and an ℓth power nonresidue mod p_2*
3. *37 is an ℓth power residue mod p, p_2 and an ℓth power nonresidue mod p_3,*

then $(2-\rho_0) \neq (\beta)^\ell$ for any prime divisor $\ell \neq 3$ of r.

Proof. If $(2-\rho_0) = (\beta)^\ell$, then $2-\rho_0 = u\beta^\ell$, where u is a unit of k_3. By Lemma 4.28, $\gcd(\ell, [\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0\rangle]) = 1$. Hence there are integers s and t such that $u = (u^s)^{[\mathcal{O}_{k_3}^\times : \langle -1,\rho_0,\mu_0\rangle]}(u^t)^\ell$, and hence such that

$$2-\rho_0 = \pm\rho_0^b\mu_0^c\beta_1^\ell, \quad (*)$$

where $\beta_1 = \beta u^t$.

Let $\mathfrak{p}$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ denote primes of k_3 containing $2-\rho_0$ and lying over the rational primes p, p_2, p_3 of our hypotheses. As in Equations (4.2) and (4.3),

$$\rho_0 \equiv 2 \mod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$$

$$\mu_0 \equiv 27/4 \mod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3.$$

Applying σ and σ^2 to both sides of the equality $(*)$, we find that

$$2-\rho_1 = \pm\rho_1^a\mu_1^b(\beta_1^\sigma)^\ell$$

$$2-\rho_2 = \pm\rho_2^a\mu_2^b(\beta_1^{\sigma^2})^\ell,$$

and hence conclude that

$$\begin{aligned}(2-\rho_1)(2-\rho_2) &= (\rho_1\rho_2)^a(\mu_1\mu_2)^b(\beta_1^\sigma\beta_1^{\sigma^2})^\ell \\ &= \rho_0^{-a}\mu_0^{-b}(\beta_1^\sigma\beta_1^{\sigma^2})^\ell \\ &\equiv 2^{-a}(27/4)^{-b}(\beta_1^\sigma\beta_1^{\sigma^2})^\ell \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3 \\ &= 2^{2b-a}3^{-3b}(\beta_1^\sigma\beta_1^{\sigma^2})^\ell \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3\end{aligned}$$

On the other hand,

$$\begin{aligned}(2-\rho_1)(2-\rho_2) &= \rho^2+(2+n)\rho+(4+3n) \\ &\equiv 5n+12 \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3 \\ &= 5(-7/6)+12 \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3 \\ &= 37/6 \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3.\end{aligned}$$

Hence $37/6 \equiv 2^{2b-a}3^{-3b}(\beta_1^\sigma\beta_1^{\sigma^2})^\ell \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3$, or

$$37 \equiv 2^{2b-a+1}3^{-3b+1}(\beta_1^\sigma\beta_1^{\sigma^2})^\ell \mod \mathfrak{p},\mathfrak{p}_2,\mathfrak{p}_3.$$

Since the residual degrees of these primes are 1 (Lemmas 4.26 and Remark 4.27), we may conclude that

$$2^{a-2b-1}3^{3b-1}37$$

is an ℓth power residue modulo the rational primes p, p_2, and p_3. Using the fact that 2 and 37 are ℓth power residues modulo p while 3 is a nonresidue, we conclude that

$$3b - 1 \equiv 0 \mod \ell.$$

But then since 37 is an ℓth power residue mod p_2, while 2 is a nonresidue, we conclude that

$$a - 2b - 1 \equiv 0 \mod \ell.$$

This implies that 37 is an ℓth power residue mod p_3; contradiction. □

Proposition 4.31. *Let $(2, y)$ be a solution to $y^r = (2 - \rho_0)(2 - \rho_1)(2 - \rho_2) = 6n + 7$, with $r \equiv 0 \mod 27$. Assume that there are prime divisors p, p_2, p_3 of y each congruent to 1 mod 27, which satisfy:*

1. *3 is a cubic nonresidue mod p, p_2*
2. *2 is a $27th$ power residue mod p and a cubic nonresidue mod p_2*
3. *37 is a cubic residue mod p, p_2 and cubic nonresidue mod p_3,*

then $(2 - \rho_0)$ is not the cube of a principal ideal.

Proof. By way of contradiction, suppose that $(2 - \rho_0) = (\beta)^3$. Then $2 - \rho_0 = u\beta^3$, with $u \in \mathcal{O}_{k_3}^\times$. From Lemma 4.29 we conclude that $[\mathcal{O}_{k_3}^\times : \langle -1, \rho_0, \mu_0 \rangle] \not\equiv 0 \mod 27$. Therefore, $u^{9k} \in \langle -1, \rho_0, \mu_0 \rangle$ for some $k \not\equiv 0 \mod 3$. Taking $9k$th powers we find that

$$\begin{aligned}(2 - \rho_0)^{9k} &= u^{9k}\beta^{27k} \\ &= \pm\rho_0^a \mu_0^b \beta^{27k}.\end{aligned}$$

Let $\mathfrak{p}$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ denote primes of k_3 containing $2-\rho_0$ and lying over the rational primes p, p_2, p_3 of our hypotheses. Conjugating with σ and σ^2, multiplying the resulting equations, and applying the congruences $\rho_0 \equiv 2 \bmod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$, $\mu_0 \equiv 27/4 \bmod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$ yields:

$$\begin{aligned}(2-\rho_1)^{9k}(2-\rho_2)^{9k} &= (\rho_1\rho_2)^a(\mu_1\mu_2)^b(\beta^\sigma\beta^{\sigma^2})^{27} \\ &= \rho_0^{-a}\mu_0^{-b}(\beta^\sigma\beta^{\sigma^2})^{27k} \\ &\equiv 2^{-a}(27/4)^{-b}(\beta^\sigma\beta^{\sigma^2})^{27k} \mod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3\end{aligned}$$

Since $(2-\rho_1)(2-\rho_2) = \rho^2 + (2+n)\rho + (4+3n) \equiv 5n+12 \equiv 37/6 \bmod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$, we conclude that $(37/6)^{9k} \equiv 2^{-a}(27/4)^{-b}(\beta^\sigma\beta^{\sigma^2})^{27k} \mod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$, or that

$$37^{9k} \equiv 2^{-a+2b+9k}3^{-3b+9k}(\beta^\sigma\beta^{\sigma^2})^{27k} \mod \mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$$

Since $\mathfrak{p}, \mathfrak{p}_2, \mathfrak{p}_3$ each have residual degree one (Lemmas 4.26 and Remark 4.27), we see that $2^{a-2b-9k}3^{9k-3b}37^{9k}$ is a $27k$th power residue modulo the rational primes p, p_2, and p_3.

Since 37 is a cubic residue mod p and since 2 is a 27th power residue mod p, we conclude that there is an integer x such that $x^{27} \equiv 3^{-3b+9k} \mod p$. Hence $3k-b \equiv 0 \bmod 9$ and $-3b+9k \equiv 0 \bmod 27$.

Since $-3b+9k$ is a multiple of 27 and since 37 is a cubic residue mod p_2, we conclude that there is an integer y such that $2^{-a+2b+9k} \equiv y^{27} \mod p_2$. Hence $9k+2b-a = c \equiv 0 \bmod 27$.

Since $-3b + 9k$ and $-a + 2b + 9k$ are each multiples of 27, we conclude that there is a rational integer z such that $z^{27} \equiv 37^{9k} \mod p_3$. This contradicts the fact that 37 is a cubic nonresidue mod p_3, and so we conclude that $(2 - \rho_0)$ is not the cube of a principal ideal. □

Theorem 4.32. *Let $(2, y)$ be a solution in integers to $Y^r = (2 - \rho_0)(2 - \rho_1)(2 - \rho_2) = 6n + 7$. If the hypotheses of Propositions 4.30 and 4.31 are satisfied, then $(2 - \rho) = \mathfrak{a}^r$, where $\mathfrak{a}$ is a representative of a class of order r in the class group of k_3.*

Proof. According to Lemma 4.25, $(2 - \rho_0) = \mathfrak{a}^r$ for some ideal $\mathfrak{a}$ of k_3. To show that $\mathfrak{a}$ has order r upon passing to the class group, we must show that no smaller positive power of $\mathfrak{a}$ is principal. If this was not the case, and some smaller positive power of $\mathfrak{a}$ was principal, then we would conclude that $(2 - \rho_0)$ is the ℓth power of a principal ideal for some $\ell > 1$ dividing r. Since a power of a principal ideal is principal we may, without loss of generality, take ℓ to be prime. Since when the hypotheses of the previous two Propositions hold, $(2 - \rho_0)$ is not the ℓth power of principal ideal for any prime ℓ dividing r, the corollary is established. □

4.7 Existence of infinitely many fields of the family with $r \mid h_{k_3}$ for arbitrary integer $r > 1$.

Showing that for any positive integer r there exists a field K_n of our family with class number divisible by r is the essential step; once existence is established the existence of infinitely many distinct fields of our family with class number divisible by r

follows. Existence requires demonstrating that there are infinitely many primes satisfying the congruence conditions sufficient to guarantee the existence of a class of order r. This is accomplished with an appeal to Bauer's Theorem in the following Lemma.

Lemma 4.33. *There are infinitely many primes satisfying the power residue hypotheses of Proposition 4.30, and there are infinitely many primes satisfying the power residue hypotheses of Proposition 4.31.*

Proof. Let

$$L = \mathbb{Q}(\zeta_\ell, 2^{1/\ell}, 37^{1/\ell})$$

$$L' = \mathbb{Q}(\zeta_{2\ell}, 3^{1/\ell}),$$

where ζ_ℓ (resp. $\zeta_{2\ell}$) denotes a primitive ℓth (resp. 2ℓth) root of unity. A rational prime p splits completely in L if and only if $p \equiv 1 \mod \ell$ and 2 and 37 are ℓth power residues mod p. A rational prime q splits completely in L' if and only if $q \equiv 1 \mod 2\ell$ and 3 is an ℓth power residue mod q. Since $L' \not\subset L$, we may apply Bauer's Theorem [2] to conclude that there are infinitely many primes that split in L but not in L'. Hence there are infinitely many primes p for which 2 and 37 are ℓth power residues mod p but for which 3 is an ℓth power nonresidue mod p. A very similar argument may be used to show that there are infinitely many primes p_2 for which 37 is an ℓth power residue mod p_2 but for which 2 and 3 are ℓth power nonresidues mod p_2. Likewise we can show that there are infinitely many primes p_3 for which 37 is an ℓth power nonresidue mod p_3. To prove that there are

infinitely many primes satisfying the power residue hypotheses of Proposition 4.31, take

$$L = \mathbb{Q}(\zeta_{27}, 2^{1/27}, 37^{1/3})$$

$$L' = \mathbb{Q}(\zeta_{27}, 3^{1/3}),$$

where ζ_{27} denotes a primitive 27th root of unity. □

Theorem 4.34. *Let r be a positive integer > 1. The family of cubic fields $\{k_{3,n} \mid n \in \mathbb{Z},\ n$ odd, and $n \geq 5\}$, where $k_{3,n}$ is obtained from $\mathbb{Q}$ by adjoining a root of $f_n(X) = X^3 + nX^2 + nX - 1$, contains infinitely many members whose class group contains a cyclic subgroup of order r.*

Proof. We begin by showing the existence of such a member. If $r \equiv 0 \bmod 3$, then replace r with $3r$ or $9r$, as needed, to guarantee that $r \equiv 0 \bmod 27$. Choose a triple (p, p_2, p_3) of primes satisfying the power residue hypotheses of Proposition 4.30 for each prime $\ell \neq 3$ dividing r. Lemma 4.33 shows that there are infinitely many such primes satisfying these hypotheses; make sure not to choose $2, 3, 37$, or 47. If $r \equiv 0 \bmod 3$, then also choose a triple (p, p_2, p_3) of primes satisfying the power residue hypotheses of Proposition 4.31. Lemma 4.33 guarantees that there are infinitely many such primes satisfying these hypotheses; once again make sure not to choose $2, 3, 37$, or 47. Choose s such that

$$\left(s \prod_{\ell | r} p_\ell p_{2,\ell} p_{3,\ell} \right)^r \equiv 7 \mod 6.$$

Then $(2, s \prod_{\ell|r} p_\ell p_{2,\ell} p_{3,\ell})$ is a solution in integers to $Y^r = f_n(X)$ for some n. From Corollary 4.32 we now conclude that $r \mid h_n$. Thus for any positive $r > 1$ which is not

divisible by 3, there is an element $k_{3,n}$ of this family of cubics which has class number divisible by r.

This result implies the existence of infinitely many such fields. Indeed, let $k_{3,n}$ be a member of the family for which $r \mid h_n$. Let r^γ be the greatest power of r dividing h_n. From the previous paragraph we know that there is a family member $k_{3,n'}$ for which $r^{\gamma+1}$ divides $h_{n'}$. But $h_{n'} \neq h_n$ implies that $k_{3,n} \neq k_{3,n'}$. We conclude that given any finite number of cubic fields with class number divisible by r, we can find an additional one. Hence this family contains infinitely many members with class number divisible by r. $\square$

Bibliography

[1] S. Balady and L.C. Washington. A family of cyclic quartic fields with explicit fundamental units. *Acta Arith.*, 187:43–57, 2019.

[2] K. Conrad. History of class field theory. https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf, October 2021.

[3] T. W. Cusick. Lower bounds for regulators. *Lecture Notes in Math.*, 1068:63–73, 1983.

[4] V. Ennola, S. Mäki, and R. Turunen. On real cyclic sextic fields. *Math. Comp.*, 45(19):591–611, 1985.

[5] I. Gaál and L. Remete. Integral bases and monogenity of the simplest sextic fields. *preprint arXiv1809.10072v1*, 2018.

[6] M.-N. Gras. Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de $\mathbb{Q}$. *Publ. Math. Besançon*, pages 1–79, 1977/78.

[7] M.-N. Gras. Families d'unités dans les extensions cycliques réelles de degré 6 de $\mathbb{Q}$. *Publ. Math. Besançon*, 2:1–26, 1984/85-1985/86.

[8] H. Hasse. Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. *Mathematische Abhandlungen*, pages 285–379, 1975.

[9] D. Hilbert. Uber die Irreducibilitat ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. reine angew. Math.*, 110:104–129, 1892.

[10] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, 3rd edition, 2002.

[11] A.J. Lazarus. *The class number and cyclotomy of simplest quartic fields.* PhD thesis, Berkeley, 1989.

[12] J-P. Serre. *Local Fields*. Springer, Berlin, 1979.

[13] K. Uchida. Class numbers of cubic cyclic fields. *J. Math. Soc. Japan*, 26(3):447–453, 1974.

[14] L.C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48(177):371–384, January 1987.

[15] P.J. Weinberger. Real quadratic fields with class numbers divisible by n. *J. Number Theory*, 5:237–241, 1973.

[16] Y. Yamamoto. On unramified galois extensions of quadratic number fields. *Osaka J. Math.*, 7:57–76, 1970.