Number Fields with Large Minimal Index

by

Zack Wolske

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Abstract

Number Fields with Large Minimal Index

Zack Wolske

Doctor of Philosophy

Graduate Department of Mathematics

University of Toronto

2018

The index of an integral element α in a number field K with discriminant D_K is the index of the subring $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$. The minimal index $m(K)$ is taken over all $\alpha \in \mathcal{O}_K$ that generate the field. This thesis proves results of the form $m(K) \ll |D_K|^U$ for all Galois quartic fields and composites of totally real Galois fields with imaginary quadratic fields, and of the form $m(K) \gg |D_K|^L$ for infinitely many pure cubic fields, both types of Galois quartic fields, and the same composite fields, with U and L depending only on the type of field. The upper bounds are given by explicit elements and depend on finding a factorization of the index form, while the lower bounds are established via effective Diophantine approximation, minima of binary quadratic forms, or norm inequalities. The upper bounds improve upon known results, while the lower bounds are entirely new. In the case of imaginary biquadratic quartic fields and the composite fields under consideration, the upper and lower bounds match.

Acknowledgements

To our unions, PSAC local 610, CUPE local 3902 and USW local 1998, for fighting to get livable wages and reduce financial stresses. Together, we're strong.

To the math faculty at UWO, Tatiana Barron, André Boivin, Mike Dawes, Graham Denham, Nicole Lemire, David Riley, and Rasul Shafikov, thank you for your careful instruction and patience. My foundations still stand up to the harshest undergraduate's scrutiny.

To my number theory instructors at Toronto, John Friedlander, Steve Kudla, Arul Shankar, and Jacob Tsimerman, for exposing me to the cutting edge of research. It helped to approach the edge with the sharpest minds.

To Alfonso Gracia-Saz, Jonathan Korman, Mary Pugh, Jason Siefken, and Sean Uppal, for trusting me to teach classes or tutorials, and providing feedback to help me improve. I'm still trying.

To Almut Burchard for her blunt criticisms, and Marcy Robertson for keeping me sane during trying times, and to both for their assistance in transferring from UWO to Toronto.

To my committee members, John Friedlander and Jacob Tsimerman, for their wise remarks and suggestions. I have not resolved all of them yet, but I hope you find something interesting in here.

To my colleagues, Tyson Davis, Daniel Ishak and Enxin Wu at UWO; Dan Fusca, Parker Glynn-Adey, and Mario Palasciano at Toronto; and to Craig Sinnamon at both; thank you for your friendship and commiseration. They were bright spots during dreary days.

To my Master's supervisor, Gord Sinnamon, for inspiring me to study math 12 years ago, encouraging me to continue, and to try again after major setbacks. This is all your fault.

To my supervisor, Henry Kim, for taking a risk. Thank you for your time and patience.

To my partner, Kristen. From UWO to York to Toronto, I wouldn't be here without you.

To my supportive siblings, Nicole, Louise, and Terry, and my mother Jess. You made me the person I am today. Thank you, thank you, thank you, thank you! I think I'm finally done school.

Contents

Notations

- $\mathbb{Z}$, the rational integers.
- $\mathbb{Q}$, the rational numbers.
- K, L or M, a number field, a finite algebraic extension of $\mathbb{Q}$.
- $\alpha, \beta, \gamma, \delta, \xi, \omega$, elements of a number field.
- ζ_n, a primitive n^{th} root of unity.
- minpol(α), the minimal polynomial of α.
- deg(α), the degree of minpol(α).
- $\{\alpha^{(1)}, \ldots, \alpha^{(\deg(\alpha))}\}$, the conjugates of α, the set of roots of minpol(α).
- $\mathcal{O}_K$, the ring of integers of K.
- $\mathcal{O}_K^\times$, the group of units of K.
- ϵ, ν, η, elements of $\mathcal{O}_K^\times$.
- $\mathcal{P} = \{\alpha \in \mathcal{O}_K : K = \mathbb{Q}(\alpha)\}$, the set of primitive integers. There is no standardized notation for this set.
- $\mathbb{Z}[\alpha]$, for $\alpha \in \mathcal{P}$, the $\mathbb{Z}$-module generated by α.
- $\mathrm{Tr}_K(\alpha)$, the trace of $\alpha \in K$, the sum of all conjugates of α.
- $N_{K/\mathbb{Q}}(\alpha)$, the (absolute) norm of $\alpha \in K$, the product of all conjugates of α.
- $N_{K/L}(\alpha)$ the relative norm of $\alpha \in K$ over L, the product of conjugates of α over L.

- D_K, the field discriminant of K.
- $D(\alpha) = D_{K/\mathbb{Q}}(\alpha)$, for $\alpha \in \mathcal{P}$, the discriminant of α.
- $I(\alpha) = \sqrt{D(\alpha)/D_K}$, the index of $\alpha \in \mathcal{P}$.
- $i(K) = \gcd\{I(\alpha), \alpha \in \mathcal{P}\}$, the field index of K.
- $m(K) = \min\{I(\alpha), \alpha \in \mathcal{P}\}$, the minimal index of K.
- $f \gg g$ for functions $f, g : \mathbb{N} \to \mathbb{R}$ if there is a positive real c such that $|f(n)| \geq c|g(n)|$ for all n. Similarly, $g \ll f$.
- $f \gg_a g$ if c is allowed to depend on a.
- $f \asymp g$ if $f \gg g$ and $f \ll g$.
- $\vec{X} = (X_1, \ldots, X_n)$, an ordered list of n variables.

Chapter 1

Introduction

Two of the earliest examples of number fields a student will see are quadratic extensions $\mathbb{Q}(\sqrt{D})$ and cyclotomic extensions $\mathbb{Q}(\zeta_n)$, where we have adjoined to $\mathbb{Q}$ all roots of $x^2 - D$ or $x^n - 1$, respectively. Along with being easy to define and having a rich history in the development of number theory, they share a desirable property: their rings of integers can be written as $\mathbb{Z}[\alpha]$, where α is $\sqrt{D}$ or $\frac{1-\sqrt{D}}{2}$ in the quadratic case, and ζ_n in the cyclotomic case. Number fields with this property are called *monogenic*, and are said to have a *power basis generated by* α. A power basis makes it a pleasure to compute with integers in the field. We can write them down using a basis with a straightforward multiplication table (depending only on the minimal polynomial of α), and the problem of factoring an ideal is replaced by factoring the minimal polynomial of α modulo rational primes. Unfortunately for computational purposes, though somewhat fortunately for the author, this is rarely the reality - many number fields are not monogenic. We measure how far an element $\alpha \in \mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$ comes from generating a power basis by its *index*, $I(\alpha) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, and call the smallest of these values the *minimal index*. It is known the the minimal index can be arbitrarily large when considering all fields, and from the examples above, can be as small as possible infinitely often. To understand what large means, we compare the minimal index to the field discriminant, a natural measure of the size of the field. This thesis answers questions relating the minimal index to the field discriminant: Are there upper bounds on the minimal index in terms of the discriminant, and what are the best upper bounds? Are there families of fields with minimal index bounded below in terms of the discriminant?

Each chapter begins with a short introduction, stating the goals and methods to be used. This is followed by background mathematical information in the terminology and techniques used in the chapter. The experienced number theorist can skip ahead to historical developments and results. The historical sections are generally chronological, but collect results by a group of collaborators as often as possible. For the families of fields in question, this section explains who has: computed integral bases, discriminants and index forms; computed the field index, the common divisor of all indices; showed infinitely or finitely many fields are monogenic; proved the minimal index is unbounded; gave upper or lower bounds on the minimal index; or computed exact minimal index. Finally, sections on results contain the detailed proofs of novel results, along with explanations of the ideas and choices behind them. For a more concise version of some of these, see [68, 69].

1.1 Algebraic Number Theory Background

Many results here can be found in or derived from Jody Esmonde and Ram Murty's book [25]. A complex number θ is *algebraic* if it is a root of a polynomial $f(x)$ with integer coefficients. Factoring if necessary, we can assume that f is irreducible, and denote its degree by n. The field we get by adjoining θ to the rational numbers is denoted $\mathbb{Q}(\theta)$, and is called a *number field* (a field is closed under adding, subtracting, or multiplying any two elements, or dividing by anything non-zero, like $\mathbb{Q}$). It is also an n-dimensional vector space over $\mathbb{Q}$ (closed under adding any elements, or multiplying by numbers from $\mathbb{Q}$), with a basis given by $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$, since $f(\theta) = 0$, we can replace θ^n with some linear combination of lower powers. For any $\alpha \in K$, the function $M_\alpha : K \to K$ given by $M_\alpha(x) = \alpha x$ is a linear transformation, and hence has a matrix representation in the basis $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. The *trace* of this matrix, the sum of elements on the diagonal, does not depend on the choice of basis, so we define the *trace of* α, $\mathrm{Tr}_K(\alpha) \in \mathbb{Q}$ to be the trace of M in any basis. This allows us to define a symmetric, nondegenerate bilinear form $B : K \times K \to \mathbb{Q}$ by $B(x, y) = \mathrm{Tr}_K(xy)$, where nondegenerate means the matrix $[B(\theta^{i-1}, \theta^{j-1})]$ is invertible.

For the rest of this section, we will use $K = \mathbb{Q}(\theta)$ to denote a number field of degree n. Since K is an n-dimensional vector space, for any $\alpha \in K$, the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent.

Thus we can find a polynomial with rational coefficients of degree at most n that α satisfies. So α is also an algebraic number, since we can multiply by any denominators in the coefficients to get a polynomial with integer coefficients. If $f(x)$ is such a polynomial, then we can multiply by any integer or polynomial with integer coefficients to construct another polynomial have α as a root. We prefer our polynomials to be as small as possible, so we define the *minimal polynomial* of α to be the non-zero polynomial with integer coefficients that is irreducible, has positive leading coefficient, and whose coefficients have no common divisor. The reader can prove it is unique (Hint: multiply two such polynomials by integers to make their leading coefficients equal, then subtract to get another polynomial - it must be zero).

In general, a number field is constructed by adjoining any finite number of algebraic numbers, e.g. $\mathbb{Q}(\alpha, \beta)$. By the primitive element theorem, we can always find a single element that generates the field, so that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ for some θ, and the powers of θ are a basis for the vector space. There is a very concise proof in [25]: if α and β have minimal polynomials $f(x)$ and $g(x)$, respectively, define a family of polynomials $h_q(x) = f(\alpha + q\beta - qx)$ for each $q \in \mathbb{Q}$. Choosing q so that $g(x)$ and $h_q(x)$ have only the root β in common forces $\alpha, \beta \in \mathbb{Q}(\alpha + q\beta)$, so taking $\theta = \alpha + q\beta$ gives the desired generator.

The set of elements whose minimal polynomial is monic (has leading coefficient 1) is called the *ring of (algebraic) integers of* K and denoted $\mathcal{O}_K$ (a ring is closed under adding, subtracting or multiplying two elements, but not necessarily dividing). Just like the rational integers $\mathbb{Z}$ are a special set inside the field $\mathbb{Q}$, the ring of integers $\mathcal{O}_K$ is special inside of K. If α is algebraic, with minimal polynomial $p(x) = a_n x^n + \cdots a_0$, then $a_n^{n-1} p(x) = (a_n x)^n + \cdots a_n^{n-1} a_0$ is a monic minimal polynomial of $a_n \alpha$, hence $a_n \alpha \in \mathcal{O}_K$.

An *integral basis* for $\mathcal{O}_K$ is a set $\{\omega_1, \ldots, \omega_n\}$ of algebraic integers such that every element of $\mathcal{O}_K$ is a linear combination of them, using coefficients from $\mathbb{Z}$. To show that such a basis exists, first note that by scaling each element of a basis $\{\omega_1, \ldots, \omega_n\}$ for the vector space K as we did to get $a_n \alpha \in \mathcal{O}_K$, we can assume all $\omega_i \in \mathcal{O}_K$. Define a dual basis for K, $\{\omega_1^*, \ldots, \omega_n^*\}$, where $\mathrm{Tr}_K(\omega_i, \omega_i^*) = 1$ and $\mathrm{Tr}_K(\omega_i, \omega_j^*) = 0$ for all $i \neq j$. For $\alpha \in \mathcal{O}_K$, writing $\alpha = \sum c_i \omega_i^*$, we have $\mathrm{Tr}(\alpha \omega_i) = c_i \in \mathbb{Z}$, for all i, since $\alpha \omega_i \in \mathcal{O}_K$. Thus $\mathcal{O}_K \subseteq \mathbb{Z}\,\omega_1^* + \cdots \mathbb{Z}\,\omega_n^*$. Then, as a submodule of a finitely generated $\mathbb{Z}$ module, $\mathcal{O}_K$ has an integral basis.

When K is monogenic, we have $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some θ with minimal polynomial $f(x)$. In

this case, the factorization of a rational prime p into prime ideals of $\mathcal{O}_K$ corresponds to the factorization of $f(x) \pmod p$. This result goes back to Dedekind, beginning the search to classify monogenic fields and showing the existence of non-monogenic fields. Suppose $f(x) \equiv \prod \overline{f_i(x)^{e_i}} \pmod p$, where each $\overline{f_i}$ is irreducible over $\mathbb{F}_p$ and choose monic lifts $f_i \in \mathbb{Z}[x]$ of $\overline{f_i}$. Let $\mathfrak{p}_i = (p, f_i(\theta))$ denote the ideal in $\mathcal{O}_K$ generated by p and $f_i(\theta)$.

We first show that $\mathfrak{p}_i$ is prime by showing $\mathcal{O}_K/\mathfrak{p}_i$ is a field: Since $\overline{f_i(x)}$ is irreducible over $\mathbb{F}_p$, $\mathbb{F}_p[x]/(\overline{f_i(x)}) \cong \mathbb{Z}[x]/(p, f_i(x))$ is a field. Then $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{Z}[x]/(p, f_i(x))$ if the kernel of the evaluation map $\mathbb{Z}[x] \to \mathbb{Z}[\theta]/\mathfrak{p}_i$ is exactly $(p, f_i(x))$, using $\mathcal{O}_K = \mathbb{Z}[\theta]$. For any $g(x) \in \mathbb{Z}[x]$, we can write $g(x) = q(x)f_i(x) + r(x)$, where $\deg r(x) < \deg f_i(x)$, since f_i is monic. If $g(\theta) \in \mathfrak{p}_i$, then so is $r(\theta)$, so $r(\theta) = pa(\theta) + f_i(\theta)b(\theta)$ for some $a(\theta), b(\theta) \in \mathbb{Z}[\theta]$. The polynomial

$$h(x) = pa(x) + f_i(x)b(x) - r(x) \in \mathbb{Z}[x]$$

has θ as a root, hence is a multiple of the minimal polynomial $f(x)$. By definition, $f(x) - \prod(f_i(x))^{e_i} \in p\,\mathbb{Z}[x]$, so $f(x) \in (p, f_i(x))$. Thus $r(x) \in (p, f_i(x))$, and so is $g(x)$.

Next, we show that $p\mathcal{O}_K = \prod \mathfrak{p}_i^{e_i}$: We have shown that $\mathfrak{p}_i$ divides $p\mathcal{O}_K$, so let e_i' be the largest integer such that $\mathfrak{p}_i^{e_i'}$ divides $p\mathcal{O}_K$. By the above, we have $\prod(f_i(\theta))^{e_i} \in p\,\mathbb{Z}[\theta]$, and since $\mathfrak{p}_i^{e_i} \subseteq p\mathcal{O}_K + (f_i(\theta))^{e_i}$, we have $\prod(\mathfrak{p}_i)^{e_i} \subseteq p\mathcal{O}_K$, thus each $e_i \geq e_i'$. Considering powers of θ, we see the index $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\,\mathbb{Z}]$ is the degree of $f_i(x)$, and so

$$\deg f = [K : \mathbb{Q}] = \sum [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\,\mathbb{Z}]e_i' = \sum e_i' \deg f_i(x),$$

thus $e_i = e_i'$.

If $K = \mathbb{Q}(\theta)$ is an n-dimensional vector space, then θ has a degree n minimal polynomial $f(x)$. The roots of $f(x)$ are called *conjugates* of θ, and denoted $\theta^{(i)}$ for $i = 1, \ldots, n$. We choose $\theta = \theta^{(1)}$, but the remaining roots can be in any order. We can define n different *field embeddings* $\sigma_i : K \to \mathbb{C}$, sending θ to $\theta^{(i)}$, and for any other element α, writing α in terms of θ, then replacing each θ by $\theta^{(i)}$. This way we have conjugates $\alpha^{(i)} = \sigma_i(\alpha)$ for any element, and they will all be distinct if and only if the minimal polynomial of α has degree n, that is, $K = \mathbb{Q}(\alpha)$. The set of elements in $\mathcal{O}_K$ with $K = \mathbb{Q}(\alpha)$ are called *primitive* integers, and

we will write $\mathcal{P}$ for primitive integral elements. The *discriminant* of an element $\alpha \in \mathcal{O}_K$ is $D(\alpha) = \prod_{i<j} \left(\alpha^{(i)} - \alpha^{(j)}\right)^2$. Notice that if two conjugates are equal, this is 0, but otherwise it is non-zero, so in particular, it is nonzero for every $\alpha \in \mathcal{P}$. Any rational integer a is fixed by every embedding, so $D(\alpha + a) = \Delta(\alpha)$. The *norm* of an integral element is the product of all of its conjugates. This is a rational integer, since it has the same absolute value as the constant term of the minimal polynomial. The norm of α can be shown to be the same as the determinant of M_α, but we will not use this fact.

We are now in a position to define the *field discriminant*, D_K. Choose an integral basis $\{\omega_1, \ldots, \omega_n\}$ of $\mathcal{O}_K$, and form the $n \times n$ matrix $(\omega_j^{(i)})$, whose (i,j)-entry is $\omega_j^{(i)}$. Then $D_K = \det(\omega_j^{(i)})^2$. The geometrically-minded reader may want to view this as the square of the volume of a fundamental domain in an n-dimensional lattice, and hence related to the size of $\mathcal{O}_K$. Specifically, we define the discriminant of n linearly independent integers $D(\beta_1, \ldots, \beta_n) = \det(\beta_j^{(i)})^2$. For the next step, we will need the Vandermonde determinant identity. For any complex numbers $c_1, \ldots, c_n$:

$$\begin{vmatrix} 1 & c_1 & c_1^2 & \cdots & c_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & c_n & c_n^2 & \cdots & c_n^{n-1} \end{vmatrix}^2 = \prod_{i<j} (c_i - c_j)^2.$$

For $\alpha \in \mathcal{P}$, applying this to the n conjugates of α, we have $D(\alpha) = D(1, \alpha, \ldots, \alpha^{n-1})$. Both sets $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and $\{\omega_1, \ldots, \omega_n\}$ are bases for K over $\mathbb{Q}$, so there is a change of basis matrix Q such that

$$[\omega_1, \ldots, \omega_n]Q = [1, \alpha, \ldots, \alpha^{n-1}].$$

Further, since every α^j is integral, Q has rational integer entries. Thus, the same matrix transforms conjugates of $\{\omega_j^{(i)}\}$ to the conjugates of powers of $\alpha^{(i)}$, since the rationals are fixed under every embedding. So, finally, (writing $\alpha^j = \alpha_j$ for notational purposes) we have

$$D(\alpha) = \det(\alpha_j^{(i)})^2 = \det\left((\omega_j^{(i)})Q\right)^2 = D_K \det Q^2.$$

We call $|\det Q|$ the *index of* α, and denote it $I(\alpha)$. For the geometrically-minded, $D(\alpha)$ is the

square of a volume, and since each power of α is an integral linear combination of $\{\omega_j\}$, that volume is a rational integer multiple of the volume of the fundamental domain defined by the integral basis. Removing squares and taking the positive sign, the multiple is the index. For the ring and lattice enthusiasts, or the historically minded, $\mathbb{Z}[\alpha]$ is a full-rank submodule of $\mathcal{O}_K$ when $\alpha \in \mathcal{P}$ and $I(\alpha) = [\mathcal{O}_K^+ : \mathbb{Z}[\alpha]^+]$, hence the name - it measures the index of the additive subgroup $\mathbb{Z}[\alpha]^+$ in $\mathcal{O}_K^+$.

Our definition may seem to depend on the choice of integral basis, since another basis will produce a different transformation, say Q'. But then $Q = \gamma Q'$ for some invertible matrix with integer entries $\gamma \in \mathrm{GL}_n(\mathbb{Z})$, and so $\det \gamma = \pm 1$. Thus $|\det Q| = |\det Q'|$, and $I(\alpha)$ is the same, no matter which integral basis we choose.

1.1.1 Historical Development

We begin with a history of results relating to indices. Some of these are discussed in more detail in the chapters on cubic fields, quartic fields, and fields containing quadratic subfields. This should not be taken as exhaustive or definitive, but rather a roughly chronological collection explaining where the major questions came from, who has contributed to their solutions, and what remains unanswered.

Suppose K is monogenic, so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α with minimal polynomial $f(x)$. Then the prime ideal factorization of $p\mathcal{O}_K$ correspond to the irreducible factors of $f(x)$ over $\mathbb{F}_p$. In 1878, Richard Dedekind established and used this correspondence [17], noting that there are exactly p primitive, linear factors over $\mathbb{F}_p$, so finding a cubic field where the ideal $2\mathcal{O}_K$ splits into 3 prime ideals of degree 1 shows that such a field cannot be monogenic. The field generated by a root of $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$ is his example, and after computing an integral basis $\{1, \alpha, \beta\}$, where $\beta^3 + \beta^2 + 2\beta - 8 = 0$, he finds the field discriminant is -503, and so $2\mathcal{O}_K$ does not ramify. He then shows it cannot split as $\mathfrak{pq}$, and hence must factor as $\mathfrak{abc}$ for distinct ideals. Along with this, by writing an integer $\omega = z + x\alpha + y\beta$ and computing its discriminant, he gives the index as a function of rational integers,

$$I(x, y) = 2x^3 - x^2y - xy^2 - 2y^3.$$

This makes it clear that every integer has even index, and introduces the first example of an *index form*, which we will use frequently. It also motivates the most common question in the area: Which fields are monogenic? [90, Problem 6]

This example of a non-monogenic field is used in the third edition (1879) of "Dirichlet-Dedekind" [20] as an early result from Dedekind's theory of ideals. It had already appeared in the second edition in 1871 (Stück 38), along with an example of a quartic field generated by a root of $\alpha^4 - \alpha^3 + \alpha^2 - 2\alpha + 4 = 0$ where $2\mathcal{O}_K$ factors as a product of two distinct ideals of degree 2. There is a unique monic, irreducible quadratic polynomial over $\mathbb{F}_2$, so this field is also not monogenic. This example is frequently overlooked in modern references, possibly because it lacks all of the computations of the cubic example and came before the published, rigorous and polished theory of ideals.

In both of these examples, every element has even index. A rational integer is called an *inessential divisor* of K (or a *common index divisor*) if it divides the index of every algebraic integer in $\mathcal{O}_K$, and is so called because it is a divisor of the discriminant of every element, but not a divisor of the field discriminant. We will denote the *field index* of K by

$$i(K) = \gcd\{I(\alpha) : \alpha \in \mathcal{P}\}.$$

Kurt Hensel [62] generalized Dedekind's constructions to show that $p|i(K)$ if and only if there are more ideal divisors of p with degree f than there are monic irreducible polynomials of degree f over $\mathbb{F}_p$ for some f. Although it is a complete characterization, it depends on finding the factorization of $p\mathcal{O}_K$ into prime ideals when the field is not necessarily monogenic, which is generally difficult. One particular reason to seek out monogenic fields is that they reduce the ideal factorization problem to the simpler problem of factoring a polynomial over a finite field.

If p is a prime $p < n$, Michael Bauer [3] showed that $p|i(K)$ for some field K of degree n in 1907, and in 1913, E. von Żyliński [110] proved the converse, that $i(K)$ only has prime divisors $p < n$. In 1930, Howard Engstrom [24] computed all possible exponents in the field index of such primes, which motivated the question: which of the possible field indices actually occur, and are there restrictions depending on the Galois closure of degree n fields? [90, Problem 22] Examples with $i(K) > 1$ are of course not monogenic, so it is an interesting problem to classify

them and their relative proportion among all fields, as well as to find non-monogenic fields with $i(K) = 1$ (that is, fields which are not monogenic, but not for a local reason).

In 1937, Marshall Hall Jr. showed that the minimal index, in contrast to the field index, is unbounded in cubic fields [59]. These are the first example of fields that are far from being monogenic, in the sense that only monogenic fields satisfy $m(K) = 1$. The proof is covered in more detail in the chapter on cubic fields, and was the starting point in the search for fields with $m(K) \gg |D_K|^N$ for some $N > 0$, which is the goal of that chapter.

Marie-Nicole Gras rekindled interest in the problem in the 1970s and early 1980s by giving necessary and sufficient conditions for cyclic and abelian fields to be monogenic, and showed that if n is not divisible by 2 or 3, then only finitely many abelian fields of degree n are monogenic [47, 48, 49, 50, 52]. The results are not generally effective, but in the case of cyclic fields of prime degree $p \geq 5$, K is monogenic only when $2p+1$ is prime and it is the maximal real subfield of $\mathbb{Q}(\zeta_{2p+1})$. These results are summarized in a conference paper [51] and extended by Georges Gras [46] to give more examples of non-monogenic fields. She later worked with François Tanoé to give necessary and sufficient conditions for a biquadratic field to be monogenic [53].

David Dummit and Hershey Kisilevsky computed the index forms for cyclic cubic fields in 1977, and used this to show that the minimal index is unbounded over all cyclic cubic fields, but has an explicit upper bound in terms of the discriminant for a given field, $m(K) \ll |D_K|^{\frac{1}{4}}$, and that infinitely many such fields are monogenic [21]. This is the first result bounding the minimal index by a power of the absolute field discriminant. Later results of this type were given by Jeffrey Lin Thunder and John Wolfskill [106], and are improved in some cases in the chapters on quartic fields and fields containing a quadratic subfield.

Kálmán Győry began a program at Debracen University, Hungary, in the 1970s to study solutions to norm form, discriminant, and index form equations (see [54, 55, 56, 57, 58]). The general strategy is to apply Baker's method to the linear forms which arise from those equations to get upper bounds on the size of possible solutions. His work showed that there are only finitely many generators for any monogenic field (where two generators which differ by a rational integer are not considered distinct), developed effective algorithms to find them and included many computational results. The program was continued by his students, István Gaál and Attila Pethő (at Debracen, working in mathematics and computer science, respectively) and

their frequent collaborator Michael Pohst (TU Berlin), (see [29, 28, 34, 35, 31, 32, 36, 33, 26]). Their work applies the strategy to families of fields by degree and Galois group, and usually answers the questions: Which fields are monogenic, and when they are, which α have $\mathcal{O}_K = \mathbb{Z}[\alpha]$? This work is being continued by Gaál's students Tímea Szabó, and László Remete (see [38, 39, 40, 41, 42, 43, 44]). In cases where the fields cannot all be classified as monogenic or not, they include algorithms to check specific fields, and computations for all fields below a fixed discriminant bound.

Toru Nakahara seems to have coined the phrase "a problem of Hasse," for determining whether a field or family of fields is monogenic, in the first faculty report at Saga University in 1973 [84, 85]. It may have been inspired by the second edition of Hasse's "Zahlentheorie" [61], according to Gaál [28, p. 1], but it is not clear if Hasse ever posed it directly. It does not appear where Gaál indicates, and every reference to the phrase factors through Nakahara's papers. Regardless of the name, Nakahara published many results on this topic [86, 87, 88], summarized many known results, [89] and inspired colleagues Yasuo Motoda [79, 80], Syed Inayat Ali Shah [93, 94, 95, 92], Tsuyoshi Uehara [81], Yoshifumi Kôhno, and Mamoona Sultan [103]. Results from this group often use Gauss and character sums with the goal of constructing infinitely many monogenic fields with prescribed Galois group or in parametrized families, or showing that all but finitely many are not monogenic.

Blair Spearman (UBC Okanagan) and Kenneth Williams (Carleton University) collaborated on over 80 papers, including many related to the question possible field indices. [98, 99, 100, 101] They - along with other contributors including Daniel Eloff, James Huard, Richard Hudson, Melissa Lavalee, Alan Sylvester, Qiduan Yang, and Jeewon Yoo - computed integral bases and discriminants for families of number fields, which could then be used to compute the index form, determine monogeneity, and answer questions relating to the field index (see [23, 60, 64, 70, 71, 72, 96, 102]).

1.2 Index Specific Background

Results that are specific to the index form can be found in [90, sec. 2.2], and concisely summarized in [28]. We begin by deriving the index form by matrix determinants [90, Prop. 2.9,

2.13]. Given an integral basis $\{\omega_1 = 1, \omega_2, \ldots, \omega_n\}$, and writing $\vec{X} = (X_1, \ldots, X_n)$, define the linear form $\ell(\vec{X}) = \sum_{i=1}^{n} \omega_i X_i$. Note that $D(\ell(\vec{X})) = D(\ell(\vec{X}) + a)$ for any rational integer a, so we are not concerned with the term $\omega_1 X_1$. To apply the Vandermonde determinant identity, write $\ell(\vec{X})^{i-1} = \sum F_j i(\vec{X})\omega_j$ for some degree $i-1$ homogeneous integral forms $F_j i$. Thus

$$\begin{aligned}
D(\ell(\vec{X})) &= \prod_{i<j} \left(\ell^{(i)}(\vec{X}) - \ell^{(j)}(\vec{X})\right)^2 \\
&= \begin{vmatrix} 1 & \ell(\vec{X}) & \cdots & \ell(\vec{X})^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \ell^{(n)}(\vec{X}) & \cdots & \ell^{(n)}(\vec{X})^{n-1} \end{vmatrix}^2 \\
&= \begin{vmatrix} 1 & \omega_2 & \cdots & \omega_n \\ \vdots & \vdots & & \vdots \\ 1 & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2 \begin{vmatrix} F_{11}(\vec{X}) & F_{12}(\vec{X}) & \cdots & F_{1n}(\vec{X}) \\ \vdots & \vdots & & \vdots \\ F_{n1}(\vec{X}) & F_{n2}(\vec{X}) & \cdots & F_{nn}(\vec{X}) \end{vmatrix}^2 \\
&= D_K I(\vec{X})^2.
\end{aligned}$$

Since each F_{ji} is homogeneous, $I(\vec{X})$ is as well, and has degree $\sum_{i=0}^{n-1} i = n(n-1)/2$. This factorization only determines $I(\vec{X})$ up to sign, so when evaluating $I(\alpha)$, we will use $|I(\vec{X})|$. The representation depends on the choice of integral basis, and eliminating the variable X_1 depended on having $\omega_i = 1$. Any $\gamma \in \mathrm{GL}_{n-1}(\mathbb{Z})$ changes $\{\omega_j\}$ to an integral basis $\{\omega'_j\}$ with $\omega'_1 = 1$, and corresponding $I'(\vec{X}) = I(\gamma(\vec{X}))/\det(\gamma)$. Conversely, any integral basis with initial term 1 defines a change of basis $\gamma \in \mathrm{GL}_{n-1}(\mathbb{Z})$ with the same property. Choosing an appropriate basis will express $I(\vec{X})$ in a form we are interested in, so we will make note of the bases we use to compute I. Note that if $I(\alpha) = m$, for $\alpha \in \mathcal{P}$, then by extending $\{1, \alpha\}$ to an integral basis, we have $I(\vec{X}) = \pm m X_2^{\frac{n(n-1)}{2}} + \text{other terms}$. Thus, we can express $m(K) = \min\{|\text{coefficient of } X_2|\}$ as I varies over all $\mathrm{GL}_{n-1}(\mathbb{Z})$ equivalent forms.

For fixed degree number fields, upper bounds on $m(K)$ in terms of $|D_K|$ were given for any number fields by Jeffrey Lin Thunder and John Wolfskill in 1996.

Theorem 1.1. *[106, Thm. 1] Let K be a number field of degree $n = r + 2s$, r the number of real places, s the number of complex places, c the maximum degree of a proper subfield of K,*

and $t = \min\{c, \log_2 n\}$. *Then*

$$m(K) < \left(n^2 t \left(\frac{2}{\pi} \right)^{\frac{s}{n-c}} \right)^{\frac{n(n-1)}{2}} |D_K|^{\frac{n^2-3n+2c}{4(n-c)}}$$

For number fields with fixed Galois group, as we will consider, n and c are fixed, so $m(K) \ll |D_K|^{\frac{n^2-3n+2c}{4(n-c)}}$. This upper bound is largest when $n = 2c$, in which case $m(K) \ll |D_K|^{\frac{n-2}{2}}$. We will improve on this for certain fields arising as quadratic extensions of number fields in Chapter 3. In the other direction, the upper bound is lowest when K has no nontrivial proper subfields, in which case $m(K) \ll |D_K|^{\frac{n-2}{4}}$. The proof, as hinted by the factor $\frac{2}{\pi}$ and the dependence on $|D_K|$, depends on Minkowski's convex body theorems to determine the volume of a minimal fundamental region in a lattice defined by embedding $\mathcal{O}_K$ in $\mathbb{R}^n$. Further, they find families of fields in each even degree $n \geq 4$ which asymptotically achieve the higher upper bound: there are infinitely many K of degree n such that $m(K) \gg_n |D_K|^{\frac{n-2}{2}}$ [106, Thm. 3]]. This is done by constructing an imaginary quadratic extension of a totally real field of degree $n/2$. These results, along with Nakahara's result on the unboundedness of $m(K)$ in imaginary V_4 fields, give the extent of what is currently known about the relations between $m(K)$ and $|D_K|$. In this thesis, we expand the examples of fields K with $m(K) \gg |D_K|^L$ for some L to include cubic fields (the only known case of odd degree), C_4 fields, composites of totally real fields and imaginary quadratic fields, and a conjectured family of real V_4 fields. We also improve the upper bounds above in the cases of V_4 fields, C_4 fields, and the same composites of fields.

1.3 Statement of Results

The results in this thesis are of two types, each relating the minimal index of a field to its discriminant. There are lower bound theorems, stating that there are infinitely many fields K such that $m(K) \gg |D_K|^L$ for some $L > 0$ depending on the type of field, and upper bound theorems, stating that every field K satisfies $m(K) \ll |D_K|^U$, for some $U > 0$ depending on the type of field. These latter theorems should be compared to the results of Thunder and Wolfskill at the end of the previous section. The former results have no predecessors in the literature, but can be compared to the known upper bounds, which are expected to be optimal.

Theorem 1.2. *There are infinitely many pairs of positive integers $a < b$ that are squarefree and coprime, such that $a > 125 \cdot 10^{120}$, $a \equiv b \bmod 3$, and $\sqrt[4]{a} < b - a < \frac{3}{2}\sqrt[4]{a}$. For all of these integers, the pure cubic fields $K = \mathbb{Q}(\sqrt[3]{ab^2})$ have $m(K) \gg |D_K|^{\frac{1}{16}}$.*

This result for cubic fields comes from the best known effective Diophantine approximation using the hypergeometric method, where explicit constants are generally small. It gives lower bounds on any rational approximation to a cube root of a rational number close to 1. That is why the theorem only applies if a and b are sufficiently large, and why they must be relatively close to each other. In number fields with degree larger than 3, the index form has at least 3 variables, so a similar approach would require results from "simultaneous Diophantine approximation," which are not currently strong enough to deduce lower bounds in terms of the field discriminant.

Theorem 1.3. *Let a, b be negative, squarefree, coprime integers. For every positive, squarefree integer c coprime to ab, the V_4 quartic field $K = \mathbb{Q}(\sqrt{ac}, \sqrt{bc})$ has $m(K) \gg_{a,b} |D_K|^{\frac{1}{2}}$.*

The lower bound for this family of biquadratic fields was first noted by Nakahara [86] as an example of a family with unbounded minimal index, though it is not given in terms of the discriminant. The proof relies on factoring the index form into three quadratic forms, and choosing an integral basis so that two are obviously positive definite. The bound is optimal in the sense that it matches the upper bound in the following theorem:

Theorem 1.4. *If K is a V_4 quartic field, then $m(K) \ll |D_K|^{\frac{1}{2}}$.*

The situation for C_4 quartic fields is more complicated, because it has only one proper subfield, and so the index form factors into two irreducible forms, compared to the three factors in V_4 fields. The known upper bounds cannot be improved without limiting the family of fields.

Theorem 1.5. *If $K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})})$ is a C_4 quartic field, with $D = B^2 + C^2$, $(A, D) = 1$ and both A, D square-free, then $m(K) \leq 16A^2BC \min\{B, C\}$. If A is fixed, then for all D that give a C_4 field, we have $m(K) \ll_A |D_K|^{\frac{1}{2}}$.*

The proofs of upper bounds for V_4 and C_4 quartic fields are by construction, finding an element with small index in each case, so the implied constants can be made explicit.

By restricting to a family parametrized by a single variable, we can find C_4 quartic fields with lower bound matching the upper bound in terms of A, B, C, but they are not optimal in terms of the discriminant.

Theorem 1.6. *There are infinitely many pairs of integers A, B such that the C_4 quartic field $K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})})$ with $D = B^2 + 1$ has $m(K) \gg A^2B$. For the given family, we have $m(K) \gg |D_K|^{\frac{2}{7}}$.*

The proof crucially uses lower bounds on the norms of (most) elements in the quadratic field $\mathbb{Q}(\sqrt{B^2+1})$. Extending the result to cyclic fields with other real quadratic subfields would require information about the unit group and principal ideals of small norm in $\mathbb{Q}(\sqrt{D})$.

The remaining results are on compositum fields, $K = LM$, where M is a totally real field and L is an imaginary quadratic. If M is fixed and L varies, the upper and lower bounds on $m(K)$ match:

Theorem 1.7. *Let M be a totally real degree m Galois field. For every imaginary quadratic field L such that $(D_L, D_M) = 1$, the minimal index of $K = LM$ satisfies $m(K) \ll_M |D_K|^{\frac{m-1}{2}}$.*

Theorem 1.8. *Let M be a totally real degree m Galois field M with odd discriminant. There are infinitely many imaginary quadratic fields L such that $K = LM$ has $m(K) \gg_M |D_K|^{\frac{m-1}{2}}$.*

The proofs depend on factoring the index form and considering norm inequalities. Again, the upper bounds are given using explicit elements, so the implied constants can be recovered.

If instead we fix L, then for the well-known family of Shanks' simplest cubic fields, we have

Theorem 1.9. *Let $L = \mathbb{Q}(\sqrt{b})$ for a fixed $b < 0$, $b \equiv 2, 3 \pmod 4$. If M is any of Shanks' simplest cubic fields such that D_M is coprime to D_L, then $K = LM$ has $m(K) \ll_b |D_K|^{\frac{1}{2}}$*

Theorem 1.10. *Let $L = \mathbb{Q}(\sqrt{b})$ for $b < 0$, $b \equiv 2, 3 \pmod 4$. Infinitely many of Shanks' simplest cubic fields M give $K = LM$ with $m(K) \gg_b |D_K|^{\frac{1}{8}}$.*

This is an interesting example of a family where both $m(L) = m(M) = 1$, while $m(LM)$ is relatively large. The proofs use norm inequalities in both the quadratic and cubic subfields. Shanks' cubics are a rare example of a parametrized family of totally real fields, where all elements of $\mathcal{O}_K \setminus \mathbb{Z}\,\mathcal{O}_K^\times$ have norms bounded away from 0. Extending to other totally real fields

would require similar families, with sufficiently few algebraic integers having small norms, so that they can be considered case-by-case.

Chapter 2

Cubic Fields

2.1 Introduction

The index forms of cubic fields are irreducible integral binary cubic forms,

$$F(x, y) = a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3.$$

There are a number of tools available to study the solutions to $F(x, y) = k$ with $x, y \in \mathbb{Z}$. It is a Thue equation, the canonical and smallest example of one, and thus there are only a finite number of solutions for any given k, an early result in Diophantine approximation. These equations can be solved efficiently when $|y| < C$ for some large C [91], so for a given field, we can compute the minimal index when given the index form. However, these techniques cannot rule out solutions with $|y| > C$, and do not apply to families of fields - they require the continued fraction expansion of a real root of $F(x, 1) = 0$ (or other Diophantine approximations). These can be computed term-by-term, but as algebraic numbers of degree 3, they do not conform to any known patterns, and depend on the particular representative chosen among equivalent index forms.

We focus on the fields having diagonal index forms $F(x, y) = a_0x^3 + a_3y^3$, which arise from pure cubic fields $\mathbb{Q}\left(\sqrt[3]{a_0a_3^2}\right)$ where 3 wildly ramifies. They provide a nice family of index forms, and the real roots $\sqrt[3]{\dfrac{-a_3}{a_1}}$ are the most studied algebraic numbers in the field of Diophantine approximations. We use a recent advancement in effective Diophantine approximations by

Voutier [108] to construct an infinite family of pure cubic fields satisfying $m(K) \gg |D_K|^{\frac{1}{16}}$. This is the first result of its kind for cubic fields, appearing in [69], and would not have been possible over ten years ago using the best known approximations.

2.1.1 Historical Development

As the simplest non-trivial case, the index problem for cubic fields has been extensively studied. A cubic field extension is Galois if and only if its discriminant is a square, in which case its Galois group is C_3 and it is called a *cyclic cubic* field. Any other cubic field is not Galois, and since the Galois closure $\tilde{K}$ of any number field K contains $\sqrt{D_K}$. Such a field has Galois group S_3, we must have $\tilde{K} = K(\sqrt{D_K})$. The earliest results on the index was studied were the *pure cubic* fields, $K = \mathbb{Q}(\sqrt[3]{m})$ for a cubefree integer m. Writing

$$m = ab^2,\ \alpha = \sqrt[3]{ab^2},\ \beta = \sqrt[3]{a^2b},\ \gamma = \frac{1 + a\alpha + b\beta}{3},$$

Richard Dedekind [18, p. 53] classified them into two families: the first type if $a^2 \not\equiv b^2 \bmod 9$, in which case an integral basis is given by $\{1, \alpha, \beta\}$ and $D_K = -3(3ab)^2$; and the second type if $a^2 \equiv b^2 \bmod 9$, where an integral basis is given by $\{\alpha, \beta, \gamma\}$ and $D_K = -3(ab)^2$. In modern parlance, we would note that 3 is wildly ramified, with $3\mathcal{O}_K = \mathfrak{p}^3$, in the first case, and tamely ramified, with $3\mathcal{O}_K = \mathfrak{p}^2\mathfrak{q}$, in the second. Modifying the second type by changing signs to make $a \equiv b \bmod 3$, Marshall Hall, Jr. computed their respective index forms [59] in 1937:

$$\begin{aligned} I(x,y) &= ax^3 - by^3 && \text{for the first type} \\ I(x,y) &= 3ax^3 + 3ax^2y + axy^2 + \frac{a-b}{9}y^3 && \text{for the second type} \end{aligned}$$

In the intervening years, Bauer [3], von Zylinski [110] and Engstrom [24] had shown that the field index $i(K)$ could only be 1 or 2. In contrast, Hall showed that the minimal index is unbounded. Hall's argument is used for other fields - see [102] for an argument finding the exact minimal index, or [86] for an argument in real biquadratic fields - so we repeat its essence here. Fix a positive integer N, and choose a set of primes $\{p_1, \ldots, p_N\}$ that are each congruent to 1 mod 6 and $p_i > i$. Let $b = 3\prod_{i=1}^{N} p_i$. For each prime, choose a non-zero congruence class

A_i such that $A_i x^3 \equiv i \pmod{p_i}$ has no solution. Such an A_i always exists, since only one-third of the non-zero congruence classes mod p_i are cubes. Choosing a to satisfy the simultaneous congruences $a \equiv A_i \bmod p_i$ and $3 \nmid a$ ensures that the field is of the first type, and $ax^3 - by^3 = i$ has no solution for every $1 \leq i \leq N$, hence the minimal index $m(K) > N$.

In his thesis, subsequently published [76], Friedrich Levi first proved what is commonly called the Delone-Faddeev correspondence, after its use by Boris Delone and Dmitry Faddeev [19]: Any triple of conjugate cubic integral domains uniquely corresponds to a $GL_2(\mathbb{Z})$ equivalence class of integral binary cubic forms. This extends to a correspondence between cubic orders and irreducible forms, and is discriminant preserving. A cubic number field K can be identified with its maximal cubic order, the ring of integers $\mathcal{O}_K$, and the Delone-Faddeev correspondence gives the equivalence class of its index form. The other forms in the same equivalence class come from choose a different integral basis for $\mathcal{O}_K$. Harold Davenport and Hans Heilbronn used this correspondence to find the asymptotic density of cubic number fields, ordered by discriminant, counting maximal cubic orders by determining the proportion of binary cubic forms with no square factors modulo every prime.

Louis Mordell (see [16]) showed that for any real binary cubic form $F(x, y)$ with determinant $D \neq 0$ (this is the negative of the polynomial discriminant), there are integers $(x, y) \neq (0, 0)$ such that $0 < F(x, y) \leq c_{\pm}|D|^{1/4}$, where $c_+ = 23^{-1/4}$, and $c_- = 7^{-1/2}$ corresponding to the sign of D. Hence, any cubic number field has an integral element of index $\ll |D_K|^{\frac{1}{4}}$ which generates the field. Further, these constants are only achieved by one $GL_2(\mathbb{Z})$ equivalence class of forms each, which represent the cubic fields of discriminant -23 and 49, respectively.

Consider a binary form with rational integer coefficients $F(x, y)$, of degree at least 3. If $F(x, y)$ is irreducible and $m \in \mathbb{Z}$, then $F(x, y) = m$ is known as a *Thue equation* after Axel Thue, who showed that it has finitely many solutions $(x, y) \in \mathbb{Z}^2$ in 1909 [105]. Determining the number of such solutions and their size has spurred decades of research and many effective techniques for their resolution. Since the index form of a cubic field is an irreducible binary cubic form with integer coefficients, the minimal index of a specific cubic field can be found by searching for solutions to $I(x, y) = \pm i$ for each $i = 1, \ldots, m(K)$. Effective Thue solvers are built into many modern computer algebra systems, which work by repeatedly applying effective upper bounds to the size of possible solutions [107, 6, 10]. The bounds can be lowered to a

range that is small enough to search using the rational approximations to $I\left(\frac{x}{y},1\right)=0$. See [28, §3.1] for current applications in cubic fields.

Marie-Nicole Gras [47] gave necessary and sufficient conditions for a cyclic cubic field to be monogenic - K is monogenic iff it has a unit $\epsilon \in \mathcal{O}_K^{\times}$ such that $\mathrm{Tr}(\epsilon+\epsilon^{-1})=-3$, and $\mathrm{Tr}(\epsilon^2+\epsilon^{-1})=\frac{n^3}{\sqrt{D_K}}$, where $n\in\mathbb{Z}$. Soon after, David Dummit and Hershey Kisilevsky [21] and independently, James Huard in his thesis [63], showed that the minimal index is unbounded in cyclic cubic fields. Dummit and Kisilevsky also gave the upper bound $m(K)\ll |D_K|^{\frac{1}{4}}$ by directly computing the index form using a normal basis.

Blair Spearman, Qiduan Yang, and Jeewon Yoo [102] show that every positive cubefree integer N is the minimal index for infinitely many pure cubic fields, using a similar method to Hall and giving an explicit element of index N. The construction does not extend to integers divisible by p^3, but such fields are known to exist, and an example with $m(K)=8$ is given.

Jeffrey Lin Thunder and John Wolfskill, [106, p. 381] note that Hall's construction makes it "extremely difficult to quantify $m(K)$ in terms of the discriminant ... much less to obtain such a result with $m(K)$ a power of the discriminant." They give an upper bound for cubic fields which is asymptotically the same as Mordell's bound, but with weaker constants, $m(K)<3^6|D_K|^{1/4}$.

The goal of this chapter is to quantify $m(K)$ in terms of the discriminant for an infinite family of pure cubic fields. The proof relies on effective Diophantine approximation. By the Thue-Siegel-Roth theorem, for an algebraic, irrational number θ, and any real $2<\mu<3$, there is a constant $c=c(\theta,\mu)$ such that

$$\left|\theta-\frac{x}{y}\right|>\frac{c}{y^{\mu}}$$

for every pair of integers (x,y). If c is effectively computable, then the exponent μ is known as an *effective irrationality measure*. Taking $\theta=\sqrt[3]{\frac{a}{b}}$, this implies that $ax^3-by^3=i$ cannot have integral solutions when i is small relative to a and b. Hence $m(K)$ can be quantified in terms of the discriminant of K, which is a constant multiple of $(ab)^2$.

2.2 Preliminaries

We will prove Theorem 1.2 in two parts:

Theorem 2.1. *Let $a < b$ be squarefree, coprime integers such that $a > 125 \cdot 10^{120}$, $b - a < \frac{3}{2}a^{1/4}$, and $3||b-a$. Then $K = \mathbb{Q}\left(\sqrt[3]{ab^2}\right)$ has $m(K) = b - a$.*

Note that we are restricting to only the wildly ramified case. This is not a necessary restriction, it is only done to simplify the calculations involving index forms. We could apply the same ideas to families with $a \not\equiv b \pmod 3$, either directly if they are wildly ramified, or by correcting the index forms and discriminants with multiples of 9 if they are tamely ramified.

Corollary 2.2. *There are infinitely many pure cubic fields K with $m(K) \gg |D_K|^{1/16}$.*

By taking $b - a$ as large as possible, we will have $m(K) \gg a^{1/4}$, and $D_K = -27(ab)^2 \ll a^4$. So to prove the corollary, we only need to establish that there are infinitely many a, b satisfying Theorem 2.1, such that $b - a \gg a^{1/4}$.

Lemma 2.3 ([59])**.** *If a, b are squarefree, coprime integers with $3||b-a$, then $K = \mathbb{Q}(\sqrt[3]{ab^2})$ is a pure cubic field of Dedekind Type I (wild ramification), and has index form $I(x, y) = ax^3 - by^3$.*

Proof. Since $3||b - a$, then $3 \nmid a$ and $b = a + 3k$ for some $3 \nmid k$. Then $b^2 \equiv a^2 + 2ak \not\equiv a^2 \pmod 9$, so it is Type I. In this case, $D_K = -27(ab)^2$, and the algebraic integers

$$\{1, \sqrt[3]{ab^2}, \sqrt[3]{a^2b}\}$$

form an integral basis, which gives the index form $I(x, y) = ax^3 - by^3$. ∎

Write $\theta = \sqrt[3]{\frac{b}{a}}$, so that θ is the real root of the polynomial $I(x, 1)$. We will need some estimates on a and b to determine an effective irrationality measure of θ, so we prove them here.

Lemma 2.4. *If $0 < a < b < 2a$ are integers, then*

$$\frac{(b-a)^2}{6a} < \left(\sqrt{b} - \sqrt{a}\right)^2 < \frac{(b-a)^2}{4a}$$

Proof. Note that $\left(\sqrt{b}-\sqrt{a}\right)^2 = (b-a)^2/\left(\sqrt{b}+\sqrt{a}\right)^2$, and since $b-a>0$,

$$\left(\sqrt{b}+\sqrt{a}\right)^2 = a+b+2\sqrt{ab} > 4a.$$

Then using $b<2a$, we have $a+b+2\sqrt{ab} < (3+2\sqrt{2})a < 6a$. ■

The following constants g, Q, E and κ are used in Voutier's theorem [108].

Lemma 2.5. *For positive integers $0<b-a<a$, and any real number g with $1>g>\pi\sqrt{3}/6 = 0.9068\ldots$, define*

$$Q = \frac{1}{3}e^g\left(\sqrt{b}+\sqrt{a}\right)^2, \quad E = 3e^{-g}\left(\sqrt{b}-\sqrt{a}\right)^{-2}, \quad \kappa = \frac{\log Q}{\log E}.$$

If $b-a<\frac{3}{2}a^{1/4}$, then $E>1$ and $\kappa<2$.

Proof. By Lemma 2.4, we have

$$\left(\sqrt{b}-\sqrt{a}\right)^{-2} > \frac{4a}{(b-a)^2} > \frac{16}{9}\sqrt{a} > 1,$$

so $E>\frac{3}{e}>1$. For any $g<1$, we have $(b-a)^4 < 108e^{-3g}a$, since $(\frac{3}{2})^4e^3<108$.

Next, we show that $Q<E^2$, and thus $\kappa<2$:

$$\begin{aligned}\frac{E^2}{Q} &= 27e^{-3g}\left(\sqrt{b}-\sqrt{a}\right)^{-4}\left(\sqrt{b}+\sqrt{a}\right)^{-2}\\ &= 27e^{-3g}\left(\sqrt{b}-\sqrt{a}\right)^{-2}(b-a)^{-2}\\ &> 108e^{-3g}a\,(b-a)^{-4}\\ &> 1,\end{aligned}$$

again using Lemma 2.4 and $(b-a)^4<108e^{-3g}a$. ■

2.3 Effective Irrationality Measures

In order to bound the index form $I(x,y) = ax^3-by^3 = a(x^3-\theta^3y^3)$ away from 0, we need to bound $|x/y-\theta|$ away from 0, thus we seek Diophantine approximations to θ. That is, we

want to find an effective irrationality measure μ and a constant $c(a,b,\mu))$ such that for every rational x/y, we have $|x/y-\theta| > \frac{1}{c(a,b,\mu)y^\mu}$.

See [7] for a historic survey on this topic. There are three known methods to derive such measures: Baker's method, Chudnovsky's method, and Bombieri's method. The first effective measures were give by Alan Baker [2] by bounding linear forms in logarithms. This has the widest applicability, but generally gives the weakest values of μ and c. By restricting to families of algebraic numbers $\sqrt[n]{\frac{b}{a}}$ for positive integers $n \geq 3$, Gregory Chudnovsky [13] and Enrico Bombieri and Julia Mueller [8] discovered alternative methods. Chudnovsky used Padé (that is, ratios of polynomials) approximations to $(1+\frac{b-a}{a})^{1/n}$, and analysed the resulting rational functions and hypergeometric remainders. This generally gives better values of c, while Bombieri and Mueller's method generally gives better values of μ. All of the authors above are interested in irrationality measures where μ is as small as possible. The large values of constants that arise can be reduced computationally by searching over all possible convergents. This works well with fixed a and b, but we need to apply the estimates to increasing values of a and b, such that $c \ll a$. We also only require $\mu = 1+\kappa \leq 3$, not necessarily the minimal value possible. Thus we rely on theorems using Chudnovsky's method, and are limited to approximations to $\sqrt[3]{\frac{b}{a}}$ with $\frac{b}{a}$ close to 1. Note that $b-a = I(-1,1)$ is the index of $\sqrt[3]{a^2b} - \sqrt[3]{ab^2}$, so we would like $b-a$ to be as large as possible, but it must be small to apply effective approximation theorems. This is the limiting factor to improving the exponent in Theorem 1.2.

The current best approximations to $\sqrt[3]{\frac{b}{a}}$ are by Paul Voutier [108], which uses results from Jian Hua Chen and Voutier [12]. It improves upon the approximations by Mike Bennett [5] and David Easton [22], which were not strong enough for our arguments. We recall Voutier's main theorem and some relevant remarks:

Theorem 2.6. *[108, Theorem 2.1] For a,b,E,Q, and κ as in Lemma 2.5, $g = 0.911$, and $c_1 = 10^{40(\kappa+1)}a$, if $E > 1$, then for all integers x, y, with $y \neq 0$,*

$$\left|\theta - \frac{x}{y}\right| > \frac{1}{c_1|y|^{\kappa+1}}.$$

We will modify the above theorem with results from the same paper [108, Sections 6 and 7] and from Chen and Voutier [12, Lemma 2.8]. They define a sequence of rational approximants

p_r/q_r to θ in terms of hypergeometric functions:

Lemma 2.7. *[108, Lemma 5.5] With a, b and θ as above, and $\frac{p_r}{q_r}$ a sequence of good rational approximations to θ via the hypergeometric method, we have*

$$\left|\theta - \frac{p_r}{q_r}\right| > \frac{a}{200bq_r^2}.$$

Whereas for integers which are not from the sequence of good approximations, we have the following:

Theorem 2.8. *[108, Lemma 6.1] Let a, b, κ, E, Q be as in Lemma 2.5 with $g = 0.911$. Let $\ell_0 = \frac{1.176\cdot 10^{40}(b-a)}{a}$. Then for any integers x, y such that $\frac{x}{y} \neq \frac{p_i}{q_i}$ for any i, and $|y| \geq \frac{1}{2\ell_0}$, we have*

$$\left|\theta - \frac{x}{y}\right| > \frac{1}{c|y|^{\kappa+1}},$$

where

$$c = 3.22 \cdot 10^{39} \cdot (2\ell_0 E)^{\kappa}.$$

By using the estimates in Lemmata 2.5 and 2.4, if $a^{\frac{1}{4}} < b - a < \frac{3}{2}a^{\frac{1}{4}}$ then

$$2\ell_0 E < 1.176 \cdot 10^{40} \cdot \frac{36e^g}{b-a},$$

so $\kappa < 2$ and $c < 93.4 \cdot 10^{40(\kappa+1)}(b-a)^{-\kappa}$.

2.4 The Minimal Index

Choose a and b squarefree and coprime, such that $a > 125\cdot 10^{120}$, $3||b-a$, and $0 < b-a < \frac{3}{2}a^{1/4}$. We proceed as in Davenport [16], separating "large" values of y from "small" values of y, and finding a lower bound of at least $b-a$ for $|I(x,y)|$ in each case. Note that $|I(x,0)| \geq a$ for any $x \neq 0$, so we can assume $y \neq 0$, and by changing signs of both x and y, we can assume that y is positive. When $y = x$, we have $|I(y,y)| = (b-a)y^3$, which has non-zero minimum $b-a$, so further assume $x \neq y$.

Proposition 2.9. *If $y = q_i$ is a denominator of a good approximant for some i, then*

$|I(x,y)| \geq \dfrac{3a}{1600}$.

Proof. Write $I(x,y) = a(x-\theta y)(x^2+\theta xy+\theta^2y^2)$. Then

$$x^2+\theta xy+\theta^2y^2 = (x+\frac{\theta}{2}y)^2+\frac{3}{4}\theta^2y^2 \geq \frac{3}{4}\theta^2y^2,$$

So $|I(x,y)| \geq \frac{3}{4}a\theta^2y^3|\theta - x/y|$. Then by Lemma 2.7, we have

$$|I(x,y)| > \frac{3}{4}a\theta^2y^3\frac{a}{200by^2}.$$

Then since $b < 2a$ and $\theta > 1$, we have $|I(x,y)| \geq \frac{3a}{1600}$. ■

Proposition 2.10. *If* $\dfrac{x}{y} \neq \dfrac{p_i}{q_i}$ *and* $y \leq \dfrac{1}{2\ell_0}$, *then* $I(x,y) \geq \dfrac{1}{2}a$.

Proof. Since we are assuming $x \neq y$,

$$\begin{aligned}|x^3-y^3| &= |x-y||x^2+xy+y^2| \\ &\geq |x^2+xy+y^2| \\ &\geq \frac{3}{4}y^2.\end{aligned}$$

We have $\ell_0 = \frac{1.176\cdot 10^{40}(b-a)}{a}$, so

$$\begin{aligned}|I(x,y)| &= |a(x^3-y^3)-(b-a)y^3| \\ &\geq \frac{3a}{4}y^2-(b-a)y^3 \\ &\geq \frac{3a}{4}-(b-a)y \\ &\geq \frac{3a}{4}-\frac{a}{2.352\cdot 10^{40}} \\ &\geq \frac{1}{2}a.\end{aligned}$$

■

Proposition 2.11. *If* $\dfrac{x}{y} \neq \dfrac{p_i}{q_i}$ *and* $y > \dfrac{1}{2\ell_0}$, *then* $I(x,y) \geq \dfrac{a(b-a)}{125\cdot 10^{120}}$.

Proof. By Theorem 2.8, we have $\left|\theta - \frac{x}{y}\right| > \frac{1}{cy^{\kappa+1}}$. Thus

$$\begin{aligned} |I(x,y)| &\geq \frac{3}{4}a\theta^2 y^3 \left|\theta - \frac{x}{y}\right| \\ &> \frac{3}{4}a\theta^2 y^3 \frac{1}{cy^{\kappa+1}}. \end{aligned}$$

Since $1 < \kappa < 2$, $|I(x,y)| \geq \frac{a(b-a)}{125 \cdot 10^{120}}$. ■

In fact, we have shown that all elements in $\mathcal{O}_K$ have the index $\gg |D_K|^{\frac{1}{4}}$, except for $\alpha = z + y\sqrt[3]{a(a+b)^2} + y\sqrt[3]{a^2(a+b)}$ with $y, z \in \mathbb{Z}$, in which case the index is $(b-a)|y|^3$.

As a result, we have an infinite family of pure cubic fields which are not monogenic, since $3||b-a$. From those, we can find fields with large index relative to their discriminant.

Proof of Corollary 2.2. Suppose $a^{1/4} < b - a < \frac{3}{2}a^{\frac{1}{4}}$, and $a > 125 \cdot 10^{120}$. Then $K = \sqrt[3]{ab^2}$ has $m(K) > a^{\frac{1}{4}}$, and $|D_K| = 27(ab)^2 \ll a^4$ as long as a and b are squarefree and coprime, and $3||b-a$. Taking a to be prime will make them coprime, since $b < 2a$. To find infinitely many squarefree integers with $b - a$ in the correct range, we will use a theorem of Nair:

Theorem 2.12. *[83, Theorem B] For a quadratic polynomial $f(n) \in \mathbb{Z}[n]$, and positive real numbers x, h, let $N_2(f, x, h)$ denote the number of integers n such that $x < n < x + h$ and $f(n)$ is squarefree. Then*

$$N_2(f, x, h) = \Lambda_2(f)h + O(\frac{h}{\log h}),$$

where $\Lambda_2(f) = \prod_p (1 - \frac{\rho(p^2)}{p^2})$, and $\rho(p^2)$ counts the number of congruence classes of $n \pmod{p^2}$ such that $f(n) \equiv 0 \pmod{p^2}$.

Let $f(k) = 3n(a+3n)$, and $b = a + 3n$. For $x = \frac{1}{3}a^{1/4}$ and $h = \frac{1}{6}a^{1/4}$, we have $x < n < x + h \Leftrightarrow a^{1/4} < b - a < \frac{3}{2}a^{\frac{1}{4}}$. If $f(n)$ is squarefree, then $3 \nmid n$, so $3||b-a$, and b is squarefree. Then, provided $\Lambda_2(f) > 0$, we have $N_2(f, x, h) > 0$ for h large enough, hence infinitely many a, b satisfying the constraints. We have $\rho(9) = 3$, since a is prime and $a > 3$. Next, $\rho(a^2) = a$, since each multiple of a gives $f(n) \equiv 0 \pmod{a^2}$. For any other prime p, $\rho(p^2) = 2$, since the only possible common divisor of n and $a + 3n$ is a, we have $3n(a+3n) \equiv 0 \pmod{p^2} \Leftrightarrow n \equiv 0$

$(\mathrm{mod}\ p^2)$ or $a + 3n \equiv 0\ (\mathrm{mod}\ p^2)$. Hence

$$\Lambda_2(f) = \frac{2(a-1)}{3a} \prod_{p \neq 3,a} \left(1 - \frac{2}{p^2}\right) = 0.276543\ldots$$

when $a > 125 \cdot 10^{120}$, where the approximation is derived from the decimal expansion of the Feller-Tornier constant at the OEIS [97].

■

Chapter 3

Fields with Quadratic Subfields

3.1 Introduction

The index form $I(\vec{X})$ of a number field K of degree n containing subfields can often be factored as

$$I(\vec{X}) = F_1(\vec{X}) \cdots F_k(\vec{X}),$$

where k or $k-1$ is the number of maximal proper subfields of K (that is, proper subfields not contained in any other proper subfield), $\vec{X} = (X_1, \ldots, x_n)$, and each $F_i \in \mathbb{Z}[\vec{X}]$. This technique has not been established in general, but is known for many families of fields, and verified for every field where the index form has been computed. In this chapter, we focus on three families of fields containing a quadratic subfield: the two Galois quartic fields, and the compositums of totally real fields with imaginary quadratic fields. In each case, the index form has been explicitly factored. The chosen fields have factors that are binary quadratic forms, or norm forms of a subfield over $\mathbb{Q}$. When a factor is a binary quadratic form, we use the minimum of positive definite forms, or appeal to results on minima of indefinite binary quadratic forms to find examples with large minimal index. When a factor is a norm, we use results that give lower bounds on norms of any integral elements outside of an exceptional set. These two approaches provide families of fields with minimal index bounded below by some power of the discriminant. The factored index form also simplifies the search for elements of small index, so we can make improvements on upper bounds for the minimal index in terms of the discriminant.

3.1.1 Quartic Fields Background

Let K be a degree 4 extension of $\mathbb{Q}$, with Galois closure $\tilde{K}$. Then $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ is one of the 5 transitive subgroups of S_4: S_4, A_4, D_4, C_4, or V_4. For the first two, S_4 and A_4, K has no proper subfield, so by a result of Thunder and Wolfskill [106, Cor. 2], the fields satisfy $m(K) < 2^{24}|D_K|^{\frac{1}{2}}$. In the dihedral case, D_4, they [106, Cor. 1] give the upper bound $m(K) < 2^{30}|D_K|$, and show that the pure quartic fields $\mathbb{Q}(\sqrt[4]{2p^2})$, where p is a rational prime, are dihedral and satisfy $m(K) \gg |D_K|$. The remaining cases are called cyclic, denoted C_4, and biquadratic (or sometimes bicyclic biquadratic), denoted V_4. Luise-Charlotte Kappe and Bette Warren [67] showed that the index form is reducible over $\mathbb{Q}$ precisely when K has a quadratic subfield, that is D_4, C_4 and V_4. These factorizations allow us to use known minima of lower degree forms, sometimes with fewer variables, and apply those bounds to $m(K)$.

This chapter considers these last two cases, where improvements can be made bounding the minimal index in terms of the discriminant, and finding families which asymptotically achieve that bound. Each of these Galois groups is abelian, hence $K \subset \mathbb{Q}(\zeta_n)$, a cyclotomic field, for some $n \in \mathbb{Z}^+$. The least such n where this holds is called the *conductor* of K. The known upper bound on the minimal index from on a quartic field K with a quadratic subfield is $m(K) \ll |D_K|^{\frac{n-2}{2}}$ [106].

3.1.2 Historical Development of V_4 Fields

Any V_4 field can be written as $\mathbb{Q}(\sqrt{ac}, \sqrt{bc})$ for integers a, b, c with $a, b > 0$ and abc squarefree. Integral bases were computed by Williams [109] and Motoda [78]. When $c > 0$, the field is totally real, and otherwise is imaginary. Nakahara [86] showed that infinitely many V_4 fields are monogenic by explicit construction of a family in our case 5; that infinitely many have $i(K) = 2$, which occurs when D_K is odd; and that $m(K)$ is unbounded in both real and imaginary fields. He computed the index form using Motoda's integral basis [78]. In the real case, the proof of unboundedness uses Hall's argument, replacing cubic non-residues with quadratic non-residues. The imaginary case is the same as our argument, and implicitly gives a lower bound for the minimal index in terms of the discriminant.

Gaál, Pethö and Pohst [34] showed that each possible field index $i(K)$ given by Engstrom

for biquadratic fields (that is, $1, 2, 3, 4, 6, 12$) occurs infinitely, using Williams's integral basis and considering possible congruence classes mod 48. They give a simple method for identifying the field index depending only on congruence conditions.

M.-N. Gras and Tanoé [53] gave necessary and sufficient conditions for a biquadratic field to be monogenic: it must satisfy a linear equation in a, b, c, and a given binary quartic Thue equation must have integral solutions. They factor the index form, and configure the factors into a Thue equation which represents ± 1 if and only if each factor does.

Jadrijević [65, 66] constructed three infinite, one-parameter families of biquadratic fields having absolutely bounded minimal index, and computed the minimal index for each. The elements of minimal index are found by factoring the index form, and are proven minimal by considering continued fractions of quadratic irrationals. The fields are given by: $a = c - 2$, $b = c + 2$ with $c \geq 3$, odd - then $m(K) = 4$; $a = c - 2$, $b = c + 4$, with $c \geq 7$, $c \equiv 1, 3 \pmod 6$ - then $m(K) = 12$; and $a = c - 1, b = 4c + 1$ with $c \geq 3$ then $m(K) = 5$ if $c = 3$, otherwise it is 40 if c is odd, and 80 if c is even.

3.1.3 Historical Development of C_4 Fields

Cyclic quartic fields were uniquely parametrized by three integers A, B, C by Hardy, Holtz, Hudson, Richman and Williams [60]. If A is odd and squarefree, $B, C > 0$, $D = B^2 + C^2$ is squarefree, and A and D are coprime, then the field $\mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right)$ is a cyclic quartic field, and every cyclic quartic field can be written uniquely in this form. Two of the authors [64] gave an integral basis and computed the discriminant for these fields. This allowed Spearman and Williams [99] to compute the index form $I(x, y, z)$ and field index $i(K)$. They showed that each possible field index given by Engstrom [24] for cyclic quartic fields (that is, $1, 2, 3, 4, 6, 12$) occurs infinitely often, and gave necessary and sufficient congruence conditions on A, B, C to determine $i(K)$. Further, they computed the proportion of cyclic quartic fields having each field index when ordered by discriminant.

Nakahara [87] showed that the minimal index is unbounded for cyclic fields with field index $i(K) = 1$, and later [88] that if the conductor is a prime of a certain form (either 1 mod 8, or $(3 + 12n)^2 + 4$, $n \in \mathbb{Z}^+$), then K is not monogenic. The conductor, in the parametrization below, is $2^{\lambda/2}AD$, hence these must have $A = \pm 1$, $\lambda = 0$, D prime with either: B a multiple

of 4, or $B = 2$, $A = -1$, and $C = 3 + 12n$. Note that in the latter case, since D is prime, it is a sum of two squares uniquely, so B is determined, but it is not known if there are infinitely many primes of this form.

Gaál and Petrányi [37] computed the minimal index of the simplest cyclic quartic fields, generated by a root of $x^4 - tx^3 - 6x^2 + tx + 1 = 0$, provided $t > 3$ and $t^2 + 16$ has no odd square factors. They all have $m(K) \leq 16$. The condition on $t^2 + 16$ allows them to use an integral basis from Lee [73], where the generator of the field has index 2^k for some $k \leq 4$. This does not extend to the parameters t where $t^2 + 16$ has odd square factors, and it is not known if the simplest quartics have unbounded minimal index.

3.1.4 Historical Development of Composite Fields

Very few results on the minimal index are known for composite fields. An integral basis for $\mathcal{O}_K$ is known immediately from integral bases of $\mathcal{O}_L$, $\mathcal{O}_M$ [90]. They are seldom monogenic, and the possible field indices $i(K)$ depend on the degree and have not been broadly categorized, so the research groups interested in finding integral bases, resolving Hasse's problem, or determining the proportion of fields with each field index do not usually study them. Nakahara and Sultan [104] determined all monogenic fields $K = LM$ with M a cyclic quartic field with prime conductor and L a quadratic field with $(\pm)$ prime discriminant. Gaál's group used the reduction to norm forms to give examples of non-monogenic sextic fields [30] (with Olajos and Pohst), and non-monogenic nonic fields, given as composites of two cubic fields [27]. Gaál and Remete [38] showed that the imaginary quadratic extensions $M(\sqrt{-n})$ of Shanks' simplest cubic fields M (generated by a root of $x^3 - ax^2 - (a+3)x - 1 = 0$ with $a^2 + 3a + 9$ squarefree) are only monogenic when $n = 1$ and $a = 0, -1, -2$, or -3.

The composite fields we will discuss are distinct from the examples used by Thunder and Wolfskill [106] to achieve the largest minimal index possible for degree $2m$ fields: our fields are $M(\sqrt{-n})$ for a rational integer $n > 0$, while theirs are $M(\sqrt{-p\alpha})$, where p is a rational prime and $\alpha \in \mathcal{O}_M \setminus \mathbb{Z}$. Our parameterized families have $m(K) \asymp_M |D_K|^{\frac{m-1}{2}}$, while theirs have $m(K) \asymp |D_K|^{m-1}$.

3.2 Minimal Index of V_4 Fields

Let a, b, c be squarefree, coprime integers, and let $K = \mathbb{Q}(\sqrt{ac}, \sqrt{bc})$. Then K is a V_4 field, with subfields $\mathbb{Q}(\sqrt{ac})$, $\mathbb{Q}(\sqrt{bc})$ and $\mathbb{Q}(\sqrt{ab})$. Let $\mathrm{Gal}(K/\mathbb{Q})$ be generated by $\{\sigma, \tau\}$, and for $\alpha \in \mathcal{P}$, arrange the conjugates $\alpha^{(i)}$ such that $\alpha = \alpha^{(1)}$, $\alpha^{(2)} = \sigma\alpha^{(1)}$, $\alpha^{(3)} = \tau\alpha^{(1)}$ and $\alpha^{(4)} = \sigma\alpha^{(3)}$. Then the discriminant of α contains the terms $(\alpha^{(1)} - \alpha^{(2)})^2(\alpha^{(3)} - \alpha^{(4)})^2$, which is fixed by both σ and τ, hence is a rational integer. There are two more pairs of products which give rational integers, and the resulting factorization of the discriminant extends to a factorization of the index form. This technique was also applied to S_3 sextic fields, the Galois closure of pure cubic fields [11], $C_2 \times C_2 \times C_2$ octic fields [77], and D_4 octic fields that are the Galois closure of pure quartic fields [40]. In each of these, it was only used to determine which of the fields were monogenic, and the explicit index form was not always necessary.

In all cases where the index form has been computed, it factors into a product of integral forms with a distinct factor for each maximal proper subfield, and possibly one additional factor. Where the index form has not been computed, the factorization has been proven for the Galois fields listed above, and for composites of fields with coprime discriminants, but not for number fields in general. In the Galois case, the differences of conjugates in the discriminant decompose into distinct products for each maximal proper subfield, so the difficulty arises in showing that each form with rational coefficients actually has integer coefficients. In the non-Galois case, there may not be field automorphisms which fix a subfield, so the discriminant does not have a natural decomposition. We conjecture that such a factorization always exists - such a program will extend these results to many other fields containing subfields.

The index forms of V_4 fields factor into three binary quadratic forms, since each field has three maximal proper subfields. They are computed in [34] (cf. [28, §6.5]), and are of the form $I(X_2, X_3, X_4) = r(bx^2 - az^2)(cz^2 - by^2)(cx^2 - ay^2)$, where

Case	$ac \pmod 4$	$bc \pmod 4$	$a, b \pmod 4$	x	y	z	r	D_K
1	1	1	1, 1	$X_3 + \frac{X_4}{2}$	$\frac{X_4}{2}$	$X_2 + \frac{X_4}{2}$	1	$(abc)^2$
2	1	1	3, 3	$X_3 + \frac{X_4}{2}$	$\frac{X_4}{2}$	$X_2 - \frac{X_4}{2}$	1	$(abc)^2$
3	1	2	any	$X_3 + \frac{X_4}{2}$	$\frac{X_4}{2}$	$\frac{X_2}{2}$	16	$(4abc)^2$
4	2	3	any	X_3	$\frac{X_4}{2}$	$X_2 + \frac{X_4}{2}$	8	$(8abc)^2$
5	3	3	any	$\frac{X_3}{2}$	$\frac{X_4}{2}$	$X_2 + \frac{X_3}{2}$	16	$(4abc)^2$

We have fixed two typos from [28]: c and z of case 4. The integral bases and discriminants for the computations were done by Williams in [109], but they only become a product of diagonal forms after changing to an alternative basis. We use this factorization to show

Theorem 3.1. *(a) If K is a biquadratic quartic field, then $m(K) \ll |D_K|^{\frac{1}{2}}$.*

(b) Fix square-free integers $a, b < 0$, with $(a, b) = 1$. As c varies over all positive, square-free integers with $(ab, c) = 1$, then $K = \mathbb{Q}\left(\sqrt{ac}, \sqrt{bc}\right)$ has $D_K \asymp_{a,b} c^2$ and $m(K) \gg |D_K|^{\frac{1}{2}}$.

Note that when two of x, y, z are equal to 1 and the other is 0, then we have

$$|I| \leq 32 \min\{|a|, |b|, |c|\}^2 \max\{|a|, |b|, |c|\}.$$

These values are possible with appropriate choices of X_2, X_3 and X_4 from $\{-1, 0, 1, 2\}$:

Case	$\min\{\lvert a\rvert, \lvert b\rvert, \lvert c\rvert\}$	X_2	X_3	X_4	x	y	z	$\lvert I(X_2, X_3, X_4)\rvert$
1	$\lvert a\rvert$	0	-1	2	0	1	1	$a^2\lvert b-c\rvert$
	$\lvert b\rvert$	-1	0	2	1	1	0	$b^2\lvert a-c\rvert$
	$\lvert c\rvert$	1	1	0	1	0	1	$c^2\lvert a-b\rvert$
2	$\lvert a\rvert$	2	-1	2	0	1	1	$a^2\lvert b-c\rvert$
	$\lvert b\rvert$	1	0	2	1	1	0	$b^2\lvert a-c\rvert$
	$\lvert c\rvert$	1	1	0	1	0	1	$c^2\lvert a-b\rvert$
3	$\lvert a\rvert$	2	-1	2	0	1	1	$16a^2\lvert b-c\rvert$
	$\lvert b\rvert$	0	0	2	1	1	0	$16b^2\lvert a-c\rvert$
	$\lvert c\rvert$	2	1	0	1	0	1	$16c^2\lvert a-b\rvert$
4	$\lvert a\rvert$	0	0	2	0	1	1	$8a^2\lvert b-c\rvert$
	$\lvert b\rvert$	-1	1	2	1	1	0	$8b^2\lvert a-c\rvert$
	$\lvert c\rvert$	1	1	0	1	0	1	$8c^2\lvert a-b\rvert$
5	$\lvert a\rvert$	1	0	2	0	1	1	$16a^2\lvert b-c\rvert$
	$\lvert b\rvert$	-1	2	2	1	1	0	$16b^2\lvert a-c\rvert$
	$\lvert c\rvert$	0	2	0	1	0	1	$16c^2\lvert a-b\rvert$

Hence $I(X_2, X_3, X_4) \ll abc \ll |D_K|^{\frac{1}{2}}$, which proves Theorem 1.4.

To establish a family which achieve the largest possible minimal index, we fix two coprime integers and vary c. Suppose that both a and b are negative, so that the forms $cx^2 - ay^2$ and $cz^2 - by^2$ are positive definite. Then $(cx^2 - ay^2)(cz^2 - by^2) \geq c$, unless $x = z = 0$, but in that case, $az^2 - bx^2 = 0$, and the element does not generate K. Hence, for fixed square-free, coprime $a, b < 0$, as we let c vary over positive integers with $(ab, c) = 1$, the field $K = \mathbb{Q}\left(\sqrt{ac}, \sqrt{bc}\right)$ has $D_K \asymp_{a,b} c^2$, while $m(K) \gg c \asymp_{a,b} |D_K|^{\frac{1}{2}}$, proving Theorem 1.3. This result first appears in [86] to show that the minimal index of imaginary V_4 fields is unbounded. The corresponding argument for real V_4 fields follows Hall's construction, and like in the cubic case, it does not give a bound in terms of D_K. The Diophantine approximation techniques from chapter 2 do not translate to quadratic forms, since

$$\left|\frac{x}{y} - \sqrt{\frac{a}{c}}\right| < \frac{\sqrt{5}}{y^2}$$

has infinitely many solutions. A related technique, simultaneous Diophantine approximation, gives effective lower bounds on products of the form

$$\left|\frac{x}{y} - \sqrt{\frac{a}{c}}\right| \left|\frac{z}{y} - \sqrt{\frac{b}{c}}\right|,$$

or lower bounds on the larger of the two factors. These approximations would apply to the search for fields with large minimal index. Unfortunately, the current best effective approximations are not strong enough to give lower bounds in terms of the field discriminant. This gives another avenue for improvements to be made in V_4 fields in future work.

3.2.1 Reduced indefinite binary quadratic forms

The family constructed for Theorem 1.3 is somewhat unsatisfactory - one expects that for many pairs $0 < b < a$, the quadratic form $az^2 - bx^2$ will have absolute minimum b, and so there should be many families with $I \asymp \min\{|a|, |b|, |c|\}^2 \max\{|a|, |b|, |c|\}$. Establishing their existence is challenging in practice.

A binary quadratic form $f(x, y) = Ax^2 + Bxy + Cy^2$ is *indefinite* if the discriminant $D = B^2 - 4AC > 0$. The group $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{-I\}$ of 2×2 matrices with determinant 1, modulo the equivalence $[\gamma] = [-\gamma] \in PSL_2(\mathbb{Z})$, acts on these forms by $\gamma \circ f = f(\gamma(x, y))$, preserving their discriminant and the integers they represent. An indefinite form is called reduced [9, 14, 15] if $\left|\sqrt{D} - 2|a|\right| < B < \sqrt{D}$. Note that this means none of the diagonal forms $az^2 - bx^2$ are reduced. There are many concepts of "reduction" for indefinite forms, going back to Gauss [45, Book IV], with authors using a definition to suits their goals - we will use this one. Every indefinite form is equivalent to a finite number of reduced forms, and the minimum of $|f(x, y)|$, $x, y \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, is the minimum of $|(\gamma \circ f)(1, 0)|$ over all reduced forms $\gamma \circ f$. For a given form f, it is simple to determine all reduced forms, and hence the nonzero minimum of $|f(x, y)|$. The difficulty in finding families with large minima comes from the dependence of the reduction algorithm on the explicit values A, B, C, so that reducing a parameterized family of forms only has predictable results if the parameters behave well with respect to reduction. We will restrict to families where the reduction follows the same steps for each member.

Theorem 3.2. *Let $a = F_{2n}F_{2n+3}$ and $b = F_{2n-1}F_{2n+2}$, where F_n denotes the n^{th} Fibonacci number. Then $(a, b) = 1$, and the quadratic forms $F_n(x, y) = ax^2 - by^2$ have a minimal non-zero value $2F_{2n}F_{2n-1}$.*

It is not known if infinitely many Fibonacci numbers are squarefree, let alone a product of four of them, so this theorem cannot currently be applied to construct V_4 fields with large minimal index. If they are both squarefree, then with $c = 1$, $K = (\sqrt{a}, \sqrt{b})$ has $D_K \asymp (ab)^2 \asymp \phi^{16n}$, and $m(K) \asymp \phi^{4n} \gg |D_K|^{\frac{1}{4}}$, where $\phi = \frac{1+\sqrt{5}}{2}$.

Following the algorithm in [15], we can determine all reduced quadratic forms equivalent to $F(x, y) = ax^2 - by^2$ by computing a finite number of primitive values v_i, starting with $F(1, 0), F(0, 1)$ and $F(1, 1)$. Subsequent values depend on the positions of the previous positive and negative values. The sequence of values is cyclic, and the minimum value of $|F(x, y)|$ is the absolute minimum among these primitive values. Suppose that $a > b$. Starting with $v_0 = a$, $v_1 = -b$, and $v_2 = a - b > 0$, we find that $v_3 = a - 4b$. If the values always alternate in sign, then $v_i = 2(v_{i-1} + v_{i-2}) - v_{i-3}$. This recurrence is satisfied by $v_i = aF_{i-1}^2 - bF_i^2$, where F_i is the i^{th} Fibonacci number, since $2(F_i^2 + F_{i-1}^2) = F_{i+1}^2 + F_{i-2}^2$ [4, Id. 30]. If we choose a and b such that $v_{2n+1} = v_{2n+2}$, then the primitive values form a cycle of length $4n + 3$, with $v_i = v_{4n+3-i}$. Thus

$$a(F_{2n+1}^2 - F_{2n}^2) = b(F_{2n+2}^2 - F_{2n+1}^2)$$

If a and b are to be coprime, then we must have $a = F_{2n}F_{2n+3}$ and $b = F_{2n-1}F_{2n+2}$. To see that they are coprime, note that $(F_i, F_i + 1) = (F_i, F_{i+2}) = 1$ for every i, so

$$(F_{2n}F_{2n+3}, F_{2n-1}F_{2n+2}) = (F_{2n+3}, F_{2n-1}) = (3F_{2n} + 2F_{2n-1}, F_{2n-1}) = (3, F_{2n-1}),$$

and $3|F_i$ iff $4|i$, thus $(a, b) = 1$.

The minimal value of this form is $v_{2n} = 2F_{2n}F_{2n-1}$, which we show with the following three lemmas.

Lemma 3.3. *The primitive values $v_0, \ldots, v_{2n+1}$ alternate in sign, with $v_{2i} > 0$ and $v_{2i+1} < 0$.*

Proof. Using d'Ocagne's identity, $F_kF_{m+1} = F_{k+1}F_m + (-1)^m F_{k-m}$, twice on $F_{2n}F_{2n+3}F_{i-1}^2$,

with $k = i - 1$ and $m = 2n + 2$, $2n - 1$, we have

$$v_i = F_{2n-1}F_iF_{i-2n-3} - F_{2n+2}F_iF_{i-2n-2} + F_{2n+3-i}F_{2n+2-i}.$$

When i is even, all three terms are positive, so $v_i > 0$. When i is odd,

$$v_i < -F_{2n-1}F_iF_{i-2n-3} + F_{2n+3-i}F_{2n+2-i} \leq 0.$$

■

Lemma 3.4. *For every i and n, we have*

$$v_{2n} = 2F_{2n}F_{2n-1} \leq F_{2n-1}F_{2n+2}F_{2i+1}^2 - F_{2n}F_{2n+3}F_{2i}^2 = |v_{2i+1}|.$$

Proof. We fix i and proceed by induction on n. When $n = 0$, $|v_{2i+1}| = F_{2i+1}^2 > 0$. Denoting the difference Δ_n by $\Delta_0 = F_{2i+1}^2$ and

$$\Delta_n = F_{2n-1}F_{2n+2}F_{2i+1}^2 - F_{2n}F_{2n+3}F_{2i}^2 - 2F_{2n}F_{2n-1},$$

for $n > 0$, we claim that $\Delta_{n+1} = \Delta_n + F_{2i}F_{4n+3-2i} + F_{4n}$, which proves the lemma.

Using $F_{k+1}F_{m+1} - F_{k-1}F_{m-1} = F_{k+m}$ [4, Id. 231], we have

$$\Delta_{n+1} - \Delta_n = F_{2i+1}^2F_{4n+3} - F_{2i}^2F_{4n+5} - 2F_{4n+1} = F_{2i}F_{2i-1}F_{4n+3} - F_{2i}^2F_{4n+2} + F_{4n}$$

Using Cassini's identity $F_{2i+1}F_{2i-1} = F_{2i}^2 + 1$ and d'Ocagne's identity, we get

$$\Delta_{n+1} - \Delta_n = F_{2i}F_{2i-1-4n-2} + F_{4n}$$

Since $2i - 4n - 3$ is odd, and the negative odd index Fibonacci numbers are positive, this proves our claim. ■

Lemma 3.5. *For every $0 \leq i \leq n$, we have*

$$v_{2n} = 2F_{2n}F_{2n-1} \leq F_{2n+3}F_{2n}F_{2i-1}^2 - F_{2n+2}F_{2n-1}F_{2i}^2 = v_{2i}.$$

Proof. This is certainly true when $n = i$, so we fix i, and proceed by induction on n. Again, define

$$\Delta_n = F_{2n+3}F_{2n}F_{2i-1}^2 - F_{2n+2}F_{2n-1}F_{2i}^2 - 2F_{2n}F_{2n-1},$$

for $n > i$, and $\Delta_i = 0$. We claim that $\Delta_{n+1} = \Delta_n + F_{2i-1}F_{4n-2i+4} + F_{4n}$. The proof follows the same steps as the previous lemma. ■

More families can be constructed by adjusting the signs of the initial primitive values v_i, so that, for example, $v_0, \ldots, v_r$ are positive before they alternate in sign and are eventually equal at the midpoint of the cycle. These families arise from coefficients $a = G(n)H(n)$, $b = G(n-1)H(n-1)$, where G and H are linear combinations of Fibonacci and Lucas numbers. Their squarefree status is also unknown, and the proofs are similar to the above, but less tidy. We mention these with the expectation that the existence of squarefree numbers across many sparse families may be easier to solve than in one particular sparse family, but we do not hold out hope for such a result in the near future.

3.3 Minimal Index of C_4 Fields

In this section, we will use the parametrization and notation from Spearman and Williams [99], which gives an index form factored into a binary quadratic and a ternary quartic form. The index forms and discriminants are separated into 5 cases:

(i) D even

(ii) D odd, B odd

(iii) D odd, B even, $A + B \equiv 3 \bmod 4$

(iv) D odd, B even, $A + B \equiv 1 \bmod 4$, $A \equiv C \bmod 4$

(v) D odd, B even, $A + B \equiv 1 \bmod 4$, $A \equiv -C \bmod 4$

Using Maple, they compute and factor the index forms as

$$I(x,y,z) = kR(y,z)\left(DS(x,y,z)^2 - A^2R(y,z)^2\right),$$

where each term is in the following table. For reference, the discriminant $D_K = 2^\lambda A^2 D^3$, is also included, from [60].

Case	λ	k	$R(y,z)$	$S(x,y,z)$
(i)	8	1	$Cy^2 - 2Byz - Cz^2$	$2x^2 - A(y^2+z^2)$
(ii)	6	$\frac{1}{4}$	$2Cy^2 - 4Byz - 2Cz^2$	$x^2 - 2A(y^2+z^2)$
(iii)	4	$\frac{1}{2}$	$-By^2 + 2Cyz + Bz^2$	$x^2 - A(y^2+z^2)$
(iv)	0	$\frac{1}{32}$	$-By^2 + 2Cyz + Bz^2$	$4x^2 + (1-A)(y^2+z^2) + 4xy - 4xz - 2yz$
(v)	0	$\frac{1}{32}$	$By^2 + 2Cyz - Bz^2$	$4x^2 + (1-A)(y^2+z^2) + 4xy - 4xz - 2yz$

This allows us to improve the upper bounds of $m(K) \ll |D_K|$ from the general quartic results of Thunder and Wolfskill [106], for families of fields with A fixed.

Theorem 3.6. *If $K = \mathbb{Q}\left(\sqrt{A(D+B\sqrt{D})}\right)$ is a cyclic quartic field, with $D = B^2 + C^2$, $(A,D) = 1$ and both A, D squarefree, then $m(K) \leq 16A^2BC\min\{B,C\}$. For any family of fields with A fixed, the minimal index is $m(K) \ll |D_K|^{\frac{1}{2}}$.*

Proof. We construct elements with the desired index, where $B < C$ and $C < B$ are considered separately for each case.

Case	B, C	(x, y, z)	$R(y, z)$	$S(x, y, z)$	$I(x, y, z)$
(i)	$B < C$	$(0, 1, 0)$	C	$-A$	A^2B^2C
	$C < B$	$(0, 1, -1)$	$2B$	$-2A$	$8A^2BC^2$
(ii)	$B < C$	$(0, 1, 0)$	$2C$	$-2A$	$2A^2B^2C$
	$C < B$	$(0, 1, -1)$	$4B$	$-4A$	$16A^2BC^2$
(iii)	$B < C$	$(0, 1, 1)$	$2C$	$-2A$	$4A^2B^2C$
	$C < B$	$(0, 0, 1)$	B	$-A$	$\frac{1}{2}A^2BC^2$
(iv)	$B < C$	$(0, 1, 1)$	$2C$	$-2A$	$\frac{1}{4}A^2B^2C$
	$C < B$	$(1, 0, 2)$	$4B$	$-4A$	$2A^2BC^2$
(v)	$B < C$	$(0, 1, 1)$	$2C$	$-2A$	$\frac{1}{4}A^2B^2C$
	$C < B$	$(1, -2, 0)$	$4B$	$-4A$	$2A^2BC^2$

If A is fixed, then $D_K \gg D^3 = (B^2 + C^2)^3 \gg \max\{B, C\}^6$. All elements in the table satisfy $I(x, y, z) \ll \max\{B, C\}^3$, hence $m(K) \ll |D_K|^{\frac{1}{2}}$. ■

For families where A is not fixed, the upper bounds do not have a direct comparison to the discriminant. It is clear that $m(K) < |D_K|$, but any power-saving estimate will depend on A, B and C. By parametrizing each of them as functions of one variable, we construct infinitely many cyclic fields which asymptotically achieve this upper bound.

Note that the factor $DS^2 - A^2R^2$ is (in absolute value) the norm of an integral element in $\mathbb{Q}(\sqrt{D})$, $N(AR + S\sqrt{D})$. So we now turn to norms of integral elements in real quadratic fields. Davenport studied the family $\mathbb{Q}(\sqrt{t^2 + 1})$ while investigating the class number problem, and proved:

Lemma 3.7 (Davenport [1, 74])**.** *If n and t are natural numbers with $|X^2 - (t^2 + 1)Y^2| = n$ for integers X, Y, then $n \geq 2t$ or n is a perfect square.*

Let $\epsilon > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{D})$, and ξ an algebraic integer of norm n. Then there is a unit η such that $\xi\eta = a + b\sqrt{D}$, has both

$$|2a|, |2b\sqrt{D}| \leq \left(\sqrt{n\epsilon} + \sqrt{n\epsilon^{-1}}\right).$$

Applying this to $D = t^2 + 1$ with $\epsilon = t + \sqrt{t^2 + 1}$ and checking cases $|b| \leq 1$ gives the result.

Theorem 3.8. *Let $B = t > 0$ be a multiple of 4, $D = t^2 + 1$, and $A \equiv 3 \pmod 4$ an odd, squarefree integer in the range $[-2\sqrt{t}, -\sqrt{t}]$ with $(A, D) = 1$. Then $D_K \asymp t^7$, and $m(K) \asymp |D_K|^{\frac{2}{7}}$.*

Proof. When $4|B$ and $A \equiv 3 \bmod 4$, we are in case (iii) [99]. Let

$$\alpha = \sqrt{A(D + B\sqrt{D})}, \quad \beta = \sqrt{A(D - B\sqrt{D})}.$$

Then an integral basis is given by

$$\left\{1, \frac{1}{2}(1 + \sqrt{D}), \frac{1}{2}(\alpha + \beta), \frac{1}{2}(\alpha - \beta)\right\},$$

and the index form with respect to this basis, is

$$\begin{aligned} I(x, y, z) &= \frac{1}{2}R(DS^2 - A^2R^2), \quad \text{where} \\ R(y, z) &= -By^2 + 2Cyz + Bz^2 \quad \text{and} \\ S(x, y, z) &= x^2 - A(y^2 + z^2). \end{aligned}$$

Since $B = t > 0$ is a multiple of 4, R will always be even. Let $C = 1$, so $D = t^2 + 1$. Take $A \equiv 3 \pmod 4$ a squarefree, negative integer in the range $-2\sqrt{t} < A < -\sqrt{t}$, chosen so that $(A, D) = 1$. In Lemma 3.9, we show that, for infinitely many t, there is at least one A satisfying these requirements.

We need to show that for $\alpha \in \mathcal{P}$, the index $I(\alpha) \gg t^2$. The primitive elements cannot lie in $\mathbb{Q}(\sqrt{D})$, so y and z cannot both be zero. We have chosen $A < 0$ so that $S(x, y, z)$ is positive definite, and since at least one of y, z is non-zero, $S \geq |A|$.

Note that $|DS^2 - A^2R^2| = |N_{\mathbb{Q}(\sqrt{D})}(AR + S\sqrt{D})|$. To determine the minimal index, we consider possible values of R and this norm. We divide the cases between large and small values of R, and use the result of Davenport, Lemma 3.7. We will also use the size of units in $\mathbb{Q}\left(\sqrt{t^2 + 1}\right)$, generated by $\epsilon = t + \sqrt{t^2 + 1}$.

If $|R(y, z)| \leq \frac{t}{2}$, we have $R^2 < D/4$, so $|DS^2 - A^2R^2| > |A^2|\frac{3D}{4}$ since $S \geq |A|$. Hence, $I(x, y, z) \gg t^2$.

If $|R(y,z)| \geq t^2$, we have $|I| \geq \frac{1}{2}|R| \gg t^2$, so we are left to consider R in the range $t/2 \leq |R(y,z)| < t^2$.

Let $|DS^2 - A^2R^2| = n$. If $n \geq 2t$, then $|R(DS^2 - A^2R^2)| \geq t^2$. Hence $n < 2t$. Since $|DS^2 - A^2R^2| = |(AR)^2 - (t^2+1)S^2|$, by Davenport's lemma, n is a perfect square, and we can find some power η of ϵ, such that $(AR + S\sqrt{D})\eta = a + b\sqrt{D}$, where $b = 0$ and $n = a^2$, or $b = \pm 1$, $a = t$ and $n = 1$.

If $n = 1$, then $AR + S\sqrt{D}$ is a unit, and we have $|AR| = 2t^2 + 1$, since $\frac{1}{2}t^{3/2} < |AR| < 2t^{5/2}$. But R is even, so this is impossible.

When $(AR + S\sqrt{D})$ is not a unit, $(AR + S\sqrt{D})\eta = a < \sqrt{2t}$. Writing $\epsilon^k = u_k + v_k\sqrt{t^2+1}$, we have $|AR| = au_k$ and $S = av_k$ for some integer k. By the bounds on A, R and a, $\dfrac{t}{\sqrt{2}} < u_k < 2t^{5/2}$, so either $u_k = t$, or $u_k = 2t^2 + 1$, all other units having $|u_k| \gg t^3$.

If $|AR| = at$, then $S = a$. Writing $R(y,z) = -ty^2 + 2yz + tz^2$, we have $t|2Ayz$. So either $|yz| \geq \frac{t}{2A}$ or $yz = 0$. If $|yz| \geq \frac{t}{2A}$, we have $|A|(y^2+z^2) \geq 2|A|yz \geq t$, while $S = x^2 + |A|(y^2+z^2)$, which contradicts $a < \sqrt{2t}$. Thus $yz = 0$, $|R| \geq t$, $A|a$, and so $|I| \geq \frac{1}{2}ta^2 \gg t^2$.

If $|AR| = a(2t^2+1)$, then $S(x,y,z) = 2at$. Suppose a is the minimal positive integer that satisfies these equations for some x, y, z. Since $4|t$, and $S(x,y,z) \equiv x^2 + y^2 + z^2 \pmod 4$, each of x, y and z are even. Thus $4|R(y,z)$, so $4|a$, and we have $S(\frac{x}{2}, \frac{y}{2}, \frac{z}{2}) = 2\left(\frac{a}{4}\right)t$, and $|AR(\frac{y}{2}, \frac{z}{2})| = \frac{a}{4}(2t^2+1)$, contradicting the minimality of a.

Thus, we have that $I(x,y,z) \gg t^2$.

Since $A^2 \asymp t$, $B = t, C = 1$, by Theorem 1.5, $m(K) \ll t^2$. Hence $m(K) \asymp t^2$, proving Theorem 3.8. ∎

To prove Theorem 1.6, we need to establish that there are infinitely many values of t and A satisfying these conditions.

Lemma 3.9. *Let $B = t > 0$ be a multiple of 4, $D = t^2 + 1$, and $A \equiv 3 \pmod 4$ an odd, squarefree integer in the range $[-2\sqrt{t}, -\sqrt{t}]$ with $(A, D) = 1$. There are infinitely many such values of A and t.*

Proof. First, there are infinitely many $t = 4k > 0$ such that $16k^2 + 1$ is squarefree [82]. To each

of these, we associate the polynomial $f_t(n) = (t^2+1)(4n+1)$, and write

$$N_2(f_t, x, h) = \#\{n \mid x < n < x+h,\ f_t(n) \text{ is squarefree}\}.$$

Taking $x = h = \sqrt{t}$, and $A = -4n-1$, we have $F_t(n) = -AD$, so A and D are coprime and squarefree for each value of n counted by N_2. By [83, Theorem B],

$$N_2(f_t, x, h) = \Lambda_2(f_t)h + O(\frac{h}{\log h}),$$

where $\Lambda_2(f_t) = \prod_p(1 - \frac{\rho(p^2)}{p^2})$, and $\rho(p^2)$ counts the number of congruence classes of $n \pmod{p^2}$ such that $f_t(n) \equiv 0 \pmod{p^2}$. By our choice of t, we have $\rho(2^2) = 0$, $\rho(p^2) = p$ if $p|(t^2+1)$, and $\rho(p) = 1$ otherwise. Hence for every t large enough, we can find at least one A satisfying our requirements. ■

3.4 Minimal index of composite fields

Next, we give improved upper bounds for the compositum of an imaginary quadratic field L and a totally real field M with coprime discriminants. The index form factors into a product of three integral forms - two from the maximal proper subfields L, M, and one from the remaining discriminant factors. As a result of having coprime discriminants, the factors from L, M are each complete norms [28, §4.4.1], and so we can apply lower bounds on the norms of integral elements in totally real or imaginary quadratic fields. When the totally real field is fixed, we construct families which asymptotically achieve the largest possible minimal index, by a similar method to the imaginary V_4 construction.

Theorem 3.10. *(a) Let $K = LM$ with L an imaginary quadratic field and M a totally real, degree m field, such that $(D_L, D_M) = 1$, so that $D_K = D_L^m D_M^2$. If M is fixed and L varies, then $m(K) \ll_M |D_K|^{\frac{m-1}{2}}$.*

(b) Fix a totally real degree m Galois field M with odd discriminant. Let $L = \mathbb{Q}(\sqrt{-n})$ with $n > 0$, $-n \equiv 2, 3 \pmod 4$, $(n, D_M) = 1$. Then $m(K) \gg_M |D_K|^{\frac{m-1}{2}}$.

In particular, if M is the Shanks' simplest cubic field, we have $m(K) \gg_M |D_K|$, i.e.,

$m(K) \gg_M |D_L|^3$. It is known that both L and M are monogenic, and yet the composite field is far from monogenic.

We also consider families where the quadratic field is fixed, and the real fields are Shanks' simplest cubic fields, by using norm inequalities in the cubic fields [75].

Theorem 3.11 (Theorem 1.9)**.** *Let $L = \mathbb{Q}(\sqrt{b})$ for a fixed $b < 0$, $b \equiv 2, 3 \pmod 4$. If M is any of Shanks' simplest cubic fields - given by $M = \mathbb{Q}\,\theta$ with θ a root of $x^3 - ax^2 - (a+3)x - 1 = 0$, and $a > 0$ varies over integers with $a^2 + 3a + 9$ squarefree - such that D_M is coprime to D_L, then $K = LM$ has $m(K) \ll_b |D_K|^{\frac{1}{2}}$*

Theorem 3.12 (Theorem 1.10)**.** *Let $L = \mathbb{Q}(\sqrt{b})$ for $b < 0$, $b \equiv 2, 3 \pmod 4$. Infinitely many of Shanks' simplest cubic fields M give $K = LM$ with $m(K) \gg_b |D_K|^{\frac{1}{8}}$.*

3.4.1 Totally real and imaginary quadratic fields

Let $K = LM$, where $L = \mathbb{Q}(\sqrt{-n})$ and M is a degree m totally real Galois field with discriminant D_M. Suppose $-n \equiv 2, 3 \pmod 4$, and $\gcd(D_L, D_M) = 1$. Then $D_K = D_L^m D_M^2$.

Let $\omega = \omega^{(1)} = \sqrt{-n}$ so that $\omega^{(2)} = -\sqrt{-n}$, and let $\{1, \delta_2, ..., \delta_m\}$ be an integral basis of $\mathcal{O}_M$. Then $\{1, \delta_2, ..., \delta_m, \omega, \omega\delta_2, ..., \omega\delta_m\}$ is an integral basis of $\mathcal{O}_K$. Write $\delta_1 = 1$. Using the notation from [39] for the image of an arbitrary integral element $\alpha = \sum_{l=1}^m X_l\delta_l + \omega \sum_{l=1}^m X_{m+l}\delta_l$ under each of the embeddings, we set, for $i = 1, 2$ and $j = 1, ..., m$,

$$L^{(i,j)} = L^{(i,j)}(X_1, ..., X_{2m}) = \sum_{l=1}^m X_l \delta_l^{(j)} + \omega^{(i)} \left(\sum_{l=1}^m X_{m+l} \delta_l^{(j)} \right),$$

so that $D_{K/\mathbb{Q}}(\alpha) = \prod \left(L^{(i_1,j_1)} - L^{(i_2,j_2)}\right)^2$, where the product is over all $(i_1, j_1) < (i_2, j_2)$ in the lexicographic ordering. Recall that $I(\alpha)^2 D_K = D_{K/\mathbb{Q}}(\alpha)$, so we get the index as a product of three primitive polynomials by factoring $\frac{1}{\sqrt{D_K}}\sqrt{D_{K/\mathbb{Q}}(\alpha)}$. These factor by collecting conjugates

over M and L, with the remaining terms left in F_3:

$$F_1 = \prod_{1\le i<j\le m} (L^{(1,i)} - L^{(1,j)})(L^{(2,i)} - L^{(2,j)})$$
$$F_2 = \prod_{j=1}^{m} (L^{(1,j)} - L^{(2,j)})$$
$$F_3 = \prod_{1\le i<j\le m} (L^{(1,i)} - L^{(2,j)}) \prod_{1\le i<j\le m} (L^{(1,j)} - L^{(2,i)}).$$

We have

$$L^{(1,i)} - L^{(1,j)} = \sum_{l=2}^{m} X_l(\delta_l^{(i)} - \delta_l^{(j)}) + \sqrt{-n}\left(\sum_{l=2}^{m} X_{m+l}(\delta_l^{(i)} - \delta_l^{(j)})\right)$$
$$L^{(1,i)} - L^{(2,j)} = \sum_{l=2}^{m} X_l(\delta_l^{(i)} - \delta_l^{(j)}) + \sqrt{-n}\left(2X_{m+1} + \sum_{l=1}^{m} X_{m+l}(\delta_l^{(i)} + \delta_l^{(j)})\right).$$

Hence

$$F_2 = \sqrt{D_L^m} N_{M/\mathbb{Q}}\left(\sum_{l=1}^{m} X_{m+l}\delta_l\right),$$

and

$$F_1 = \prod_{1\le i<j\le m} \left(\left(\sum_{l=2}^{m} X_l(\delta_l^{(i)} - \delta_l^{(j)})\right)^2 + n\left(\sum_{l=2}^{m} X_{m+l}(\delta_l^{(i)} - \delta_l^{(j)})\right)^2\right)$$
$$F_3 = \prod_{1\le i<j\le m} \left(\left(\sum_{l=2}^{m} X_l(\delta_l^{(i)} - \delta_l^{(j)})\right)^2 + n\left(2X_{m+1} + \sum_{l=2}^{m} X_{m+l}(\delta_l^{(i)} + \delta_l^{(j)})\right)^2\right).$$

Then $F_i = f_i G_i$ for $i = 1, 2, 3$, where $f_1 = D_M$, $f_2 = \sqrt{D_L^m}$, $f_3 = 1$ and each G_i is a primitive polynomial with integers coefficients [39]. The index form is $I(X_2, .., X_{2m}) = \sqrt{\dfrac{(F_1F_2F_3)^2}{D_K}} = G_1G_2G_3$.

Note that if $\alpha = \omega + \delta_2$, i.e., $X_1 = 0, X_2 = 1, X_3 = \cdots = X_m = 0$ and $X_{m+1} = 1, X_{m+2} = \cdots = X_{2m} = 0$,

$$F_1 = \prod_{i<j} (\delta_2^{(i)} - \delta_2^{(j)})^2, \quad F_2 = |D_L|^{\frac{m}{2}}, \quad F_3 = \prod_{i<j} ((\delta_2^{(i)} - \delta_2^{(j)})^2 + 4n).$$

Hence $I(\omega + \delta_2) \ll_M n^{\frac{m(m-1)}{2}}$. So $m(K) \ll_M n^{\frac{m(m-1)}{2}} \asymp_M |D_K|^{\frac{2m-2}{4}}$, which improves the

general bound $|D_K|^{\frac{2m-2}{2}}$ in [106], and this proves Theorem 3.10 (a).

Fix a totally real Galois field M. In order to generate the field, at least one of X_{m+l}, $l = 1, ..., m$ is not zero. Then

$$|F_3| \geq n^{\frac{m(m-1)}{2}} \prod_{1 \leq i < j \leq m} \left(\left(2X_{m+1} + \sum_{l=2}^{m} X_{m+l}(\delta_l^{(i)} + \delta_l^{(j)}) \right)^2 \right).$$

Here $\prod_{1 \leq i < j \leq m} \left(2X_{m+1} + \sum_{l=2}^{m} X_{m+l}(\delta_l^{(i)} + \delta_l^{(j)}) \right)$ is invariant under $Gal(M/\mathbb{Q})$, and hence is in $\mathbb{Z}$. So $|F_3| \geq n^{\frac{m(m-1)}{2}}$. Therefore, $|G_3| \gg_M n^{\frac{m(m-1)}{2}}$, and $m(K) \gg_M n^{\frac{m(m-1)}{2}}$, proving Theorem 3.10 (b).

3.4.2 Simplest cubic and imaginary quadratic fields

In the special case where the totally real fields are Shanks' simplest cubics, we can also give a lower bound on the minimal index when the quadratic field is fixed, by using norm inequalities in the cubic fields [75].

Let $n > 0$, $a > 0$ be integers such that $-n \equiv 2, 3 \pmod 4$ and n, $a^2 + 3a + 9$ are squarefree and coprime. Let $K = LM$, where $L = \mathbb{Q}(\sqrt{-n})$ and $M = \mathbb{Q}(\theta)$, and θ is a root of $x^3 - ax^2 - (a+3)x - 1$. Let $\omega = \sqrt{-n}$. Then $\{1, \theta, \theta^2, \omega, \omega\theta, \omega\theta^2\}$ is an integral basis of K, $D_L = -4n$, $D_M = (a^2 + 3a + 9)^2$, and $D_K = D_L^3 D_M^2$.

The conjugates of ω, θ are

$$\omega^{(1)} = \sqrt{-n}, \quad \omega^{(2)} = -\sqrt{-n}, \quad \theta^{(1)} = \theta, \quad \theta^{(2)} = \frac{-1}{1+\theta}, \quad \theta^{(3)} = \frac{-1-\theta}{\theta}.$$

Choose θ to be the smallest of the three roots.

$$-1 - \frac{1}{a} < \theta < -1 - \frac{1}{2a}, \quad a + 1 < \theta^{(2)} < a + 1 + \frac{2}{a}, \quad -\frac{1}{a+2} < \theta^{(3)} < -\frac{1}{a+3}.$$

Hence for $a \geq 7$,

$$|\theta^{(1)} - \theta^{(2)}| < a + 2 + \frac{3}{a}, \quad |\theta^{(1)} - \theta^{(3)}| < 1 + \frac{1}{a}, \quad |\theta^{(2)} - \theta^{(3)}| < a + 1 + \frac{3}{a}.$$

Set $\delta_1 = \theta$, and $\delta_2 = \theta^2$ and $L^{(i,j)}$, F_i, f_i, G_i as in the previous section.

We have

$$F_2 = |D_L|^{\frac{3}{2}} N_{M/\mathbb{Q}}(X_4 + X_5\delta_1 + X_6\delta_2),$$

and

$$F_1 = \prod_{1\le i<j\le 3} \left(\left((X_2(\delta_1^{(i)} - \delta_1^{(j)}) + X_3(\delta_2^{(i)} - \delta_2^{(j)}) \right)^2 + n \left(X_5(\delta_1^{(i)} - \delta_1^{(j)}) + X_6(\delta_2^{(i)} - \delta_2^{(j)}) \right)^2 \right)$$

$$F_3 = \prod_{1\le i<j\le 3} \left(\left((X_2(\delta_1^{(i)} - \delta_1^{(j)}) + X_3(\delta_2^{(i)} - \delta_2^{(j)}) \right)^2 + n \left(2X_4 + X_5(\delta_1^{(i)} + \delta_1^{(j)}) + X_6(\delta_2^{(i)} + \delta_2^{(j)}) \right)^2 \right)$$

Note that if $X_3 = X_5 = X_6 = 0$, $X_2 = X_4 = 1$, $|F_1F_2F_3| \ll n^{\frac{5}{2}} a^4 (4n + \sqrt{D_M})^2$. Hence $I(\omega + \delta_1) \ll n(4n + a^2)^2$. Hence if we fix L, we obtain $m(K) \ll_L |D_K|^{\frac{1}{2}}$. This proves Theorem 1.9.

If $X_2 \neq 0$ or $X_3 \neq 0$, then both $|F_1|, |F_3| \gg (a^2+3a+9)^2$. Hence $|G_1G_2G_3| \gg (a^2+3a+9)^2$. Hence $I(X_2, ..., X_6) \gg a^4$. Suppose $X_2 = X_3 = 0$. Then $X_5 \neq 0$ or $X_6 \neq 0$, and (ignoring the factor of n^3) both G_2 and G_3 can be written as norms of elements in $\mathcal{O}_M \setminus \mathbb{Z}$:

$$\prod_{1\le i<j\le 3} (2X_4 + X_5(\delta_1^{(i)} + \delta_1^{(j)}) + X_6(\delta_2^{(i)} + \delta_2^{(j)})) = N_{M/\mathbb{Q}} \left((X_4 + X_5\delta_1 + X_6\delta_2) + (X_4 + X_5\delta_1^{(2)} + X_6\delta_2^{(2)}) \right).$$

Recall $F_2 = \sqrt{D_L^3} N_{M/\mathbb{Q}}(X_4 + X_5\delta_1 + X_6\delta_2)$.

We will use the following result to give a lower bound on the norms of most elements, and then show it must apply to at least one of our norm forms.

Lemma 3.13 (Lemmermeyer-Pethő)**.** *Suppose M is a simplest cubic field, $M = \mathbb{Q}(\theta)$, where θ is a root of $x^3 - ax^2 - (a+3)x - 1$, and $a^2 + 3a + 9$ is square-free. Then every element in $\xi \in \mathcal{O}_M$ either has $N_{M/\mathbb{Q}}(\xi) \ge 2a + 3$, or $\xi\eta \in \mathbb{Z}$ for some $\eta \in \mathcal{O}_M^\times$.*

We say that $\xi, \xi' \in \mathcal{O}_M$ are *associated* if $\xi' = \xi\eta$ for some unit η. So the theorem states that any element not associated to an integer has relatively large norm, $\gg |D_M|^{\frac{1}{4}}$.

Let $\xi = X_4 + X_5\delta_1 + X_6\delta_2 \in \mathcal{O}_M$. We will show that ξ and $\xi + \xi^{(2)}$ cannot both be associated to integers for any $\xi \in \mathcal{O}_M$.

Suppose $\xi = A\eta$ for $\eta \in \mathcal{O}_M^\times$ and $A \in \mathbb{Z}$. Every element in $\mathcal{O}_M \setminus \mathbb{Z}$ has square discriminant $D_M I(\xi)^2$, so if η has trace zero, then it is a root of a polynomial $x^3 - cx \pm 1$, which has

discriminant $\pm 4c^3 - 27 = D_M I(\eta)^2$. But the Diophantine equation $4x^3 - 27 = y^2$ only has the integral solutions $(3, \pm 9)$. So when $a > 0$, no unit in $\mathcal{O}_M$ has trace zero.

Suppose $\xi + \xi^{(2)} = B\nu$ for $\nu \in \mathcal{O}_M^\times$ and $B \in \mathbb{Z}$. Denote the minimal polynomial of η by $f(x) = x^3 - c_2 x^2 + c_1 x \pm 1$. Then $\xi + \xi^{(2)} = Ac_2 - \xi^{(3)}$, hence

$$\pm B^3 = N_{M/\mathbb{Q}}(\xi + \xi^{(2)}) = A^3 N_{M/\mathbb{Q}}(c_2 - \eta^{(3)}) = A^3(c_1 c_2 \pm 1).$$

Thus $A^3 | B^3$, so let $\frac{B}{A} = D$. Then $\pm D^3 = c_1 c_2 \pm 1$, and so $(D, c_2) = 1$. By comparing traces, we have

$$B\mathrm{Tr}(\nu) = \mathrm{Tr}(\xi + \xi^{(2)}) = \mathrm{Tr}(Ac_2 - \xi^{(3)}) = 3Ac_2 - Ac_2 = 2Ac_2.$$

Thus $D\mathrm{Tr}(\nu) = 2c_2$. Since $(D, c_2) = 1$, we have $D = \pm 1$ or ± 2. Since these units have non-zero traces, and $c_1 = \pm \mathrm{Tr}(\eta^{-1})$, we have $c_1 c_2 = \pm 2, \pm 7$ or ± 9. Of the possible choices, the only simplest cubic fields they arise in have conductor 7 (when $a = -1$), so when $a > 0$, at least one of ξ, $\xi + \xi^{(2)}$ is not associated to an integer for any $\xi \in \mathcal{O}_M$. Then by [75], if $\xi + \xi^{(2)}$ is not associated to an integer, $|N_{M/\mathbb{Q}}(\xi + \xi^{(2)})| \gg_L a$, and $|G_3| \gg_L a^2$. If ξ is not associate to an integer, then $|G_2| \gg_L a$. Therefore in all cases, $|G_1 G_2 G_3| \gg_L a$. So when the quadratic field is fixed and a varies, $m(K) \gg_L |D_K|^{\frac{1}{8}}$. This proves Theorem 1.10.

Chapter 4

Future Work

There are many improvements and extensions that can be made to these results. Many of the applications came from factoring the index form. A systematic method for doing this, depending on the maximal proper subfields of K, will have broad applications to various index problems: factorizations are frequently used to compute the field index, or to show that families of fields cannot be monogenic, and can also be used as we do to establish lower bounds on the minimal index, or to make clear what the correct upper bounds are. This can be established in the Galois case by showing that the field discriminant divides a product of discriminants of maximal subfields. Both Galois and non-Galois factorization statements are equivalent to matrix factorizations, with entries in the polynomial ring $Q(\vec{X})$.

In the case of cubics, experimental computation suggest there should be many fields with $m(K) > \frac{1}{2\sqrt[4]{27}}|D_K|^{\frac{1}{4}}$. We are limited by the dependence on $\sqrt[3]{\frac{b}{a}}$ being very close to 1 to give effective Diophantine approximations, and it is unlikely this will improve without new methods. Nonetheless, the results can be extended to pure cubics with $\sqrt[3]{\frac{b}{a}}$ close to any integer with some modification.

Any field where most elements have norms bounded away from 0 is a candidate for forming a composite field with large minimal index. This include composites of any number of quadratic imaginary fields, real quadratic fields of the form $Q\left(\sqrt{t^2+1}\right)$, and Shanks' simplest cubic fields. The nonic fields generated by composing two of Shanks' simplest cubics are Galois, with four maximal cubic subfields, and so the index form splits into four factors, which are susceptible to arguments involving norm bounds.

Aside form the imaginary V_4 fields, where all of the minimal indices are relatively large, little is known about the number of fields with large minimal index, as a proportion of all fields of the same type, ordered by discriminant. Results in this direction will shape what is known about the distribution of the minimal index, which was a primary motivator for showing the existence of fields with large minimal index.

Bibliography

[1] N. C. Ankeny, S. Chowla, and H. Hasse. On the class-number of the maximal real subfield of a cyclotomic field. *J. Reine Angew. Math.*, 217:217–220, 1965.

[2] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[3] M. Bauer. Über die außerwesentlichen Diskriminantenteiler einer Gattung. *Math. Ann.*, 64(4):573–576, 1907.

[4] A. T. Benjamin and J. J. Quinn. *Proofs that really count*, volume 27 of *The Dolciani Mathematical Expositions*. Mathematical Association of America, Washington, DC, 2003. The art of combinatorial proof.

[5] M. A. Bennett. Explicit lower bounds for rational approximation to algebraic numbers. *Proc. London Math. Soc. (3)*, 75(1):63–78, 1997.

[6] Y. Bilu and G. Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[7] E. Bombieri. Forty years of effective results in Diophantine theory. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 194–213. Cambridge Univ. Press, Cambridge, 2002.

[8] E. Bombieri and J. Mueller. On effective measures of irrationality for $\sqrt[r]{a/b}$ and related numbers. *J. Reine Angew. Math.*, 342:173–196, 1983.

[9] D. A. Buell. *Binary quadratic forms*. Springer-Verlag, New York, 1989. Classical theory and modern computations.

[10] Y. Bugeaud and K. Győry. Bounds for the solutions of Thue-Mahler equations and norm form equations. *Acta Arith.*, 74(3):273–292, 1996.

[11] M.-L. Chang. Non-monogeneity in a family of sextic fields. *J. Number Theory*, 97(2):252–268, 2002.

[12] J. H. Chen and P. Voutier. Complete solution of the Diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations. *J. Number Theory*, 62(1):71–99, 1997.

[13] G. V. Chudnovsky. On the method of Thue-Siegel. *Ann. of Math. (2)*, 117(2):325–382, 1983.

[14] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[15] J. H. Conway. *The sensual (quadratic) form*, volume 26 of *Carus Mathematical Monographs*. Mathematical Association of America, Washington, DC, 1997. With the assistance of Francis Y. C. Fung.

[16] H. Davenport. On a conjecture of Mordell concerning binary cubic forms. *Proc. Cambridge Philos. Soc.*, 37:325–330, 1941.

[17] R. Dedekind. Ueber den zusammenhang zwischen der theorie der ideale und der theorie der hheren congruenzen. *Abhandlungen der Kniglichen Gesellschaft der Wissenschaften in Gttingen*, 23:3–38, 1878.

[18] R. Dedekind. Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern. *J. Reine Angew. Math.*, 121:40–123, 1900.

[19] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree*. Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[20] P. G. L. Dirichlet. *Vorlesungen über Zahlentheorie*. Herausgegeben und mit Zusätzen versehen von R. Dedekind. Vierte, umgearbeitete und vermehrte Auflage. Chelsea Publishing Co., New York, 1968.

[21] D. S. Dummit and H. Kisilevsky. Indices in cyclic cubic fields. pages 29–42, 1977.

[22] D. Easton. Effective irrationality measures for certain algebraic numbers. *Math. Comp.*, 46(174):613–622, 1986.

[23] D. Eloff, B. K. Spearman, and K. S. Williams. Integral bases for an infinite family of cyclic quintic fields. *Asian J. Math.*, 10(4):765–771, 2006.

[24] H. T. Engstrom. On the common index divisors of an algebraic field. *Trans. Amer. Math. Soc.*, 32(2):223–237, 1930.

[25] J. Esmonde and M. R. Murty. *Problems in algebraic number theory*, volume 190 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2005.

[26] I. Gaál. Computing elements of given index in totally complex cyclic sextic fields. *J. Symbolic Comput.*, 20(1):61–69, 1995.

[27] I. Gaál. Solving index form equations in fields of degree 9 with cubic subfields. *J. Symbolic Comput.*, 30(2):181–193, 2000.

[28] I. Gaál. *Diophantine equations and power integral bases*. Birkhäuser Boston, Inc., Boston, MA, 2002. New computational methods.

[29] I. Gaál and K. Győry. Index form equations in quintic fields. *Acta Arith.*, 89(4):379–396, 1999.

[30] I. Gaál, P. Olajos, and M. Pohst. Power integral bases in orders of composite fields. *Experiment. Math.*, 11(1):87–90, 2002.

[31] I. Gaál, A. Pethő, and M. Pohst. On the resolution of index form equations in quartic number fields. *J. Symbolic Comput.*, 16(6):563–584, 1993.

[32] I. Gaál, A. Pethő, and M. Pohst. On the resolution of index form equations in dihedral quartic number fields. *Experiment. Math.*, 3(3):245–254, 1994.

[33] I. Gaál, A. Pethő, and M. Pohst. Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields. *J. Number Theory*, 57(1):90–104, 1996.

[34] I. Gaál, A. Pethö, and M. Pohst. On the indices of biquadratic number fields having Galois group V_4. *Arch. Math. (Basel)*, 57(4):357–361, 1991.

[35] I. Gaál, A. Pethö, and M. Pohst. On the resolution of index form equations in biquadratic number fields. I, II. *J. Number Theory*, 38(1):18–34, 35–51, 1991.

[36] I. Gaál, A. Pethö, and M. Pohst. On the resolution of index form equations in biquadratic number fields. III. The bicyclic biquadratic case. *J. Number Theory*, 53(1):100–114, 1995.

[37] I. Gaál and G. Petrányi. Calculating all elements of minimal index in the infinite parametric family of simplest quartic fields. *Czechoslovak Math. J.*, 64(139)(2):465–475, 2014.

[38] I. Gaál and L. Remete. Power integral bases in a family of sextic fields with quadratic subfields. *Tatra Mt. Math. Publ.*, 64:59–66, 2015.

[39] I. Gaál and L. Remete. Integral bases and monogenity of pure fields. *J. Number Theory*, 173:129–146, 2017.

[40] I. Gaál and L. Remete. Non-monogenity in a family of octic fields. *Rocky Mountain J. Math.*, 47(3):817–824, 2017.

[41] I. Gaál, L. Remete, and T. Szabó. Calculating power integral bases by solving relative Thue equations. *Tatra Mt. Math. Publ.*, 59:79–92, 2014.

[42] I. Gaál, L. Remete, and T. Szabó. Calculating power integral bases by using relative power integral bases. *Funct. Approx. Comment. Math.*, 54(2):141–149, 2016.

[43] I. Gaál and T. Szabó. A note on the minimal indices of pure cubic fields. *JP J. Algebra Number Theory Appl.*, 19(2):129–139, 2010.

[44] I. Gaál and T. Szabó. Power integral bases in parametric families of biquadratic fields. *JP J. Algebra Number Theory Appl.*, 24(1):105–114, 2012.

[45] C. F. Gauss. *Disquisitiones arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.

[46] G. Gras. Non monogénéité d'anneaux d'entiers. In *Théorie des nombres, Années 1986/87–1987/88, Fasc. 1*, Publ. Math. Fac. Sci. Besançon, page 43. Univ. Franche-Comté, Besançon, 1988.

[47] M.-N. Gras. Sur les corps cubiques cycliques dont l'anneau des entiers est monogène. *C. R. Acad. Sci. Paris Sér. A*, 278:59–62, 1974.

[48] M.-N. Gras. **Z**-bases d'entiers 1, θ, θ^2, θ^3 dans les extensions cycliques de degré 4 de **Q**. In *Number theory, 1979–1980 and 1980–1981*, Publ. Math. Fac. Sci. Besançon, pages Exp. No. 6, 14. Univ. Franche-Comté, Besançon, 1981.

[49] M.-N. Gras. Non monogénéité de l'anneau des entiers de certaines extensions abéliennes de **Q**. In *Number theory (Besançon), 1983–1984*, Publ. Math. Fac. Sci. Besançon, pages Exp. No. 5, 25. Univ. Franche-Comté, Besançon, 1984.

[50] M.-N. Gras. Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de **Q**. In *Séminaire de théorie des nombres, Paris 1984–85*, volume 63 of *Progr. Math.*, pages 97–107. Birkhäuser Boston, Boston, MA, 1986.

[51] M.-N. Gras. Non monogénéité d'anneaux d'entiers. In *Séminaire de théorie des nombres, 1985–1986 (Talence, 1985–1986)*, pages Exp. No. 15, 8. Univ. Bordeaux I, Talence, 1986.

[52] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de **Q** de degré premier $l \geq 5$. *J. Number Theory*, 23(3):347–353, 1986.

[53] M.-N. Gras and F. Tanoé. Corps biquadratiques monogènes. *Manuscripta Math.*, 86(1):63–79, 1995.

[54] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné. *Acta Arith.*, 23:419–426, 1973.

[55] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné. II. *Publ. Math. Debrecen*, 21:125–144, 1974.

[56] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné. III. *Publ. Math. Debrecen*, 23(1-2):141–165, 1976.

[57] K. Győry. Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains. *Acta Math. Hungar.*, 42(1-2):45–80, 1983.

[58] K. Győry. On norm form, discriminant form and index form equations. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, volume 34 of *Colloq. Math. Soc. János Bolyai*, pages 617–676. North-Holland, Amsterdam, 1984.

[59] M. Hall. Indices in cubic fields. *Bull. Amer. Math. Soc.*, 43(2):104–108, 1937.

[60] K. Hardy, R. H. Hudson, D. Richman, K. S. Williams, and N. M. Holtz. Calculation of the class numbers of imaginary cyclic quartic fields. *Math. Comp.*, 49(180):615–620, 1987.

[61] H. Hasse. *Zahlentheorie*. Zweite erweiterte Auflage. Akademie-Verlag, Berlin, second edition, 1963.

[62] K. Hensel. Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung. *J. Reine Angew. Math.*, 113:128–160, 1894.

[63] J. G. Huard. *Index forms and power bases for cyclic cubic fields*. ProQuest LLC, Ann Arbor, MI, 1978. Thesis (Ph.D.)–The Pennsylvania State University.

[64] R. H. Hudson and K. S. Williams. The integers of a cyclic quartic field. *Rocky Mountain J. Math.*, 20(1):145–150, 1990.

[65] B. Jadrijević. Establishing the minimal index in a parametric family of bicyclic biquadratic fields. *Period. Math. Hungar.*, 58(2):155–180, 2009.

[66] B. Jadrijević. Solving index form equations in two parametric families of biquadratic fields. *Math. Commun.*, 14(2):341–363, 2009.

[67] L.-C. Kappe and B. Warren. An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly*, 96(2):133–137, 1989.

[68] H. H. Kim and Z. Wolske. Number fields with large minimal index containing quadratic subfields. *IJNT*, (to appear), 2018.

[69] H. H. Kim and Z. Wolske. Pure cubic fields with large minimal index. *Acta Arith.*, 182(3):271–277, 2018.

[70] M. J. Lavallee, B. K. Spearman, and K. S. Williams. Lifting monogenic cubic fields to monogenic sextic fields. *Kodai Math. J.*, 34(3):410–425, 2011.

[71] M. J. Lavallee, B. K. Spearman, K. S. Williams, and Q. Yang. Dihedral quintic fields with a power basis. *Math. J. Okayama Univ.*, 47:75–79, 2005.

[72] M. J. Lavallee, B. K. Spearman, K. S. Williams, and Q. Yang. Dihedral quintic fields with a power basis. *Math. J. Okayama Univ.*, 47:75–79, 2005.

[73] J. H. Lee. Evaluation of the Dedekind zeta functions at $s = -1$ of the simplest quartic fields. *J. Number Theory*, 143:24–45, 2014.

[74] F. Lemmermeyer. Small norms in quadratic fields, 2013.

[75] F. Lemmermeyer and A. Pethő. Simplest cubic fields. *Manuscripta Math.*, 88(1):53–58, 1995.

[76] F. Levi. Cubic number fields and cubic form classes. (kubische zahlkrper und binre kubische formenklassen.) (german). *Leipz. Ber.*, 66:26–37, 1914.

[77] N. T. Motoda, Yasuo and K. H. Park. On power integral bases of the 2-elementary abelian extension. *Trends in Math.*, 9(1):55–63, 2006.

[78] Y. Motoda. On biquadratic fields. *Mem. Fac. Sci. Kyushu Univ. Ser. A*, 29(2):263–268, 1975.

[79] Y. Motoda. On integral bases of certain real monogenic biquadratic fields. *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, 33(1):9–22, 2004.

[80] Y. Motoda and T. Nakahara. Monogenesis of algebraic number fields whose Galois groups are 2-elementary abelian. In *Proceedings of the 2003 Nagoya Conference "Yokoi-Chowla Conjecture and Related Problems"*, pages 91–99. Saga Univ., Saga, 2004.

[81] Y. Motoda, T. Nakahara, S. I. A. Shah, and T. Uehara. On a problem of Hasse. In *Algebraic number theory and related topics 2007*, RIMS Kôkyûroku Bessatsu, B12, pages 209–221. Res. Inst. Math. Sci. (RIMS), Kyoto, 2009.

[82] T. Nagel. Zur Arithmetik der Polynome. *Abh. Math. Sem. Univ. Hamburg*, 1(1):178–193, 1922.

[83] M. Nair. Power free values of polynomials. *Mathematika*, 23(2):159–183, 1976.

[84] T. Nakahara. Examples of algebraic number fields which have not unramified extensions. *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, (1):1–8, 1973.

[85] T. Nakahara. On cyclic biquadratic fields related to a problem of Hasse. *Monatsh. Math.*, 94(2):125–132, 1982.

[86] T. Nakahara. On the indices and integral bases of noncyclic but abelian biquadratic fields. *Arch. Math. (Basel)*, 41(6):504–508, 1983.

[87] T. Nakahara. On the minimum index of a cyclic quartic field. *Arch. Math. (Basel)*, 48(4):322–325, 1987.

[88] T. Nakahara. A simple proof for non-monogenesis of the rings of integers in some cyclic fields. In *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., pages 167–173. Oxford Univ. Press, New York, 1993.

[89] T. Nakahara. Hasse's problem for monogenic fields. *Ann. Math. Blaise Pascal*, 16(1):47–56, 2009.

[90] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[91] A. Pethő. On the resolution of Thue inequalities. *J. Symbolic Comput.*, 4(1):103–109, 1987.

[92] S. I. A. Shah and T. Nakahara. Non-monogenesis of the ring of integers in a sextic field of a prime conductor. In *Proceedings of the Jangjeon Mathematical Society*, volume 1 of *Proc. Jangjeon Math. Soc.*, pages 81–84. Jangjeon Math. Soc., Hapcheon, 2000.

[93] S. I. A. Shah and T. Nakahara. Non-monogenetic aspect of the ring of integers in certain abelian fields. In *Proceedings of the Jangjeon Mathematical Society*, volume 1 of *Proc. Jangjeon Math. Soc.*, pages 75–79. Jangjeon Math. Soc., Hapcheon, 2000.

[94] S. I. A. Shah and T. Nakahara. Monogenesis of the rings of integers in certain imaginary abelian fields. *Nagoya Math. J.*, 168:85–92, 2002.

[95] S. I. A. Shah and T. Nakahara. A prototype of certain abelian fields whose rings of integers have a power basis. *Rep. Fac. Sci. Engrg. Saga Univ. Math.*, 31(1):7–19, 2002.

[96] A. K. Silvester, B. K. Spearman, and K. S. Williams. The index of a dihedral quartic field. *JP J. Algebra Number Theory Appl.*, 3(1):121–144, 2003.

[97] N. J. Sloane. The On-line Encyclopedia of Integer Sequences. https://oeis.org. Sequence A065474.

[98] B. K. Spearman and K. S. Williams. Cubic fields with a power basis. *Rocky Mountain J. Math.*, 31(3):1103–1109, 2001.

[99] B. K. Spearman and K. S. Williams. The index of a cyclic quartic field. *Monatsh. Math.*, 140(1):19–70, 2003.

[100] B. K. Spearman and K. S. Williams. On the distribution of cyclic cubic fields with index 2. *Int. J. Number Theory*, 2(2):235–247, 2006.

[101] B. K. Spearman and K. S. Williams. The simplest D_4-octics. *Int. J. Algebra*, 2(1-4):79–89, 2008.

[102] B. K. Spearman, Q. Yang, and J. Yoo. Minimal indices of pure cubic fields. *Arch. Math. (Basel)*, 106(1):35–40, 2016.

[103] M. Sultan, Y. Kôhno, and T. Nakahara. Monogenity of biquadratic fields related to Dedekind-Hasse's problem. *Punjab Univ. J. Math. (Lahore)*, 47(2):77–82, 2015.

[104] M. Sultan and T. Nakahara. On certain octic biquartic fields related to a problem of Hasse. *Monatsh. Math.*, 176(1):153–162, 2015.

[105] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135:284–305, 1909.

[106] J. L. Thunder and J. Wolfskill. Algebraic integers of small discriminant. *Acta Arith.*, 75(4):375–382, 1996.

[107] N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *J. Number Theory*, 31(2):99–132, 1989.

[108] P. M. Voutier. Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers revisited. *J. Théor. Nombres Bordeaux*, 19(1):263–288, 2007.

[109] K. S. Williams. Integers of biquadratic fields. *Canad. Math. Bull.*, 13:519–526, 1970.

[110] E. von Żyliński. Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper. *Math. Ann.*, 73(2):273–274, 1913.