INDICES OF ALGEBRAIC INTEGERS IN CUBIC FIELDS

by

JEREMY T SMITH

Bachelor of Science, 2012
University of Dallas
Irving, Texas

Master of Science, 2014
Texas Christian University
Fort Worth, Texas

Submitted to the Graduate Faculty of the
College of Science and Engineering
Texas Christian University
in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy

May 2018

ACKNOWLEDGEMENTS

I am extremely grateful to my advisor, George Gilbert, for his willingness to take on a Ph.D. candidate despite his busy schedule, as well as his guidance and incredible patience throughout this long process. I'd also like to extend my appreciation to the math faculty and graduate students, for enthusiastically sharing their wealth of knowledge and contributing to my development as a mathematician.

Special thanks are extended to my close friends, who have always believed in me and pushed me to achieve my full potential. Lastly, I am forever grateful to my family for their love and support. I am especially thankful for my parents, who have always provided an exemplar of hard work that I try my best to emulate every day.

Contents

1 Introduction 1

2 Sets of Indices 15

2.1 Indices and Discriminants 15

2.2 The Factorization of (2) in a Cubic Field 20

2.3 Some Lemmas 25

2.4 The Main Result 34

3 Unbounded Minimal Indices 66

3.1 An Indicial Form for Cubic Fields 66

3.2 The Main Result 71

1 Introduction

The topic of indices of algebraic integers is a largely underdeveloped area of algebraic number theory. Although indices are quite elementary in concept, existence questions in all families of number fields (with the exception of quadratic fields) still abound. In cubic fields alone, much is still unknown. As is typical of number theory in general, an all-encompassing theory of indices remains elusive to the extent that new results are typically relegated to developing the theory for specific families of number fields. Such will remain the case for the present dissertation, as our sole concern will be with cubic fields.

The historical motivation for the study of indices is rooted in the contributions of Richard Dedekind [2]. The key idea with which Dedekind grappled was that while number fields are always generated by a single element over $\mathbb{Q}$, the same is not always true for number rings over $\mathbb{Z}$. The example he gave (which was the first of its kind) was the cubic field F generated by a root θ of the polynomial x^3+x^2-2x+8. While there are infinitely many algebraic integers generating F over $\mathbb{Q}$, the ring of integers of F can be generated over $\mathbb{Z}$ by a minimum of two algebraic integers. In fact, one example of a basis for $\mathcal{O}_F$ over $\mathbb{Z}$ is given by $\{1, \theta, (\theta^2+\theta)/2\}$. Clearly, $\mathcal{O}_F$ cannot be generated by θ over $\mathbb{Z}$; more generally, $\mathcal{O}_F$ cannot be generated over $\mathbb{Z}$ by any $\mathbb{Z}$-linear combination of these basis elements.

The concept of indices is inseparably linked to a discussion of bases for number rings over $\mathbb{Z}$. Our motivation for studying them comes from our interest in the structure of these bases and in their relation to orders generated by a single element within their respective number rings. In this dissertation, we uncover results about indices in families of cubic fields. The results obtained extend and generalize the work of Spearman and Williams [10, 11] on power bases and index sets, and of Hall [5] and of Dummitt and Kisilevsky [3] on minimal indices. In the subsequent exposition, we will lay the groundwork for exploring these results, and then give a preview of our own results. We begin by discussing the relevant background from algebraic number theory, and introducing the concept of index.

Throughout, let $F \subseteq \mathbb{C}$ be a number field of degree n, with number ring $\mathcal{O}_F$. Let $\sigma_j : F \hookrightarrow \mathbb{C}$, with $j \in \{1, ..., n\}$ and $\sigma_1 = id$, be the n embeddings of F into $\mathbb{C}$. If $\mathcal{B} = \{\beta_1, ..., \beta_n\}$ is any $\mathbb{Q}$-basis for F, the *discriminant* of $\mathcal{B}$ is given by

$$\mathrm{disc}(\mathcal{B}) = \mathrm{disc}(\beta_1, ..., \beta_n) := \det(\sigma_j(\beta_i))^2 \in \mathbb{Q} - \{0\}\,,$$

where $(\sigma_j(\beta_i))$ denotes the matrix with entry $\sigma_j(\beta_i)$ in the i^{th} row and the j^{th} column.

Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree n with roots θ_1, ..., $\theta_n \in \mathbb{C}$. Then $f(x) = d \cdot \prod_{i=1}^{n}(x - \theta_i)$, for some $d \in \mathbb{Q}$. The *discriminant* of $f(x)$ is given by

$$\mathrm{disc}(f(x)) := d^{2n-2} \cdot \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

If $f(x)$ is the minimal polynomial over $\mathbb{Q}$ of $\theta \in \mathcal{O}_F$, and $F = \mathbb{Q}(\theta)$, we have

$$\mathrm{disc}(f(x)) = \mathrm{disc}(1, \theta, ..., \theta^{n-1}).$$

The number ring $\mathcal{O}_F$ is a free $\mathbb{Z}$-module of rank n. A basis for $\mathcal{O}_F$ over $\mathbb{Z}$ is called an *integral basis*. If $\mathcal{B} = \{\beta_1, ..., \beta_n\}$ where $\beta_i \in \mathcal{O}_F$ for each $i \in \{1, ..., n\}$, we have that $\mathrm{disc}(\mathcal{B}) \in \mathbb{Z}$. This leads to the following important proposition:

Proposition 1.1. *Let F be a number field. A set $\mathcal{B}$ is an integral basis for $\mathcal{O}_F$ if and only if $\mathcal{B} \subset \mathcal{O}_F$, $\mathcal{B}$ is a $\mathbb{Q}$-basis for F, and $|disc(\mathcal{B})| \in \mathbb{N}$ is minimal over the set of all $\mathbb{Q}$-bases for F contained in $\mathcal{O}_F$.*

If $\mathcal{B}$ is an integral basis for F, then $\operatorname{disc}(\mathcal{B})$ is called the *field discriminant* of F, denoted by Δ_F. While there are a countably infinite number of distinct integral bases for $\mathcal{O}_F$, Δ_F is an invariant of F due to the minimality of $|\operatorname{disc}(\mathcal{B})|$.

Let $\theta \in \mathcal{O}_F$. Recall $\mathbb{Z}[\theta]$ is the $\mathbb{Z}$-submodule of $\mathcal{O}_F$ consisting of all polynomials in θ. Since $[F : \mathbb{Q}] = n$, the minimal polynomial of θ over $\mathbb{Q}$ has degree at most n. Thus $\mathbb{Z}[\theta]$ is a finitely generated $\mathbb{Z}$-submodule of $\mathcal{O}_F$. The $\mathbb{Z}$-module index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_F$ is called the *index* of θ in $\mathcal{O}_F$, written

$$\operatorname{ind}_F(\theta) := [\mathcal{O}_F : \mathbb{Z}[\theta]].$$

Depending on the choice of θ, $\operatorname{ind}_F(\theta)$ need not be finite. If the minimal polynomial of θ over $\mathbb{Q}$ has degree less than n, then $\mathbb{Z}[\theta]$ is freely generated over $\mathbb{Z}$ by fewer than n elements. In this case, $\operatorname{ind}_F(\theta) = \infty$. However, if the minimal polynomial of θ over $\mathbb{Q}$ has degree n, then $\mathcal{O}_F$ and $\mathbb{Z}[\theta]$ have the same rank. Thus, $\operatorname{ind}_F(\theta) < \infty$.

In this dissertation, we will be concerned exclusively with the case in which $\operatorname{ind}_F(\theta) < \infty$. Hence, we will have no need to reference the field from which we are computing the index. From now on, we will simply write $\operatorname{ind}(\theta)$ instead, where it will always be implied that θ is a generator for F.

Let $\mathcal{B}_1$ be any integral basis for $\mathcal{O}_F$ and let $\mathcal{B}_2 = \{1, \theta, ..., \theta^{n-1}\}$. Since $\mathcal{B}_1$ and $\mathcal{B}_2$ are both $\mathbb{Q}$-bases for F consisting of algebraic integers, we have that $\mathcal{O}_F$ and $\mathbb{Z}[\theta]$ are both (isomorphic to) full $\mathbb{Z}$-lattices in $\mathbb{R}^n$. The ratio of the volume of a fundamental parallelotope of $\mathbb{Z}[\theta]$ to the volume of a fundamental parallelotope of $\mathcal{O}_F$ is the absolute value of the determinant of the change-of-basis matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$. This ratio is also equal to $|\mathcal{O}_F/\mathbb{Z}[\theta]|$ by the third isomorphism theorem. Therefore, $\operatorname{ind}(\theta)$ is the absolute value of the determinant of the change-of-basis matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$.

We can use this fact to derive a more useful one. Suppose $\{\beta_1, ..., \beta_n\}$ is an integral basis for $\mathcal{O}_F$. Then for any $i \in \{0, 1, ..., n-1\}$, we have $\theta^i = \sum_{j=1}^{n} a_{ij}\beta_j$ for some $a_{ij} \in \mathbb{Z}$. Applying the embeddings σ_k to both sides for each $k \in \{1, ..., n\}$, gives

$$\sigma_k(\theta^i) = \sum_{j=1}^{n} a_{ij}\sigma_k(\beta_j).$$

Converting this equivalence to matrices, taking determinants, and squaring both sides gives

$$\mathrm{disc}(1, \theta, ..., \theta^{n-1}) = (\det(a_{ij}))^2 \Delta_F.$$

Since (a_{ij}) is the change-of-basis matrix from $\{1, \theta, ..., \theta^{n-1}\}$ to $\{\beta_1, ..., \beta_n\}$, we have that $\mathrm{ind}(\theta) = |\det(a_{ij})|$. This gives the following proposition:

Proposition 1.2. *Let $F = \mathbb{Q}(\theta)$, with $\theta \in \mathcal{O}_F$, be a number field of degree n. Then*

$$disc(1, \theta, ..., \theta^{n-1}) = (ind(\theta))^2 \Delta_F.$$

This provides us with a more useful way of computing the index of an algebraic integer, as we will see later.

For any $\theta \in \mathcal{O}_F$ such that $F = \mathbb{Q}(\theta)$, it is well-known that $\mathcal{O}_F$ has an integral basis of the form

$$\mathcal{B} = \left\{1, \frac{\theta + b_{1,0}}{k_1}, \frac{\theta^2 + b_{2,1}\theta + b_{2,0}}{k_2}, ..., \frac{\theta^{n-1} + b_{n-1,n-2}\theta^{n-2} + ... + b_{n-1,0}}{k_{n-1}}\right\},$$

where $b_{i,l}, k_i \in \mathbb{N}$ for each $i \in \{0, 1, ..., n-1\}$ and $l \in \{0, 1, ..., n-2\}$, $k_0 = b_{0,0} = 1$, and $k_i \mid k_{i+1}$ for each $i \in \{0, 1, ..., n-2\}$.[1] We call $\mathcal{B}$ a *θ-standard form* for $\mathcal{O}_F$. Since

[1] See Hall [5] for the proof of the cubic case. The degree n case follows similarly.

the change-of-basis matrix from $\{1, \theta, ..., \theta^{n-1}\}$ to $\mathcal{B}$ is a lower triangular matrix with diagonal entries given by the k_i, we have that $\operatorname{ind}(\theta) = \prod_{i=0}^{n-1} k_i$. Thus, indices can be thought of as products of denominators of integral bases in standard form.

From the definition of index, $\mathcal{O}_F = \mathbb{Z}[\theta]$ exactly when $\operatorname{ind}(\theta) = 1$. When this is the case, F is said to be *monogenic*. Moreover, the basis $\{1, \theta, ..., \theta^{n-1}\}$ for F over $\mathbb{Q}$ is actually an integral basis for $\mathcal{O}_F$, called a *power basis*. If $\operatorname{ind}(\theta) > 1$ for every $\theta \in \mathcal{O}_F$, then F is said to be *non-monogenic*.

A field F is non-monogenic exactly when $\mathcal{O}_F$ cannot be generated over $\mathbb{Z}$ by a single element. Dedekind's example of the field F generated by a root θ of $x^3 + x^2 - 2x + 8$ provides an example of a non-monogenic field. Since $\{1, \theta, (\theta^2 + \theta)/2\}$ is an integral basis for $\mathcal{O}_F$, we have that $\operatorname{ind}(\theta) = 2$. However, it can be shown that no algebraic integer in $\mathcal{O}_F$ of index 1 exists. It follows that any integral basis for $\mathcal{O}_F$ in standard form must have some basis elements with denominators.

It is well-known that quadratic and cyclotomic fields are monogenic. Indeed, any quadratic field $F = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}$ and squarefree, has ring of integers given by

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,\ 3 \pmod{4}, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Furthermore, if $F = \mathbb{Q}(\zeta_n)$ is any cyclotomic field, where $n \in \mathbb{Z}$ and ζ_n is a primitive nth root of unity, then $\mathcal{O}_F$ has an integral basis given by

$$\left\{\zeta_n^j : 1 \leq j \leq n-1, \gcd(j, n) = 1\right\}.$$

Hence $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$.

The characterization of all monogenic number fields is still an open problem. In the past, number theorists have typically focused on finding families of monogenic number fields. However, such families are usually more exotic than the standard examples given above. We will see a few of these examples later.

Determining whether a given number field is monogenic is equivalent to determining whether it contains an algebraic integer of index 1. A more general question we might ask is: what is the smallest natural number assumed by the index of an algebraic integer in a given number ring? Even more generally, we might ask: which natural numbers occur as indices of algebraic integers within that number ring?

For any number field F, we define

$$S_F := \{\operatorname{ind}(\theta) : F = \mathbb{Q}(\theta),\ \theta \in \mathcal{O}_F\} \subseteq \mathbb{N}.$$

Since $S_F \neq \varnothing$, we define the *minimal index* of $\mathcal{O}_F$ by

$$m(F) := \min\ S_F.$$

If $m(F) = 1$, then F is monogenic. In general, if $m(F) = \operatorname{ind}(\theta)$, then a θ-standard form for $\mathcal{O}_F$ will have denominators that multiply to give $m(F)$. In this sense, $m(F)$ describes how close $\mathcal{O}_F$ is to having a power basis; the closer $m(F)$ is to 1, the closer F is to being monogenic.[2]

[2] While the presence of some denominator $k_i > 1$ in an integral basis for $\mathcal{O}_F$ in θ-standard form certainly indicates that $\operatorname{ind}(\theta) > 1$, it does not necessarily indicate that $m(F) > 1$. This is easy to see in the case of the quadratics, in which $\operatorname{ind}(\sqrt{d}) = 2$ for each squarefree $d \equiv 1 \pmod 4$ with $d \neq 1$, whereas each quadratic is monogenic.

Given an element of S_F, we can easily determine infinitely many more. This is summarized in the following proposition:

Proposition 1.3. *Let $F = \mathbb{Q}(\theta)$ be a number field of degree n, with $\theta \in \mathcal{O}_F$. Then for any $a, b \in \mathbb{Z}$ with $a \neq 0$,*

$$ind(a\theta + b) = |a|^n \cdot ind(\theta).$$

The proof is an easy application of change-of-basis matrices. One consequence of this proposition is that the value of b does not affect the index of θ. Hence, when computing $\operatorname{ind}(\theta)$, we can ignore the basis element 1 when we write θ as a linear combination of the basis elements in some α-standard form.

Determining the set S_F is equivalent to finding the values assumed by a polynomial form dependent on F, called an *indicial form*. For a number field of degree n, an indicial form is a homogeneous polynomial $I_F(x_1, ..., x_{n-1}) : \mathbb{Z}^{n-1} \to \mathbb{Z}$ of degree $\dfrac{n(n-1)}{2}$ in $n-1$ variables whose image is $\pm S_F$. To derive an indicial form, first take any integral basis for F of the form $\{\beta_0, ..., \beta_{n-1}\}$, where $\beta_0 = 1$. For arbitrary $\theta \in \mathcal{O}_F$, we have that $\operatorname{ind}(\theta) = \operatorname{ind}(\theta - x_0)$ by Proposition 1.3. Thus, without loss of generality we may write $\theta = \displaystyle\sum_{i=1}^{n-1} x_i\beta_i$. Finally, we compute the determinant of the change-of-basis matrix from $\{1, \alpha, ..., \alpha^{n-1}\}$ to $\{\beta_0, ..., \beta_{n-1}\}$. This determinant gives the indicial form.[3] Since integral bases are unique up to linear transformation by a matrix in $SL_n(\mathbb{Z})$, indicial forms are also unique up to unimodular substitution. Thus, distinct indicial forms for a given number field represent the same set of integers $\pm S_F$.

[3] The indicial form for any quadratic field L is given by $I_L(x) = x$. Thus $S_L = \mathbb{N}$. We will provide some nontrivial examples of indicial forms when we discuss cubic fields. Indicial forms for number fields of degree greater than 3 are not easy to derive. In fact, as the degree of the number field increases, the indicial form becomes increasingly cumbersome to compute.

For any $\theta \in \mathcal{O}_F$, $\operatorname{ind}(\theta)$ may computed by writing $\theta = \sum_{i=1}^{n-1} c_i\beta_i$ for some $c_i \in \mathbb{Z}$ and then calculating $|I_F(c_1, ..., c_{n-1})|$. Thus, determining whether a number field is monogenic is equivalent to determining whether an element in $\{\pm 1\}$ is represented by the form. In general, finding the set of all integers represented by an integral form like the indicial form is a highly nontrivial problem. Hence, analyzing the indicial form might only be practical when determining whether a specific index exists.[4]

A more practical way to harness the power of the indicial form is to show that every index has a common divisor, called a *common index divisor*. The *field index* of a number field F summarizes all common index divisors for F, and is given by

$$i(F) = \gcd \{\operatorname{ind}(\theta) : F = \mathbb{Q}(\theta),\ \theta \in \mathcal{O}_F\}.$$

If it can be shown that an indicial form for F always has a particular prime factor, we will have that $i(F) > 1$. This is useful for eliminating the possibility of monogeneity. For its use in determining S_F, we always have that $S_F \subseteq i(F) \cdot \mathbb{N}$.

We now narrow our discussion to cubic fields, starting with an overview of some definitions and properties. Recall that a cubic field F may be classified in two ways according to the Galois group of its normal closure K over $\mathbb{Q}$. If $\operatorname{Gal}(K/\mathbb{Q}) \cong C_3$, then F is called a *cyclic cubic*. In this case, $F = K$ and is a totally real extension of $\mathbb{Q}$. If $\operatorname{Gal}(K/\mathbb{Q}) \cong S_3$, then F is called a *non-cyclic cubic*. In this case, K is a degree 6 extension of $\mathbb{Q}$ containing 3 isomorphic cubic subfields and a unique quadratic subfield L. We call L the quadratic field *associated* to F. Likewise, we say F and its conjugates are *associated* to L.

[4] A common way to do this is to use congruence conditions to obtain a contradiction with nth power residues modulo a prime.

Let $L = \mathbb{Q}(\sqrt{d})$ be any quadratic field, with $d \in \mathbb{Z}$ and squarefree. The set of all cubic fields associated to L is denoted by $C(d)$. Although $d = 1$ does not yield a quadratic field, we still denote the set of all cyclic cubics by $C(1)$ for consistency. The index results for cubic fields that are most important to us will focus on the families $C(d)$ for a given squarefree $d \in \mathbb{Z}$.

The simplest family of non-cyclic cubics is the set of *pure cubics*. This is the set of all cubic fields of the form $F = \mathbb{Q}(\sqrt[3]{ab^2})$, where $a, b \in \mathbb{N}$, squarefree, and relatively prime. Let $\theta = \sqrt[3]{ab^2}$. Since the minimal polynomial of θ over $\mathbb{Q}$ is given by $x^3 - ab^2$, the primitive cube roots of unity $\zeta_3 = \dfrac{-1 \pm \sqrt{-3}}{2}$ are contained in the normal closure of $\mathbb{Q}(\theta)$. Thus, the associated quadratic of any pure cubic is $\mathbb{Q}(\sqrt{-3})$. Conversely, we know from Kummer Theory that any cubic associated to $\mathbb{Q}(\sqrt{-3})$ must be a pure cubic. Hence, the set of all pure cubics is $C(-3)$.

An integral basis for $\mathcal{O}_F$ is given by $\{1, \theta, f(\theta)\}$, where

$$f(\theta) = \begin{cases} \theta^2/b & \text{if } a^2 \not\equiv b^2 \pmod{9}, \\ \dfrac{b + b\theta + \theta^2}{3b} & \text{if } a^2 \equiv b^2 \pmod{9}. \end{cases}$$

In the latter case, the signs of a and b are chosen so that $a \equiv b \equiv 1 \pmod{3}$. For each integral basis, a corresponding indicial form is given by

$$I_F(x, y) = \begin{cases} bx^3 - ay^3 & \text{if } a^2 \not\equiv b^2 \pmod{9}, \\ \dfrac{b(3x + y)^3 - ay^3}{9} & \text{if } a^2 \equiv b^2 \pmod{9}. \end{cases}$$

For the pure cubics, the indicial form is simple enough to provide immediate results. For instance, we can quickly deduce that $F = \mathbb{Q}(\sqrt[3]{n})$ is monogenic for any squarefree $n \not\equiv \pm 1 \pmod{9}$. Simply observe in this case that $a = n$, $b = \pm 1$, and $n^2 \not\equiv 1 \pmod{9}$, which gives $I_F(\pm 1, 0) = \pm 1$. This shows the following:

Proposition 1.4. *There exist infinitely many pure cubic fields whose ring of integers has a power basis.*

We now look at the relevant history of index results for cubic fields and then follow with a discussion of the specific index questions we aim to answer.

One of the first results came from Engstrom [4] in 1930. He determined that for any cubic field F, we have $i(F) \in \{1, 2\}$.[5] Furthermore, he determined that the exact value of $i(F)$ depends only on prime ideal factorization of (2) in $\mathcal{O}_F$:

Theorem 1.5 (Engstrom [4]). *If F is a cubic field, then $i(F) = 2$ if and only if (2) is completely split in $\mathcal{O}_F$.*

In 1937, Hall proved that the minimal index runs unbounded over the set of all pure cubics by applying congruence conditions for cubic nonresidues to an indicial form:

Theorem 1.6 (Hall, Theorem 2 [5]). *Given any integer $N > 0$, there is a pure cubic field $F = \mathbb{Q}(\sqrt[3]{ab^2})$ with $a, b \in \mathbb{N}$ relatively prime and squarefree in which every integer of F has an index greater than N.*

Dummit and Kisilevsky [3] proved an identical result in 1977 for a subfamily of the cyclic cubics, namely, the family of degree 3 subfields of cyclotomic fields of the form $F = \mathbb{Q}(\zeta_l)$, where $l \equiv 1 \pmod 3$ is any prime and ζ_l is any primitive lth root of unity. Since $\mathrm{Gal}(F/\mathbb{Q})$ is generated by $\tau : \zeta_l \to \zeta_l^g$, where g is any primitive root modulo p, F is a cyclic extension of $\mathbb{Q}$ of degree $l - 1$. Thus F has a unique subfield of degree 3 over $\mathbb{Q}$ which must be cyclic as well. The result, given below, was again proved by invoking a convenient indicial form for the above family of cyclic cubics.

[5] If $i(F) = 1$, it is not necessarily true that $\mathcal{O}_F$ contains an element of index 1; rather, there exist a pair of elements in $\mathcal{O}_F$ whose indices have no common factor. If $i(F) = 2$, then 2 divides the index of every element of $\mathcal{O}_F$ and there exists some element in $\mathcal{O}_F$ whose index is not divisible by 4.

Theorem 1.7 (Dummit-Kisilevsky, Theorem 2 [3]). *Given any $N > 0$, there exists a cubic subfield F of a prime cyclotomic field $F_l = \mathbb{Q}(\zeta)$, with $l \equiv 1 \ (mod\, 3)$ and ζ a primitive lth root of unity, such that $m(F) > N$.*

In addition, Dummit and Kisilevsky showed that there are infinitely many cyclic cubics among this family with a power basis. In 1979, Huard [6] extended this result by showing that for any $I \in \mathbb{N}$ there are infinitely many cyclic cubic fields containing an algebraic integer of index I. Hence, he proved that

$$\bigcup_{F \in C(1)} S_F = \mathbb{N}.$$

Spearman and Williams [10] showed in 2001 that, given a fixed quadratic, there are infinitely many associated cubics whose ring of integers has a power basis. This expands upon Proposition 1.4, in which the fixed quadratic is $\mathbb{Q}(\sqrt{-3})$.

In 2008, Spearman and Williams [11] took Huard's result a step further and determined which indices occur in subfamilies of $C(1)$ according to a dependence on the field index. The index sets they determined are broken down as follows:

$i(F)$	$\bigcup_{F \in C(1)} S_F$
1	$\{8^n m : n \in \mathbb{N} \cup \{0\}, m \in 2\mathbb{N} - 1\}$
2	$2\mathbb{N}$

(1)

They also showed that for each index set in the right-hand column, every element of the set is the index of an algebraic integer in infinitely many cyclic cubic fields.

In 2016, Spearman, Yang, and Yoo [12] extended Hall's result on unbounded minimal indices among the pure cubics by showing that every cubefree natural number occurs as the minimal index of infinitely many pure cubics. Using ideas similar to theirs, we can easily prove the following theorem:

Theorem 1.8. *Every natural number is the index of an algebraic integer in infinitely many pure cubics.*

Proposition 1.8 is a natural extension of Proposition 1.4. Furthermore, it immediately implies that

$$\bigcup_{F \in C(-3)} S_F = \mathbb{N}.$$

Notice the similarity of this result with Huard's result for cyclic cubics. While Theorem 1.8 includes any cubefree index, it is currently unknown whether the result of Spearman, Yang, and Yoo extends to include these as well.

The results we will prove expand upon the aforementioned index results. We have two main goals. The first is to generalize the two results of Spearman and Williams on indices in cubic fields. We will extend their result on power bases in non-cyclic cubics by showing that, given a fixed quadratic field $L = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree, and a fixed $I \in \mathbb{N}$, there are infinitely many cubic fields F associated to L whose number rings contain an algebraic integer of index I.[6] At the same time, we will generalize their result on index sets in cyclic cubics. Spearman and Williams split up the full set of indices for $C(1)$ into subsets according to the field index $i(F)$; we shall do this for each family $C(d)$. However, rather than breaking up the index sets according to a dependence on $i(F)$, we will do so according to a dependence on the factorization of the prime ideal (2) in $\mathcal{O}_F$.

Due to Theorem 1.5, the shift to a dependence on the factorization of (2) turns out to be quite natural. By the Kronecker-Weber Theorem, if F is a cyclic cubic,

[6] Accomplishing this for $I = 1$ will immediately prove the result of Spearman and Williams.

then $F \subset \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive mth root of unity, and m is the conductor of F. It is known that m is either equal to 9 or is of the form m_0 or $9m_0$, where m_0 is a product of primes of the form $3n+1$. Regardless, we have that $2 \nmid m$. Hence 2 does not ramify in $\mathbb{Q}(\zeta_m)$ and so cannot ramify in F. Therefore, since F is normal over $\mathbb{Q}$, we have that (2) is either inert in F or completely split in F. Consequently, Theorem 1.5 tells us that for a cyclic cubic F, $i(F) = 1$ and $i(F) = 2$ correspond precisely to when (2) is inert and completely split, respectively, in $\mathcal{O}_F$. In fact, the first column in Table 1, which lists the possible values of $i(F)$, may be replaced by a column listing these two possible factorizations of (2) in $\mathcal{O}_F$.

Thus, the result of Spearman and Williams on index sets for cyclic cubics can easily be reformulated in terms of a dependence on the factorization of (2) in $\mathcal{O}_F$. This lays the foundation for us to do so as well. However, there are five possible factorizations of (2) within the set of all cubic fields. For any cubic field F, it still holds that $i(F) = 2$ is equivalent to (2) being completely split in $\mathcal{O}_F$ by Theorem 1.5. Thus, it follows that if (2) is not completely split in $\mathcal{O}_F$, then we must have $i(F) = 1$. Hence, we may subdivide the case $i(F) = 1$ into four subcases, to account for the other four possible factorizations of (2) in a cubic field. As mentioned earlier, the choice of $d = 1$ reduces the number of possible factorizations in $C(d)$ to two. More generally, the choice of d will reduce the number of possible factorizations of (2) in $C(d)$ from five to one or two. For a fixed squarefree $d \in \mathbb{Z}$ and fixed possible factorization of (2) in $C(d)$, we will give the set of indices of all algebraic integers within all cubic fields in $C(d)$ with the given factorization of (2). Furthermore, like Spearman and Williams, we will show that for each index I in each index set, there are infinitely many cubic fields in $C(d)$ with the given factorization of (2) that contain an algebraic integer of index I.

Our second goal is to extend Hall's result on unbounded minimal indices in pure cubics. The families of cubics for which we extend this result will be the same as in our first goal. In particular, we fix a squarefree $d \in \mathbb{Z}$ and show that the minimal indices run unbounded over the set of all cubics in $C(d)$. Hall proved this for the pure cubics, which corresponds to the case $d = -3$. Dummit and Kisilevsky proved the cyclic cubic case of $d = 1$. Rather than reprove these, we exclude the cases $d = -3, 1$ from our proof. The structure of our argument will loosely follow the main ideas employed by Hall to prove Theorem 1.6, as well as those used by Dummit and Kisilevsky to prove Theorem 1.7.

2 Sets of Indices

In this chapter, we will work towards proving the first of our two main results. Given a squarefree $d \in \mathbb{Z}$, we will determine the set of all natural numbers that are indices of algebraic integers in the set of all cubic fields in $C(d)$ with a given factorization of the prime ideal (2). Furthermore, we will show that each element of each index set is an index in infinitely many such cubic fields. When $d \neq 1$, this amounts to fixing a quadratic field and determining indices of integers within subsets of the set of all associated cubics. When $d = 1$, this amounts to determining indices of integers within subsets of the set of all cyclic cubics.

2.1 Indices and Discriminants

The proof of our result requires the construction of infinitely many cubic fields in $C(d)$ for a given squarefree $d \in \mathbb{Z}$. To ensure that any such cubic field F is an element of $C(d)$ requires some condition on F relating it to d. Given a quadratic field $L = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree, we know that any non-cyclic cubic field whose discriminant has squarefree part equal to d will be associated to L. We also know that any cubic field whose discriminant is a perfect square (so that its squarefree part is $d = 1$), is a cyclic cubic field. The following proposition summarizes these relationships:

Proposition 2.1. *Let $d \in \mathbb{Z}$ be squarefree. Then $F \in C(d)$ if and only if $\Delta_F = dn^2$ for some $n \in \mathbb{N}$.*

We obtain our cubic fields by constructing irreducible cubic polynomials $f(x) \in \mathbb{Z}[x]$ whose roots are algebraic integers of the desired indices. As we will see below, by constructing $f(x)$ carefully, we can compute both $\operatorname{disc}(f(x))$ and Δ_F to produce a desired index. We do this by applying Proposition 1.2, which gives

$$\text{disc}(f(x)) = (\text{ind}(\theta))^2\Delta_F$$

for any root θ of $f(x)$. This leads to the following corollary of Proposition 2.1:

Corollary 2.1.1. *Suppose $d \in \mathbb{Z}$ is squarefree, $f(x) \in \mathbb{Z}[x]$ is a monic cubic polynomial irreducible over $\mathbb{Q}$, θ is a root of $f(x)$, and $F = \mathbb{Q}(\theta)$. Then $F \in C(d)$ if and only if disc$(f(x)) = dn^2$ for some $n \in \mathbb{N}$.*

To assist with the construction of our generating polynomials $f(x)$, we employ some important simplifications.

Suppose $F = \mathbb{Q}(\theta)$ is a cubic field, with $\theta \in \mathcal{O}_F$. Let $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$ be the minimal polynomial of θ over $\mathbb{Q}$. By a simple change of basis over $\mathbb{Q}$, we also have that $F = \mathbb{Q}(3\theta + a)$ where $3\theta + a \in \mathcal{O}_F$. Since $3\theta + a$ is a root of

$$\begin{aligned} g(x) &= 27 \cdot f\left(\frac{x-a}{3}\right) \\ &= (x-a)^3 + 3a(x-a)^2 + 9b(x-a) + 27c \\ &= x^3 - (3a^2 - 9b)x + (2a^3 - 9ab + 27c) \in \mathbb{Z}[x] \end{aligned}$$

and generates F, we have that $g(x)$ is the minimal polynomial of $3\theta + a$ over $\mathbb{Q}$. Thus, there exists $\theta \in \mathcal{O}_F$ which generates F and has minimal polynomial of the form $x^3 - Ax + B \in \mathbb{Z}[x]$.

By a tedious manipulation of the roots, we have disc$(x^3 - Ax + B) = 4A^3 - 27B^2$. As a result, Proposition 1.2 gives

$$4A^3 - 27B^2 = (\text{ind}(\theta))^2\Delta_F$$

for any cubic field $F = \mathbb{Q}(\theta)$, where θ is a root of an irreducible polynomial of the form $x^3 - Ax + B \in \mathbb{Z}[x]$.

For any prime p and $n \in \mathbb{Z}$ with $n \neq 0$, write $n = p^k m$ where $k \in \mathbb{Z}_{\geq 0}$, $m \in \mathbb{Z}$ and $p \nmid m$. The *p-adic valuation* $v_p : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ is given by $v_p(n) = k$. For consistency, we define $v_p(0) = \infty$.

Suppose $F = \mathbb{Q}(\theta)$ is a cubic field and θ is a root of $x^3 - Ax + B \in \mathbb{Z}[x]$. Let p be any prime in which $v_p(A) \geq 2$ and $v_p(B) \geq 3$. Then we may write $v_p(A) = 2i + i'$ and $v_p(B) = 3j + j'$, where $i, j \geq 1$, $i' \in \{0, 1\}$, and $j' \in \{0, 1, 2\}$. Let $m = \min\{i, j\}$. Then θ/p^m is a root of $x^3 - (A/p^{2m})x + B/p^{3m} \in \mathbb{Z}[x]$. Thus $F = \mathbb{Q}(\theta/p^m)$ with $\theta/p^m \in \mathcal{O}_F$. Moreover, by construction we have $v_p(A/p^{2m}) < 2$ or $v_p(B/p^{3m}) < 3$. Therefore, any cubic field F may be generated by a polynomial of the form $f(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where $v_p(A) < 2$ or $v_p(B) < 3$ for all primes p.[7]

To compute $\operatorname{ind}(\theta)$ by using Proposition 1.2 also requires knowing the value of Δ_F for the constructed cubic field F. Llorente and Nart show that Δ_F may be computed exclusively in terms of the coefficients A and B of $f(x)$. As they do, we define

$$\begin{aligned} s_p &= v_p(4A^3 - 27B^2), \\ \Delta_p &= (4A^3 - 27B^2)/p^{s_p} \end{aligned}$$

for any prime p. Their result is given below.

[7] In order for F to be a cubic field, $f(x)$ must be irreducible over $\mathbb{Q}$. Hence, we can never have $B = 0$. In the event that $A = 0$, we have $v_p(A) = \infty > 2$, which will be useful in subsequent theorems.

Theorem 2.2 (Llorente-Nart, Theorem 2 [7])**.** *Let A and B be integers such that the cubic polynomial $x^3 - Ax + B$ is irreducible over $\mathbb{Q}$, and such that either $v_p(A) < 2$ or $v_p(B) < 3$ for all primes p. Let θ be a root of $x^3 - Ax + B$ and set $F = \mathbb{Q}(\theta)$ so that $[F : \mathbb{Q}] = 3$. Then the discriminant of the cubic field F is given by*

$$\Delta_F = sign(4A^3 - 27B^2)2^\alpha 3^\beta \prod_{\substack{p>3 \\ s_p \equiv 1 \ (mod\, 2)}} p \prod_{\substack{p>3 \\ 1 \le v_p(B) \le v_p(A)}} p^2,$$

where

$$\alpha = \begin{cases} 3 & if\, s_2 \equiv 1 \ (mod\, 2), \\ 2 & if\, 1 \le v_2(B) \le v_2(A), \\ & or\, s_2 \equiv 0 \ (mod\, 2) \ and\ \Delta_2 \equiv 3 \ (mod\, 4), \\ 0 & otherwise, \end{cases}$$

$$\beta = \begin{cases} 5 & if\, 1 \le v_3(B) < v_3(A), \\ 4 & if\, v_3(A) = v_3(B) = 2, \\ & or\ A \equiv 3 \ (mod\, 9), 3 \nmid B, B^2 \not\equiv 4 \ (mod\, 9), \\ 3 & if\, v_3(A) = v_3(B) = 1, \\ & or\ 3 \mid A, 3 \nmid B, A \not\equiv 3 \ (mod\, 9), B^2 \not\equiv A+1 \ (mod\, 9), \\ & or\ A \equiv 3 \ (mod\, 9), B^2 \equiv 4 \ (mod\, 9), B^2 \not\equiv A+1 \ (mod\, 27), \\ 1 & if\, 1 = v_3(A) < v_3(B), \\ & or\ 3 \mid A, A \not\equiv 3 \ (mod\, 9), B^2 \equiv A+1 \ (mod\, 9), \\ & or\ A \equiv 3 \ (mod\, 9), B^2 \equiv A+1 \ (mod\, 27), s_3 \equiv 1 \ (mod\, 2), \\ 0 & if\, 3 \nmid A \\ & or\ A \equiv 3 \ (mod\, 9), B^2 \equiv A+1 \ (mod\, 27), s_3 \equiv 0 \ (mod\, 2), \end{cases}$$

With some effort, the reader will notice that any values of $A, B \in \mathbb{Z}$ satisfying the hypothesis of the Theorem 2.2, will fall under one of the several cases for the value of α (and similarly for the value of β).

The proof of Theorem 2.2 invokes facts about the factorizations of rational primes p into prime ideals in $\mathcal{O}_F$. This is because the value of Δ_F is derived from the ramification indices of prime $\mathcal{O}_F$-ideals. Indeed, $p \mid \Delta_F$ if and only if p is ramified in $\mathcal{O}_F$. The different ideal allows us to say more.

Let $\mathcal{D}_{F/\mathbb{Q}}$ denote the different of F over $\mathbb{Q}$. Let $\mathcal{I}_{\mathcal{O}_F}$ be the multiplicative group of all fractional $\mathcal{O}_F$-ideals. If $N : \mathcal{I}_{\mathcal{O}_F} \to \mathbb{Z}$ is the ideal norm from F over $\mathbb{Q}$, then

$$N(\mathcal{D}_{F/\mathbb{Q}}) = \Delta_F.$$

If $\mathcal{P}$ is an $\mathcal{O}_F$-ideal with ramification index $e_{\mathcal{P}}$, then $v_{\mathcal{P}}(\mathcal{D}_{F/\mathbb{Q}}) \geq e_{\mathcal{P}} - 1$. Let p be a prime and suppose $\mathcal{P}$ is above p. Then p is said to be *wildly ramified* at $\mathcal{P}$ if $p \mid e_{\mathcal{P}}$. Otherwise, p is said to be *tamely ramified* at $\mathcal{P}$. If p is tamely ramified at $\mathcal{P}$, then $v_{\mathcal{P}}(\mathcal{D}_{F/\mathbb{Q}}) = e_{\mathcal{P}} - 1$. However, if p is wildly ramified at $\mathcal{P}$, then $v_{\mathcal{P}}(\mathcal{D}_{F/\mathbb{Q}}) \geq e_{\mathcal{P}}$.

Since F is a cubic field, the prime ideal factorization of any rational prime in $\mathcal{O}_F$ has factors with ramification indices lying within the set $\{1, 2, 3\}$. Hence 2 and 3 are the only primes that are potentially wildly ramified in $\mathcal{O}_F$. Thus, 2 and 3 are the only factors of Δ_F whose powers may be greater than 2. This is why they are given special attention in the computation of Δ_F in Theorem 2.2. Hence, they will be given special attention in our results as well.

For us, the main consequence of Theorem 2.2 is that the index of any algebraic integer with minimal polynomial of the form $f(x) = x^3 - Ax + B$, where $v_p(A) < 2$ and $v_p(B) < 3$ for all primes p, may be computed with knowledge of the values of A and B alone. This narrows our task to selecting appropriate $A, B \in \mathbb{Z}$ so that

$f(x)$ is irreducible over $\mathbb{Q}$ and so that, by applying Proposition 1.2, a desired index is produced.

2.2 The Factorization of (2) in a Cubic Field

Since the index sets we obtain will depend on the factorization of the prime ideal (2) in $\mathcal{O}_F$, we need to determine conditions on d under which each factorization occurs in a given $C(d)$. We can do this based on congruence classes of d modulo 8.

We mentioned in the introduction that (2) is either inert or completely split in the case that $d = 1$, so we will focus below on the non-cyclic cubic cases. These are precisely the cases in which the cubics in $C(d)$ have associated quadratics; we will take advantage of this fact to determine our factorizations.

Throughout, our notation for prime ideal factorizations is as follows: the inertia degree of a prime is its subscript, the ramification index is its superscript, and distinct prime ideals are distinguished by apostrophes. For any prime p, there are five possible prime ideal factorizations of (p) in a cubic field: $\mathcal{Q}_1^2\mathcal{Q}_1'$, $\mathcal{Q}_1^3$, $\mathcal{Q}_1\mathcal{Q}_2$, $\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''$, and $\mathcal{Q}_3$. There are three possible factorizations of (p) in a quadratic field: $\mathcal{P}_1^2$, $\mathcal{P}_2$, and $\mathcal{P}_1\mathcal{P}_1'$.

By knowing the factorization of (2) in a given quadratic field, we will be able to deduce the possible factorizations of (2) in the family of all associated cubics. Criteria for the factorization of (2) in a quadratic field is well-known and given below.

Proposition 2.3. *Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \in \mathbb{Z}$ squarefree. Then*

$$(2)\mathcal{O}_L = \begin{cases} \mathcal{P}_1^2 & \textit{if } d \equiv 2,\ 3\ (\textit{mod}\ 4), \\ \mathcal{P}_2 & \textit{if } d \equiv 5\ (\textit{mod}\ 8), \\ \mathcal{P}_1\mathcal{P}_1' & \textit{if } d \equiv 1\ (\textit{mod}\ 8). \end{cases}$$

Proof. Apply Dedekind's factorization criteria by factoring the polynomial

$$f(x) = \begin{cases} x^2 - d & \text{if } d \equiv 2,\ 3 \pmod 4, \\ x^2 - x - \dfrac{1-d}{4} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

over $\mathbb{F}_2$. We are able to do this because $f(x)$ is the minimal polynomial of $\theta = \sqrt{d}$ and $\theta = \dfrac{1+\sqrt{d}}{2}$ over $\mathbb{Q}$, respectively, and $2 \nmid \operatorname{ind}(\theta)$ in either case. □

To obtain a similar criteria for factorizations of (2) in cubic fields, we need another result from Llorente and Nart.

Theorem 2.4 (Llorente-Nart, Theorem 1 [7])**.** *Let F be a cubic field. If $F = \mathbb{Q}(\theta)$ where $\theta \in \mathcal{O}_F$ has minimal polynomial over $\mathbb{Q}$ given by $f(x) = x^3 - Ax + B \in \mathbb{Z}[x]$ and $v_2(A) < 2$ or $v_2(B) < 3$, then the factorization of (2) in $\mathcal{O}_F$ is dependent on A and B, and is given as follows:*

$$(2)\mathcal{O}_F = \begin{cases} \mathcal{Q}_1^2\mathcal{Q}_1' & \textit{if } 1 = v_2(A) < v_2(B), \\ & \textit{or, } A \textit{ odd, } B \textit{ even, and } s_2 \textit{ odd,} \\ & \textit{or, } A \textit{ odd, } B \textit{ even, } s_2 \textit{ even, and } \Delta_2 \equiv 3 \ (\textit{mod } 4), \\ \mathcal{Q}_1^3 & \textit{iff } 1 \le v_2(B) \le v_2(A), \\ \mathcal{Q}_1\mathcal{Q}_2 & \textit{if } A \textit{ even and } B \textit{ odd,} \\ & \textit{or, } A \textit{ odd, } B \textit{ even, } s_2 \textit{ even, and } \Delta_2 \equiv 5 \ (\textit{mod } 8), \\ \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1'' & \textit{iff } A \textit{ odd, } B \textit{ even, } s_2 \textit{ even, and } \Delta_2 \equiv 1 \ (\textit{mod } 8), \\ \mathcal{Q}_3 & \textit{iff } A \textit{ odd and } B \textit{ odd.} \end{cases}$$

Unsurprisingly, Theorem 2.4 (along with a similar theorem for the prime 3 and the primes $p > 3$) is used by Llorente and Nart to prove Theorem 2.2. However, we will use it as a lemma to obtain congruence conditions on d for the way in which (2) factors in any cubic in $C(d)$. For each congruence condition on d, we will have one or two possible factorizations of (2) in $C(d)$. When we determine the index set for a given d and possible factorization of (2), we will refer back to Theorem 2.4 to directly verify that the factorization of (2) is achieved within the infinitely many $F \in C(d)$ we construct by investigating the coefficients of their generating polynomials.

For any prime p, we now determine the possible factorizations of the prime ideal (p) in $\mathcal{O}_F$. We will first describe these possible factorizations in terms of a dependence on the factorization of (p) in $\mathbb{Q}(\sqrt{d})$. We will then deduce the desired dependence on d for the specific case of $p = 2$.

Proposition 2.5. *Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \in \mathbb{Z}$ squarefree, let $F \in C(d)$, and let p be any prime. Then, given a factorization of (p) in $\mathcal{O}_L$, the possible factorizations of (p) in $\mathcal{O}_F$ are given as follows:*

$$(p)\mathcal{O}_F = \begin{cases} \mathcal{Q}_1^3 \text{ or } \mathcal{Q}_1^2\mathcal{Q}_1' & \text{if } (p)\mathcal{O}_L = \mathcal{P}_1^2, \\ \mathcal{Q}_1^3 \text{ or } \mathcal{Q}_1\mathcal{Q}_2 & \text{if } (p)\mathcal{O}_L = \mathcal{P}_2. \\ \mathcal{Q}_1^3,\ \mathcal{Q}_3, \text{ or } \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1'' & \text{if } (p)\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_1', \end{cases}$$

Proof. We naturally divide this proof into 3 cases, based on the factorization of (p) in $\mathcal{O}_L$. In each case, we eliminate the factorizations of (p) that are not possible in $\mathcal{O}_F$. We repeatedly use the fact that the compositum field $K = FL$ is Galois over $\mathbb{Q}$.

Case 1: $(p)\mathcal{O}_L = \mathcal{P}_1^2$.

Since (p) ramifies in $\mathcal{O}_L$, (p) also ramifies in $\mathcal{O}_K$. But K is the smallest extension of F that is normal over $\mathbb{Q}$. So, if F_1, F_2, and F_3 are the cubic fields conjugate to F, where $F = F_1$, then $K = F_1F_2F_3$. Therefore (p) must also ramify in $\mathcal{O}_F$. Thus, the only possible factorizations of (p) in $\mathcal{O}_F$ are $\mathcal{Q}_1^3$ and $\mathcal{Q}_1^2\mathcal{Q}_1'$.

Case 2: $(p)\mathcal{O}_L = \mathcal{P}_2$.

If $(p)\mathcal{O}_F = \mathcal{Q}_3$, then $(p)\mathcal{O}_K = \mathcal{R}_6$. Therefore, generated by the Frobenius element, the decomposition group $\mathcal{D}_{\mathcal{R}_6}(K/\mathbb{Q}) \cong C_6$. However, $\mathcal{D}_{\mathcal{R}_6}(K/\mathbb{Q}) \subset \mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, which has no cyclic subgroup of order 6.

If $(p)\mathcal{O}_F = \mathcal{Q}_1^2\mathcal{Q}_1'$, then every prime ideal in $\mathcal{O}_K$ above p must ramify, with all ramification indices equal and divisible by 2. Thus, the only possible factorization of (p) in $\mathcal{O}_K$ is given by $(p)\mathcal{O}_K = \mathcal{R}_1^2(\mathcal{R}_1')^2(\mathcal{R}_1'')^2$. But since $(p)\mathcal{O}_L = \mathcal{P}_2$, every prime ideal in $\mathcal{O}_K$ above p must have an inertia degree of at least 2, a contradiction.

If $(p)\mathcal{O}_F = \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''$, then (p) is completely split in each cubic field F_i conjugate to F. But since (p) is completely split in each F_i if and only if (p) is completely split in $K = F_1F_2F_3$, this contradicts that $(p)\mathcal{O}_L = \mathcal{P}_2$.

This leaves $\mathcal{Q}_1\mathcal{Q}_2$ or $\mathcal{Q}_1^3$ as the only possible factorizations of (p) in $\mathcal{O}_F$.

Case 3: $(p)\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_1'$.

If $(p)\mathcal{O}_F = \mathcal{Q}_1^2\mathcal{Q}_1'$, then we must have that $(p)\mathcal{O}_K = \mathcal{R}_1^2(\mathcal{R}_1')^2(\mathcal{R}_1'')^2$, as in case 2. But since $(p)\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_1'$ and K/L is Galois, both $\mathcal{P}_1$ and $\mathcal{P}_1'$ are either inert, totally ramified, or completely split in $\mathcal{O}_K$, which is impossible.

If $(p)\mathcal{O}_F = \mathcal{Q}_1\mathcal{Q}_2$, then every prime ideal in $\mathcal{O}_K$ above p must have an inertia degree of 2. Thus, the only possible factorization of (p) in $\mathcal{O}_K$ is given by $(p)\mathcal{O}_K = \mathcal{R}_2\mathcal{R}_2'\mathcal{R}_2''$. But this is again incompatible with $(p)\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_1'$.

This leaves $\mathcal{Q}_1^3$, $\mathcal{Q}_3$, or $\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''$ as the only possible factorizations of (p) in $\mathcal{O}_F$. □

In particular, Proposition 2.5 holds for $p = 2$. We now pass over to congruence classes of d modulo 8 to give the desired result.

Corollary 2.5.1. *Given $d \in \mathbb{Z}$ squarefree, let $F \in C(d)$. Then the possible factorizations of (2) in $\mathcal{O}_F$ are given as follows:*

$$(2)\mathcal{O}_F = \begin{cases} \mathcal{Q}_1^2\mathcal{Q}_1' & \textit{if } d \equiv 2,\ 3\ (\textit{mod}\ 4), \\ \mathcal{Q}_1^3 \textit{ or } \mathcal{Q}_1\mathcal{Q}_2 & \textit{if } d \equiv 5\ (\textit{mod}\ 8), \\ \mathcal{Q}_3, \textit{ or } \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1'' & \textit{if } d \equiv 1\ (\textit{mod}\ 8). \end{cases}$$

Proof. If $d = 1$, we mentioned before that (2) is either inert or completely split. Now assume $d \neq 1$, so that F is associated to the quadratic field $L = \mathbb{Q}(\sqrt{d})$. Suppose $F = \mathbb{Q}(\theta)$ where $\theta \in \mathcal{O}_F$ and has minimal polynomial over $\mathbb{Q}$ given by $f(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, with $v_p(A) < 2$ or $v_p(B) < 3$ for all primes p. Suppose also that $(2)\mathcal{O}_L = \mathcal{Q}_1^3$. Then by Theorem 2.4, we have that $1 \leq v_2(B) \leq v_2(A)$. Therefore $2^{2v_2(B)} \parallel 4A^3 - 27B^2$. Hence

$$\begin{aligned} \Delta_2 &= (4A^3 - 27B^2)/2^{2v_2(B)} \\ &= 4A^3/2^{2v_2(B)} - 27(B/2^{v_2(B)})^2 \\ &\equiv -27(B/2^{v_2(B)})^2 \\ &\equiv 5 \text{ (mod 8)}. \end{aligned}$$

On the other hand, by Proposition 2.1 we have $\Delta_F = dn^2$ for some $n \in \mathbb{N}$. Since $2 \mid v_2(4A^3 - 27B^2)$ and

$$dn^2 = \Delta_F = \frac{4A^3 - 27B^2}{(\mathrm{ind}(\theta))^2},$$

it follows that d is odd. Thus

$$\Delta_2 = d(n/2^{v_2(n)})^2 \equiv d \text{ (mod 8)},$$

which implies that $d \equiv \Delta_2 \equiv 5 \pmod 8$. Hence, by combining Proposition 2.3 and Proposition 2.5, the result follows. $\square$

When we say we have found the possible factorizations of (2) in $\mathcal{O}_F$, this leaves open the possibility that for each congruence class of d modulo 8 we may be able to rule out more factorizations than we do. However, we will see that this is not the case when we prove the main theorem, for we will give explicit examples of cubics in $C(d)$ for a given d, in which each of the above possible factorizations of (2) occur.

Observe that for a given congruence class of d modulo 8, some factorizations of (2) are not possible in $C(d)$. In fact, the sets of possible factorizations of (2) are pairwise disjoint with respect to the three cases. Hence, by picking a factorization of (2), the congruence class of d will be uniquely determined. However, since we must apply Theorem 2.4 to determine whether a desired factorization is achieved in a given cubic field, knowing the congruence class of d must be established first in order to prove the main theorem. Thus, we will think of the choice of a factorization of (2) as the choice to narrow the family $C(d)$ to a particular subfamily.

2.3 Some Lemmas

Let $\mathcal{A} = \{\mathcal{Q}_1^2\mathcal{Q}_1', \mathcal{Q}_1^3, \mathcal{Q}_1\mathcal{Q}_2, \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1'', \mathcal{Q}_3\}$. For each squarefree $d \in \mathbb{Z}$ and factorization $\mathcal{J} \in \mathcal{A}$ of (2), we define

$$C(d, \mathcal{J}) := \{F \in C(d) : (2)\mathcal{O}_F = \mathcal{J}\}.$$

Notice that $C(d, \mathcal{J}) \subseteq C(d)$ for each possible factorization $\mathcal{J}$ of (2) in $C(d)$. If $\mathcal{J}$ is not a possible factorization of (2) in $C(d)$, we simply have that $C(d, \mathcal{J}) = \varnothing$. The cubic fields we construct to obtain our index sets will be partitioned into these families. We define

$$S_{d,\mathcal{J}} := \bigcup_{F \in C(d,\mathcal{J})} S_F$$

to be the desired index sets for each family $C(d, \mathcal{J})$.

We obtain the index sets $S_{d,\mathcal{J}}$ for each squarefree $d \in \mathbb{Z}$ and $\mathcal{J} \in \mathcal{A}$ by introducing candidate subsets of $\mathbb{N}$. We show these candidates are, in fact, equivalent to the index sets by double containment. We first show that the index sets are contained within these candidate sets by showing that there exist restrictions on the possible indices in each case. Then, in the proof of the main result, we show that each of these candidate sets is contained within its respective index set. For instance, by Theorem 1.5, we already know that $S_{d,\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''} \subseteq 2\mathbb{N}$. We will show that $S_{d,\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''} = 2\mathbb{N}$ in the proof of the main result.

We will provide the restrictions on each index set as lemmas to be used in the main theorem. But first, we need a result on polynomial discriminants.

Proposition 2.6. *Let $f(x), g(x) \in \mathbb{Z}[x]$ are polynomials of degree n. Suppose that $g(x) = \dfrac{f(ax+b)}{c}$, where $a, b, c \in \mathbb{Z}$ and $a, c \neq 0$. Then*

$$disc(g(x)) = \frac{a^{n(n-1)}}{c^{2n-2}} disc(f(x)).$$

Proof. For each $i \in \{1, ..., n\}$, let $\alpha_i \in \mathbb{C}$ be the roots of $f(x)$. Write

$$f(x) = d \cdot \prod_{i=1}^{n} (x - \alpha_i),$$

where $d \in \mathbb{Z}$. Then

$$g(x) = \frac{f(ax+b)}{c} = \frac{d}{c} \cdot \prod_{i=1}^{n} (ax + b - \alpha_i) = \frac{da^n}{c} \cdot \prod_{i=1}^{n} \left(x - \frac{\alpha_i - b}{a} \right).$$

Then, by the definition of polynomial discriminant, we have that

$$\begin{aligned} \operatorname{disc}(g(x)) &= \left(\frac{da^n}{c}\right)^{2n-2} \prod_{1 \le i < j \le n} \left(\frac{\alpha_i - b}{a} - \frac{\alpha_j - b}{a}\right)^2 \\ &= \left(\frac{d^{2n-2} a^{n(2n-2)}}{c^{2n-2}}\right) \frac{1}{a^{n(n-1)}} \cdot \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= \frac{a^{n(n-1)}}{c^{2n-2}} \operatorname{disc}(f(x)). \end{aligned}$$

□

The following corollary will be used repeatedly.

Corollary 2.6.1. *Let $f(x), g(x) \in \mathbb{Z}[x]$ be cubic polynomials irreducible over $\mathbb{Q}$ such that $f(x) = 27g\left(\frac{x-v}{3}\right)$ for some $v \in \mathbb{Z}$. Then*

$$disc(f(x)) = 3^6 disc(g(x)).$$

Proof. Observe that $g(x) = \frac{f(3x+v)}{27}$. Thus using $a = 3$, $c = 27$ and $n = 3$, we may apply Lemma 2.6 to obtain the result. □

We now give the lemmas which provide restrictions on the contents of our index sets.

Lemma 2.7. *Let F be a cubic field such that $(2)\mathcal{O}_F = \mathcal{Q}_3$. Let $\theta \in \mathcal{O}_F$. If $2 \mid ind(\theta)$, then $\frac{\theta + k}{2} \in \mathcal{O}_F$ for some $k \in \mathbb{Z}$.*

Proof. The proof is similar to that of Lemma 2.2 of Spearman and Williams [11]. We saw earlier that if θ is a root of $g(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, then $3\theta + a$

is a root of $f(x) = x^3 - Ax + B$, where $A = 3a^2 - 9b$, $B = 2a^2 - 9ab + 27c$, and $f(x) = 3^3 g\left(\frac{x-a}{3}\right)$. Then by Corollary 2.6.1, we have

$$4A^3 - 27B^2 = \text{disc}(f(x)) = 3^6\text{disc}(g(x)).$$

Since $\text{disc}(g(x)) = (\text{ind}(\theta))^2\Delta_F$ and $2 \mid \text{ind}(\theta)$, we have that $2 \mid \text{disc}(g(x))$. Therefore $2 \mid 4A^3 - 27B^2$, so that B is even. But since $(2)\mathcal{O}_K = \mathcal{Q}_3$, we have by Theorem 2.4 that if $v_2(A) < 2$ or $v_2(B) < 3$, then A and B are both odd. So since B is even, we must have that $v_2(A) \geq 2$ and $v_2(B) \geq 3$. Thus $\frac{3\theta + a}{2}$ is a root of $x^3 - (A/4)x + B/8 \in \mathbb{Z}[x]$, so that $\frac{3\theta + a}{2} \in \mathcal{O}_F$. So $\frac{\theta + a}{2} = \frac{3\theta + a}{2} - \theta \in \mathcal{O}_F$. □

Lemma 2.8. *Let F be a cubic field such that $(2)\mathcal{O}_F = \mathcal{Q}_3$. If $F = \mathbb{Q}(\theta)$ for some $\theta \in \mathcal{O}_F$, then ind$(\theta) = 2^t n$ with $t \in \mathbb{Z}_{\geq 0}$, $t \equiv 0 \ (mod\, 3)$, and $n \in 2\mathbb{N} - 1$.*

Proof. This proof closely follows that of Lemma 2.3 of Spearman and Williams [11]. Suppose for contradiction there exists $\theta \in \mathcal{O}_F$ such that $F = \mathbb{Q}(\theta)$, $2^t \parallel \text{ind}(\theta)$ for some $t \in \mathbb{N}$, and $t \not\equiv 0 \pmod 3$. Let $t^* \in \mathbb{N}$ be smallest such t, corresponding to $\theta^* \in \mathcal{O}_F$. Since $t^* \not\equiv 0 \pmod 3$, then $2 \mid \text{ind}(\theta^*)$. Thus, by Lemma 2.7, $\frac{\theta^* + k}{2} \in \mathcal{O}_F$ for some $k \in \mathbb{Z}$. Then by Proposition 1.3, we have $2^{t^*-3} \parallel \text{ind}\left(\frac{\theta^* + k}{2}\right)$ with $t^* - 3 \not\equiv 0 \pmod 3$, so that $t^* - 3 > 0$. But this contradicts the minimality of t^*. □

Lemma 2.9. *Let F be a cubic field such that $(2)\mathcal{O}_F = \mathcal{Q}_1^3$. Let $\theta \in \mathcal{O}_F$. If $4 \mid$ ind(θ), then $\frac{\theta + k}{2} \in \mathcal{O}_F$ for some $k \in \mathbb{Z}$.*

Proof. Again, if θ is a root of $g(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, then $3\theta + a$ is a root of $f(x) = x^3 - Ax + B$ where $A = 3a^2 - 9b$ and $B = 2a^2 - 9ab + 27c$. Suppose that $v_2(A) < 2$ or $v_2(B) < 3$. Then since $(2)\mathcal{O}_F = \mathcal{Q}_1^3$, we have by Theorem 2.4 that $1 \leq v_2(B) \leq v_2(A)$. Note by Theorem 2.2, this gives that $4 \parallel \Delta_F$. We have two cases.

Case 1: Suppose $v_2(B) = 1$. Then $4A^3 - 27B^2 = 4(A^3 - 27(B/2)^2)$, where

$$A^3 - 27(B/2)^2 \equiv 1 \text{ (mod 2)}.$$

Thus $4 \parallel 4A^3 - 27B^2 = \text{ind}(\theta)^2\Delta_F$, so that $2 \nmid \text{ind}(\theta)$, a contradiction.

Case 2: Suppose $v_2(B) = 2$. Then $4A^3 - 27B^2 = 16(2(A/2)^3 - 27(B/4)^2)$, where

$$2(A/2)^3 - 27(B/4)^2 \equiv 1 \text{ (mod 2)}.$$

Thus $16 \parallel 4A^3 - 27B^2 = \text{ind}(\theta)^2\Delta_F$, so that $2 \parallel \text{ind}(\theta)$, a contradiction.

So $v_2(A) \geq 2$ and $v_2(B) \geq 3$. Thus, $\dfrac{3\theta + a}{2}$ is a root of $x^3 - (A/4)x + B/8 \in \mathbb{Z}[x]$, so that $\dfrac{3\theta + a}{2} \in \mathcal{O}_F$. Therefore, $\dfrac{\theta + a}{2} = \dfrac{3\theta + a}{2} - \theta \in \mathcal{O}_F$. □

Lemma 2.10. *Let F be a cubic field such that $(2)\mathcal{O}_F = \mathcal{Q}_1^3$. If $F = \mathbb{Q}(\theta)$ for some $\theta \in \mathcal{O}_F$, then ind$(\theta) = 2^t n$ with $t \in \mathbb{Z}_{\geq 0}$, $t \not\equiv 2$ (mod 3), and n odd.*

Proof. The proof is similar to that of Lemma 2.8. Suppose for contradiction there exists some $\theta \in \mathcal{O}_F$ such that $F = \mathbb{Q}(\theta)$, $2^t \parallel \text{ind}(\theta)$ for some $t \in \mathbb{N}$, and $t \equiv 2$ (mod 3). Let $t^* \in \mathbb{N}$ be the smallest such t, corresponding to $\theta^* \in \mathcal{O}_F$. Since $t^* \equiv 2$ (mod 3), then $4 \mid \text{ind}(\theta^*)$. Thus, by Lemma 2.9, $\dfrac{\theta^* + k}{2} \in \mathcal{O}_F$ for some $k \in \mathbb{Z}$. Then by Proposition 1.3, we have $2^{t^*-3} \parallel \text{ind}\left(\dfrac{\theta^* + k}{2}\right)$ with $t^* - 3 \equiv 2$ (mod 3), so that $t^* - 3 > 0$. But this contradicts the minimality of t^*. □

It is immediate from Lemma 2.8 that

$$S_{d,\mathcal{Q}_3} \subseteq \{8^n m : n \in \mathbb{Z}_{\geq 0},\ m \in 2\mathbb{N} - 1\}$$

for any $d \equiv 1 \pmod 8$. Likewise, we have from Lemma 2.10 that

$$S_{d,\mathcal{Q}_1^3} \subseteq \{8^n m : n \in \mathbb{Z}_{\geq 0},\ m \in 2\mathbb{N}-1\} \cup \{2 \cdot 8^n m : n \in \mathbb{Z}_{\geq 0},\ m \in 2\mathbb{N}-1\}$$

for any $d \equiv 5 \pmod 8$. For shorthand, we will denote these two sets by $8^n\,(2\mathbb{N}-1)$ and $8^n\,(2\mathbb{N}-1) \cup 2 \cdot 8^n\,(2\mathbb{N}-1)$, respectively.

The following two lemmas will also be used repeatedly in the proof of the main result.

Lemma 2.11. *If $v \not\equiv 0$ (mod 3), then $3v^2+1 \equiv 4v^6$ (mod 27).*

Proof. Write $v = 3w \pm 1$ for some $w \in \mathbb{Z}$. Then by the binomial theorem we have

$$4(3w \pm 1)^6 - 3(3w \pm 1)^2 - 1 \equiv (4 \pm 72w) - (3 \pm 18w) - 1 \equiv 0 \pmod{27}.$$

□

Lemma 2.12. *If $p(x) = x^3 - Ax + B \in \mathbb{Z}[x]$ and $q(x) = \dfrac{p(3x+v)}{27}$ for some $v \in \mathbb{Z}$, then*

$$q(x) = x^3 + vx^2 + \left(\frac{3v^2 - A}{9}\right) + \left(\frac{v^3 - Av + B}{27}\right).$$

Proof. Observe

$$\begin{aligned} q(x) &= \frac{(3x+v)^3 - A(3x+v) + B}{27} \\ &= \frac{27x^3 + 27vx^2 + 9v^2x + v^3 - 3Ax - Av + B}{27} \\ &= x^3 + vx^2 + \left(\frac{3v^2 - A}{9}\right)x + \left(\frac{v^3 - Av + B}{27}\right), \end{aligned}$$

as desired. □

Lastly, we shall generalize a result from Silvester, Spearman, and Williams [9] on squarefree values of quadratic polynomials. We will use this result not only for the main result in this chapter, but also for the main result in the next. In this chapter, it will provide us with the ability to construct infinitely many cubic fields in $C(d, \mathcal{J})$, for a given d and $\mathcal{J}$, that possess an algebraic integer of index I for all $I \in S_{d,\mathcal{J}}$. We will use a result from Nagel:

Theorem 2.13 (Nagel [8]). *Let $F(x) \in \mathbb{Z}[x]$ be a primitive quadratic polynomial with disc$(F(x)) \neq 0$. Then there exist infinitely many $v \in \mathbb{N}$ such that $F(v)$ is squarefree.*

The generalized result is given below.

Theorem 2.14. *Let $F(x) \in \mathbb{Z}[x]$ be a primitive quadratic polynomial such that disc$(F(x)) \neq 0$. Let $n \in \mathbb{N}$ be squarefree and let $r \in \mathbb{Z}$. Suppose $F(r) \neq 0$ and that for every prime $p \mid n$, we have $p^2 \nmid F(r)$ or $p \nmid F'(r)$. Let $q \in \mathbb{N}$ be a prime or a unit with gcd$(q, n) = 1$ and $q^2 \parallel F(r)$ if $q > 1$. Let $m = q^k n$ for some $k \in \mathbb{N}$. Then there exist infinitely many positive integers $v \equiv r \pmod{m}$ such that $F(v) = q^2 w$, w is squarefree, and gcd$(q, w) = 1$.*

Proof. The proof follows the same general structure as that of Proposition 2 from Silvester, Spearman, and Williams [9]. Let $F(x) = dx^2 + ex + f \in \mathbb{Z}[x]$ be a primitive quadratic polynomial with nonzero discriminant. Let

$$M = \prod_{\substack{p \mid m \\ p \parallel F(r)}} p,$$

$$N = \prod_{\substack{p \mid m \\ p^2 \mid F(r)}} p,$$

where p runs over all primes dividing m with the given conditions. Then set

$$\begin{aligned} G(x) &= \frac{F(mMNqx + (mMq^2 + r))}{MNq} \\ &= \frac{d[mMNqx + (mMq^2 + r)]^2 + e[mMNqx + (mMq^2 + r)] + f}{MNq} \\ &= dm^2MNqx^2 + m[2d(mMq^2 + r) + e]x + \frac{dm^2M^2q^4 + mMq^2(2dr + e) + F(r)}{MNq}. \end{aligned}$$

Let

$$\begin{aligned} A &= dm^2MNq \\ B &= m[2d(mMq^2 + r) + e] \\ C &= \frac{dm^2M^2q^4 + mMq^2(2dr + e) + F(r)}{MNq}. \end{aligned}$$

Clearly $A \neq 0$ so that $G(x)$ is quadratic. Moreover, $A, B \in \mathbb{Z}$. Since $\gcd(M, N) = 1$, we have $MN \mid m$. Furthermore, since $q^2 \parallel F(r) = dr^2 + er + f$, and $q \parallel N$ if $q > 1$, we have that $MNq \mid F(r)$. Thus $C \in \mathbb{Z}$ and therefore $G(x) \in \mathbb{Z}[x]$.

Next we will show that $G(x)$ is primitive. Suppose to the contrary that p is a prime such that $p \mid \gcd(A, B, C)$. If $p = q$, then $q^3 \mid F(r)$ since $q \mid C$ and $q^2 \mid MNq$. But since $q^2 \parallel F(r)$, this is a contradiction. Thus $p \neq q$.

Now suppose $p \mid m = q^k n$. Since $p \neq q$, $p \mid n$. Since $p \mid C$, we must have that $p \mid F(r)$. If $p \parallel F(r)$, then $p \parallel M$ and $p \nmid N$. Thus since $p \mid C$, we have that $p^2 \mid F(r)$, a contradiction. If $p^2 \mid F(r)$, then $p \nmid M$ and $p \parallel N$. But since $p \mid n$ and $p^2 \mid F(r)$, we have by hypothesis that $p \nmid F'(r) = 2dr + e$. So since $p \mid C$, we have that $p^2 \mid m$ with $p \neq q$. Thus $p^2 \mid n$. But this contradicts that n is squarefree. Thus $p \nmid m$, and consequently, $p \nmid MN$.

So since $p \mid A$, we must have that $p \mid d$. As a result, since $p \mid B$, we must have $p \mid e$. Finally, since $p \mid C$, $p \mid d$, and $p \mid e$, we must have that $p \mid f$. Thus $p \mid \gcd(d, e, f) = 1$, a contradiction. Thus $G(x)$ is primitive.

By Lemma 2.6, we have that

$$\operatorname{disc}(G(x)) \quad = \quad \frac{(mMNq)^{2(2-1)}}{(MNq)^{2(2)-2}}\operatorname{disc}(F(x)) = m^2\operatorname{disc}(F(x)) \neq 0,$$

which shows that the discriminant of $G(x)$ is nonzero.

Furthermore, for any $y \in \mathbb{Z}$, we have $\gcd(Ay^2+By+C, MNq) = \gcd(C, MNq) = 1$ since $MNq \mid A, B$ and $\gcd(A, B, C) = 1$. Therefore, by Theorem 2.13, there exist infinitely many positive integers y such that $G(y) = Ay^2 + By + C$ is squarefree and relatively prime to MNq.

Moreover, we have that

$$F(mMNqy + (mMq^2 + r)) = MNq \cdot G(y) = q^2M(N/q) \cdot G(y),$$

where $\gcd(q, M(N/q) \cdot G(y)) = 1$. Thus there exist infinitely many $v \equiv r \pmod{m}$ such that $F(v) = q^2w$, w is squarefree, and $\gcd(q, w) = 1$.

□

2.4 The Main Result

The proof of the main result loosely follows the proofs of the results of Spearman and Williams in [10, 11]. Since our result will generalize both of theirs, our proof will implicitly prove theirs as well. To note when this occurs, we restate their results using our notation. In [10], they show

$$\begin{aligned} S_{1,\mathcal{Q}_3} &= 8^n\left(2\mathbb{N}-1\right), \\ S_{1,\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''} &= 2\mathbb{N}. \end{aligned}$$

In [11], they show that for any squarefree $d \in \mathbb{Z}$ such that $d \neq 1$, we have that $1 \in S_F$ for infinitely many $F \in C(d)$.

As mentioned before, given a fixed squarefree $d \in \mathbb{Z}$, the cases of our proof will depend on both the congruence class of d modulo 8 and the factorization of (2) in $C(d)$. In each case, we will construct an infinite family of cubic polynomials of the form $p_v(x) = x^3 - A(v)x + B(v)$, where $A(v), B(v) \in \mathbb{Z}[v]$ are quadratic polynomials in v. To produce the desired index sets, $A(v)$ and $B(v)$ will be chosen so as to satisfy several conditions. First, they must share a common squarefree factor $F(v)$ for infinitely many $v \in \mathbb{Z}$. This will give us our infinitely many algebraic integers of a given index. Second, they must be chosen so that $p_v(x)$ is irreducible over $\mathbb{Q}$. This ensures that any root θ_v of $p_v(x)$ generates a cubic field F_v. Third, $\mathrm{disc}(p_v(x))$ must have squarefree part equal to d. This will give $F_v \in C(d)$ by Corollary 2.1.1. Fourth, they must be chosen so that, by applying Theorem 2.4, the desired factorization of (2) is achieved. Finally, they must be chosen so that when we apply Theorem 2.2, we obtain a value of Δ_{F_v} that gives the desired value of $\mathrm{ind}(\theta_v)$ when we apply

Proposition 1.2. In particular, we must be able to solve the equation

$$4(A_v)^3 - 27(B_v)^2 = (\mathrm{ind}(\theta_v))^2 \Delta_{F_v}$$

for $\mathrm{ind}(\theta_v)$ to give any natural number in our candidate index sets. As has already been stated, it will be particularly important to control the ramification of the primes 2 and 3 in order to accomplish this.

All of the cases follow the same general format of introducing the polynomials $p_v(x)$ and showing that all appropriate conditions are satisfied.

Theorem 2.15. *For any equivalence class of d modulo 8 and prime ideal factorization of (2) in $C(d)$, the index sets $S_{d,\mathcal{J}}$ are given below:*

	$\mathcal{J}$	$S_{d,\mathcal{J}}$
$d \equiv 2, 3 \ (mod\, 4)$	$\mathcal{Q}_1^2 \mathcal{Q}_1'$	$\mathbb{N}$
$d \equiv 5 \ (mod\, 8)$	$\mathcal{Q}_1^3$	$8^n\,(2\mathbb{N}-1) \cup 2 \cdot 8^n\,(2\mathbb{N}-1)$
	$\mathcal{Q}_1 \mathcal{Q}_2$	$\mathbb{N}$
$d \equiv 1 \ (mod\, 8)$	$\mathcal{Q}_1 \mathcal{Q}_1' \mathcal{Q}_1''$	$2\mathbb{N}$
	$\mathcal{Q}_3$	$8^n\,(2\mathbb{N}-1)$

Moreover, for each $I \in S_{d,\mathcal{J}}$ there are infinitely many $F \in C(d, \mathcal{J})$ such that $\mathcal{O}_F$ possesses an algebraic integer of index I.

Proof. Lemmas 2.8 and 2.10 show that each set $S_{d,\mathcal{J}}$ is contained in the candidate subset of $\mathbb{N}$ provided in the third column. In this proof, we will show the reverse containments. We break the proof into three major cases: $d \equiv 2,\ 3 \pmod 4$, $d \equiv 5 \pmod 8$, and $d \equiv 1 \pmod 8$. We subdivide each case according to the possible factorizations of (2) in $C(d)$. This gives five natural cases.

By Proposition 1.3, we have that $\mathrm{ind}(m\theta) = m^3\mathrm{ind}(\theta)$ for any $m \neq 0$. In particular, this holds when $m = 2$ or $m = 3$. Thus, if we show that I is an index, we will immediately have that $2^{3i}I$ and $3^{3i}I$ are indices for any $i \in \mathbb{Z}_{\geq 0}$. Hence, for each of our five prospective cases we may assume that if I is in the candidate index set, then $3^3 \nmid I$, $2^3 \nmid I$, $2^2 \nmid I$, $2^4 \nmid I$, and $2 \nmid I$. Thus, respectively, we may assume $v_3(I) \in \{0, 1, 2\}$, $v_2(I) \in \{0, 1, 2\}$, $v_2(I) \in \{0, 1\}$, $v_2(I) \in \{1, 2, 3\}$, and $v_2(I) = 0$.

Case 1: $d \equiv 2,\ 3 \pmod 4$.

For each $I \in \mathbb{N}$ such that $v_3(I) \in \{0,\ 1,\ 2\}$, we will show that $I \in S_{d,\mathcal{Q}_1^2\mathcal{Q}_1'}$. Furthermore, we will show that there exist infinitely many $F \in C(d, \mathcal{Q}_1^2\mathcal{Q}_1')$ such that $\mathcal{O}_F$ possesses an element of index I.

For each $v_3(I) \in \{0,\ 1,\ 2\}$, define

$$F(x) = x^2 + 2^2 \cdot 3^{3-v_3(I)}dIx + 3^2dI^2\left(3 + 2^2 \cdot 3^{4-2v_3(I)}d\right) \in \mathbb{Z}[x].$$

First, we will apply Theorem 2.14 to obtain congruence conditions on x for which $F(x)$ is squarefree infinitely often.

Observe that $F(x)$ is clearly primitive. Moreover,

$$\begin{aligned} \mathrm{disc}(F(x)) &= \left(2^2 \cdot 3^{3-v_3(I)}dI\right)^2 - 4 \cdot 3^2dI^2\left(3 + 2^2 \cdot 3^{4-2v_3(I)}d\right) \\ &= 2^4 \cdot 3^{6-2v_3(I)}d^2I^2 - 2^2 \cdot 3^3dI^2 - 2^4 \cdot 3^{6-2v_3(I)}d^2I^2 \\ &= -2^2 \cdot 3^3dI^2 \neq 0. \end{aligned}$$

We now partition $F(x)$ into two cases; the first being that $d \equiv 2 \pmod 4$ or $2 \mid I$, and the second being that $d \equiv 3 \pmod 4$ and $2 \nmid I$.

First, suppose $d \equiv 2 \pmod 4$ or $2 \mid I$. Let $n = 6d/(2^{v_2(d)} \cdot 3^{v_3(d)})$ for any $v_2(d) \in \{0, 1\}$ and $v_3(d) \in \{0, 1\}$. Note that n is squarefree and $F(1) \equiv 1 \pmod p$ for every prime $p \mid n$. Hence, for each prime $p \mid n$, we have that $p \nmid F(1)$. Thus, with $r = 1$ and $q = 1$, we may apply Theorem 2.14 to conclude that there exist infinitely many positive integers $v \equiv 1 \pmod n$ such that $F(v)$ is squarefree.

Now suppose that $d \equiv 3 \pmod 4$ and $2 \nmid I$. Then

$$\begin{aligned} &F(0) \equiv 1 \ (\text{mod } 2), \\ &F(1) \equiv 1 \ (\text{mod } 3d/3^{v_3(d)}), \end{aligned}$$

for any $v_3(I) \in \{0,\ 1,\ 2\}$, $v_2(d) \in \{0, 1\}$, and $v_3(d) \in \{0, 1\}$. By the Chinese Remainder Theorem, there exists $r \in \mathbb{Z}$ with

$$\begin{aligned} &r \equiv 0 \ (\text{mod } 2), \\ &r \equiv 1 \ (\text{mod } 3d/3^{v_3(d)}). \end{aligned}$$

This gives that $F(r) \equiv 1 \ (\text{mod } 6d/3^{v_3(d)})$. Let $n = 6d/3^{v_3(d)}$ and again note that n is squarefree. Then for any prime p such that $p \mid n$, we have that $p \nmid F(r)$. Thus, with the r given above and $q = 1$, we may again apply Theorem 2.14 to conclude that there exist infinitely many positive integers $v \equiv r \pmod n$ such that $F(v)$ is squarefree.

Combining both cases, we have shown that there exist infinitely many positive integers

$$v \equiv r \pmod{6d/(2^{v_2(d)} \cdot 3^{v_3(d)})}$$

such that $F(v)$ is squarefree.

Since the leading coefficient of $F(x)$ is positive, there exists $N \in \mathbb{N}$ such that $F'(x) > 0$ and $F(x) > 1$ for all $x \geq N$. Since the interval $[N, \infty)$ excludes only finitely many positive integers, there exist infinitely many integers $v \geq N$ such that $v \equiv r \pmod{6d/(2^{v_2(d)} \cdot 3^{v_3(d)})}$ and $F(v)$ is squarefree. Denote the set of all such v by V. As $F(x)$ is strictly increasing on the interval $[N, \infty)$, note that no two distinct values of v in V can give the same value to $F(v)$.

Since $v \equiv r \pmod{6d/(2^{v_2(d)} \cdot 3^{v_3(d)})}$ for all $v \in V$, we have that

$$F(v) \equiv F(r) \equiv 1 \pmod{6d/(2^{v_2(d)} \cdot 3^{v_3(d)})}.$$

Thus it is clear that $\gcd(F(v), 6d) = 1$ for each $v \in V$.

For each $v \in V$ and $v_3(I) \in \{0,\ 1,\ 2\}$, set $p_v(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where

$$\begin{aligned} &A = 3F(v), \\ &B = 2\left(v + 2 \cdot 3^{3-v_3(I)} dI\right) F(v). \end{aligned}$$

We will show that $p_v(x)$ is an Eisenstein polynomial for each $v \in V$.

First, we show that

$$\gcd\left(v + 2 \cdot 3^{3-v_3(I)} dI, F(v)\right) = 1.$$

Suppose there exists some prime p such that $p \mid \left(v + 2 \cdot 3^{3-v_3(I)}dI\right)$ and $p \mid F(v)$. Observe

$$\begin{aligned}
F(v) &- \left(v + 2 \cdot 3^{3-v_3(I)}dI\right)^2 \\
&= v^2 + 2^2 \cdot 3^{3-v_3(I)}dIv + 3^2dI^2\left(3 + 2^2 \cdot 3^{4-2v_3(I)}d\right) - \left(v + 2 \cdot 3^{3-v_3(I)}dI\right)^2 \\
&= v^2 + 2^2 \cdot 3^{3-v_3(I)}dIv + 3^3dI^2 + 2^2 \cdot 3^{6-2v_3(I)}d^2I^2 - v^2 - 2^2 \cdot 3^{3-v_3(I)}dIv \\
&\quad -2^2 \cdot 3^{6-2v_3(I)}d^2I^2 \\
&= 3^3dI^2.
\end{aligned}$$

Thus $p \mid 3^3dI^2$. But since $\gcd(F(v), 6d) = 1$ and $p \mid F(v)$, we must have that $p \nmid 3d$. Thus $p \mid I^2$ so that $p^2 \mid 3^3dI^2$. Since $p^2 \mid \left(v + 2 \cdot 3^{3-v_3(I)}I\right)^2$, this gives that $p^2 \mid F(v)$. But this contradicts that $F(v)$ is squarefree.

So since $2 \nmid F(v)$, $\gcd\left(v + 2 \cdot 3^{3-v_3(I)}dI, F(v)\right) = 1$, and $F(v) > 1$ is squarefree, we have for any prime $p \mid F(v)$ that $p \mid A, B$ and $p^2 \nmid B$. Thus $p_v(x)$ is p-Eisenstein for each prime $p \mid F(v)$. Therefore $p_v(x)$ is irreducible over $\mathbb{Q}$ for each $v \in V$. Thus the field generated by $p_v(x)$, call it F_v, is a cubic field.

Next, observe that

$$\begin{aligned}
\operatorname{disc}(p_v(x)) &= 4A^3 - 27B^2 \\
&= 4(3F(v))^3 - 27\left[2\left(v + 2 \cdot 3^{3-v_3(I)}dI\right)F(v)\right]^2 \\
&= 2^2 \cdot 3^3F(v)^2\left[F(v) - \left(v + 2 \cdot 3^{3-v_3(I)}dI\right)^2\right] \\
&= 2^2 \cdot 3^3F(v)^2\left[3^3dI^2\right] \\
&= d(2 \cdot 3^3F(v)I)^2.
\end{aligned}$$

Thus, by Corollary 2.1.1 we have that $F_v \in C(d)$ for each $v \in V$.

Next, we compute Δ_{F_v} for each $v_3(I) \in \{0, 1, 2\}$ by using Theorem 2.2. Recall that s_p and Δ_p are defined before Theorem 2.2. Since $F(v)$ is squarefree and $3 \nmid F(v)$, it is clear that $v_p(A) < 2$ for all primes p, so that the hypotheses of Theorem 2.2 hold. Now if $d \equiv 2 \pmod 4$, then $s_2 \equiv 1 \pmod 2$. Thus, by Theorem 2.2 we have that $2^3 \parallel \Delta_{F_v}$. On the other hand, if $d \equiv 3 \pmod 4$, we have that $s_2 \equiv 0 \pmod 2$ and

$$\Delta_2 \equiv d(3^3 F(v) I / 2^{v_2(I)})^2 \equiv 3 \pmod 4.$$

In this case, we have by Theorem 2.2 that $2^2 \parallel \Delta_{F_v}$. Hence, combining both cases, we may conclude that $2^{2+v_2(d)} \parallel \Delta_{F_v}$.

Furthermore, for each $v_3(I) \in \{0,\ 1,\ 2\}$ we have that

$$A = 3F(v) = 3\left[v^2 + 2^2 \cdot 3^{3-v_3(I)} dIv + 3^2 dI^2 \left(3 + 2^2 \cdot 3^{4-2v_3(I)} d\right)\right] \equiv 3v^2 \pmod{27}.$$

This gives that $A + 1 \equiv 3v^2 + 1 \pmod{27}$. Moreover, since $v \equiv 1 \pmod 3$, we get $A \equiv 3 \pmod 9$. Also,

$$B^2 = \left[2\left(v + 2 \cdot 3^{3-v_3(I)} dI\right) F(v)\right]^2 \equiv (2v \cdot v^2)^2 \equiv 4v^6 \pmod{27}.$$

Since $v \equiv 1 \pmod 3$ for all $v \in V$, we have by Lemma 2.11 that $B^2 \equiv A+1 \pmod{27}$. Lastly, note that $s_3 \equiv v_3(d) \pmod 2$. Thus, by Theorem 2.2, $3^{v_3(d)} \parallel \Delta_{F_v}$.

Next, since $\gcd(d/(2^{v_2(d)} \cdot 3^{v_3(d)}), 6) = 1$ and d is squarefree, we have that

$$\prod_{\substack{p > 3 \\ s_p \equiv 1 \pmod 2}} p = |d|/(2^{v_2(d)} \cdot 3^{v_3(d)})$$

and

$$\prod_{\substack{p > 3 \\ 1 \leq v_p(B) \leq v_p(A)}} p^2 = F(v)^2.$$

Therefore, by Theorem 2.2 we have that

$$\Delta_{F_v} = \operatorname{sign}(d) \cdot 2^{2+v_2(d)} \cdot 3^{v_3(d)} \left(|d|/(2^{v_2(d)} \cdot 3^{v_3(d)})\right) F(v)^2 = 2^2 dF(v)^2.$$

Note that since distinct values of $v \in V$ gives distinct values of $F(v)$, each value of Δ_{F_v} is distinct. Consequently, each of the cubic fields F_v are distinct.

Now, set $q_v(x) = \dfrac{p_v(3x+v)}{27}$. Then by Lemma 2.12, we have

$$q_v(x) = x^3 + vx^2 + \left(\frac{3v^2 - A}{9}\right) x + \left(\frac{v^3 - Av + B}{27}\right).$$

Observe that $v^2 - A/3 \equiv 0 \pmod 3$ and

$$v^3 - Av + B \equiv v^3 - 3v^2 \cdot v + 2v \cdot v^2 \equiv 0 \pmod{27}.$$

Thus $q_v(x) \in \mathbb{Z}[x]$. Since $p_v(x) = 27q_v\left(\dfrac{x-v}{3}\right)$, we have that $q_v(x)$ is irreducible over $\mathbb{Q}$ since $p_v(x)$ is irreducible over $\mathbb{Q}$. Moreover, $q_v(x)$ and $p_v(x)$ generate the same cubic extension F_v of $\mathbb{Q}$.

Finally, let θ_v be any root of $q_v(x)$. Then by Corollary 2.6.1, we have that

$$\begin{aligned} d(2IF(v))^2 &= \frac{\operatorname{disc}(p_v(x))}{3^6} \\ &= \operatorname{disc}(q_v(x)) \\ &= \operatorname{ind}(\theta_v)^2 \Delta_{F_v} \\ &= \operatorname{ind}(\theta_v)^2 \cdot 2^2 dF(v)^2, \end{aligned}$$

which gives that $I = \mathrm{ind}(\theta_v)$. Therefore $I \in S_{d,\mathcal{Q}_1^2\mathcal{Q}_1'}$ and is an index of an algebraic integer in $F_v \in C(d, \mathcal{Q}_1^2\mathcal{Q}_1')$ for each $v \in V$.

Case 2: $d \equiv 5 \pmod 8$.

By Corollary 2.5.1, there are 2 possible factorizations of (2) in $C(d)$ for any $d \equiv 5 \pmod 8$, namely, $\mathcal{Q}_1^3$ or $\mathcal{Q}_1\mathcal{Q}_2$. So, we break Case 2 into two subcases.

Case 2a: $(2) = \mathcal{Q}_1^3$.

Since $d \equiv 5 \pmod 8$, we can write $d \equiv 5 + 8j \pmod{32}$ for some $j \in \{0, 1, 2, 3\}$. It is easy to check that

$$1 + 3^{3+6(v_2(I)+j)}d \equiv 2^{3+v_2(I)} \pmod{32}.$$

for each $j \in \{0, 1, 2, 3\}$ and $v_2(I) \in \{0, 1\}$. This gives

$$\begin{aligned} v_2(3^3d + 3^{6(v_2(I)+j+1)}d^2) &= v_2((3^3d)(1 + 3^{3+6(v_2(I)+j)}d)) \\ &= v_2(1 + 3^{3+6(v_2(I)+j)}d) \\ &= 3 + v_2(I). \end{aligned}$$

For any $j \in \{0, 1, 2, 3\}$ and $v_2(I) \in \{0, 1\}$, define

$$F(x) = 2^{11-v_2(I)}x^2 + 2^{5-2v_2(I)} \cdot 3^{3(v_2(I)+j+1)}dIx + \frac{3^3d + 3^{6(v_2(I)+j+1)}d^2}{2^{3+v_2(I)}}(I/2^{v_2(I)})^2$$

and observe that $F(x) \in \mathbb{Z}[x]$.

Again, we will apply Theorem 2.14 to obtain congruence conditions on x for which $F(x)$ is squarefree infinitely often. First, since the leading coefficient of $F(x)$ is a power of 2 and the constant term is odd, we have that $F(x)$ is primitive. Moreover,

$$\begin{aligned}
\operatorname{disc}(F(x)) &= \left(2^{5-2v_2(I)} \cdot 3^{3(v_2(I)+j+1)} dI\right)^2 \\
&\quad -4 \cdot 2^{11-v_2(I)} \cdot \frac{3^3 d + 3^{6(v_2(I)+j+1)} d^2}{2^{3+v_2(I)}} (I/2^{v_2(I)})^2 \\
&= 2^{10-4v_2(I)} \cdot 3^{6(v_2(I)+j+1)} d^2 I^2 \\
&\quad -2^{10-4v_2(I)} \cdot 3^3 dI^2 - 2^{10-4v_2(I)} \cdot 3^{6(v_2(I)+j+1)} d^2 I^2 \\
&= -2^{10-4v_2(I)} \cdot 3^3 dI^2 \neq 0.
\end{aligned}$$

Now, let $n = d/3^{v_3(d)}$, where $v_3(d) \in \{0,\ 1\}$. Observe that n is squarefree and $F(1) \not\equiv 0 \pmod{p}$ for any prime $p \mid n$. Hence, for any prime $p \mid n$, we have that $p \nmid F(1)$. Thus, with $r = 1$ and $q = 1$, we may apply Theorem 2.14 to conclude that there exist infinitely many positive integers $v \equiv 1 \pmod{n}$ such that $F(v)$ is squarefree.

Let V denote the same set as in previous cases, so that $F(v) > 1$ for all $v \in V$ and no two distinct values of v in V give the same value to $F(v)$. Since $v \equiv 1 \pmod{n}$ for all $v \in V$, we have $F(v) \equiv F(1) \not\equiv 0 \pmod{p}$ for every prime $p \mid n$. Thus $\gcd(F(v), 6d) = 1$ for each $v \in V$.

For each $v \in V$ and $v_2(I) \in \{0, 1\}$, set $p_v(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where

$$\begin{aligned}
A &= 3 \cdot 2^{1+v_2(I)} F(v), \\
B &= 2^{1+v_2(I)} \left(2^7 v + 3^{3(v_2(I)+j+1)} d(I/2^{v_2(I)})\right) F(v).
\end{aligned}$$

We will show that $p_v(x)$ is an Eisenstein polynomial for each $v \in V$.

First, we show that

$$\gcd\left(2^7v + 3^{3(v_2(I)+j+1)}d(I/2^{v_2(I)}), F(v)\right) = 1.$$

Suppose there exists some prime p such that $p \mid 2^7v + 3^{3(v_2(I)+j+1)}d(I/2^{v_2(I)})$ and $p \mid F(v)$. Observe

$$\begin{aligned} 2^{3+v_2(I)}F(v) &- \left[2^7v + 3^{3(v_2(I)+j+1)}d(I/2^{v_2(I)})\right]^2 \\ &= 2^{14}v^2 + 2^{8-v_2(I)} \cdot 3^{3(v_2(I)+j+1)}dIv + \left(3^3d + 3^{6(v_2(I)+j+1)}d^2\right)(I/2^{v_2(I)})^2 \\ &\quad - \left[2^{14}v^2 + 2^{8-v_2(I)} \cdot 3^{3(v_2(I)+j+1)}dIv + 3^{6(v_2(I)+j+1)}d^2(I/2^{v_2(I)})^2\right] \\ &= 3^3d(I/2^{v_2(I)})^2. \end{aligned}$$

So $p \mid 3^3d(I/2^{v_2(I)})^2$. But since $\gcd(F(v), 6d) = 1$ and $p \mid F(v)$, we must have $p \nmid 6d$. Thus $p \mid (I/2^{v_2(I)})^2$ so that $p^2 \mid 3^3d(I/2^{v_2(I)})^2$. Thus $p^2 \mid \left[2^7v + 3^{3(v_2(I)+j+1)}d(I/2^{v_2(I)})\right]^2$ so that $p^2 \mid 2^{3+v_2(I)}F(v)$. Then since $p \neq 2$, we must have $p^2 \mid F(v)$. But this contradicts that $F(v)$ is squarefree.

So since $\gcd(2^7v + 3^{3(v_2(I)+j+1)}d(I/2^{v_2(I)}), F(v)) = 1$, $F(v) > 1$, and $2 \nmid F(v)$, we have for any prime $p \mid F(v)$ that $p \mid A, B$ and $p^2 \nmid B$. Thus $p_v(x)$ is p-Eisenstein for each prime $p \mid F(v)$. Therefore $p_v(x)$ is irreducible over $\mathbb{Q}$ for each $v \in V$. Thus, the field generated by $p_v(x)$, say F_v, is a cubic field.

We now show that $F_v \in C(d, \mathcal{Q}_1^3)$ for each $v \in V$. Observe

$$\begin{aligned}
\operatorname{disc}(p_v(x)) &= 4A^3 - 27B^2 \\
&= 4(3 \cdot 2^{1+v_2(I)} F(v))^3 - 27\left[2^{1+v_2(I)}\left(2^7 v + 3^{3(v_2(I)+j+1)} d(I/2^{v_2(I)})\right) F(v)\right]^2 \\
&= 2^{2+2v_2(I)} \cdot 3^3 F(v)^2 \left[2^{3+v_2(I)} F(v) - \left(2^7 v + 3^{3(v_2(I)+j+1)} d(I/2^{v_2(I)})\right)^2\right] \\
&= 2^{2+2v_2(I)} \cdot 3^3 F(v)^2 \left[3^3 d(I/2^{v_2(I)})^2\right] \\
&= d(2 \cdot 3^3 I F(v))^2.
\end{aligned}$$

Thus, by Corollary 2.1.1 we have that $F_v \in C(d)$ for each $v \in V$.

Since $F(v)$ is squarefree and $3 \nmid F(v)$, we have that $v_p(A) < 2$ for all primes $p \neq 2$. Since $2 \nmid F(v)$, $v_2(I) + 1 \leq 2$ for each $v_2(I) \in \{0, 1\}$, and

$$2^7 v + 3^{3(v_2(I)+j+1)} d(I/2^{v_2(I)}) \equiv 1 \pmod{2},$$

we have that $v_2(B) < 3$. Therefore $v_p(A) < 2$ or $v_p(B) < 3$ for all primes p. Also note that $1 \leq v_2(B) = v_2(A) = 1 + v_2(I)$. Thus, by Theorem 2.4, we have that $(2)\mathcal{O}_{F_v} = Q_1^3$.

Next, we compute Δ_{F_v} for each $v_2(I) \in \{0, 1\}$. First, since $1 \leq v_2(B) \leq v_2(A)$, we have by Theorem 2.2 that $2^2 \parallel \Delta_{F_v}$. Next, observe

$$A = 3 \cdot 2^{1+v_2(I)} F(v) \equiv 3 \cdot 2^{12} v^2 \equiv 3v^2 \pmod{27}.$$

This gives that $A + 1 \equiv 3v^2 + 1 \pmod{27}$. Also, since $v \equiv 1 \pmod{3}$, we get $A \equiv 3 \pmod{9}$. Furthermore,

$$B^2 = 2^{2+2v_2(I)}(2^{14} v^2)(2^{11-v_2(I)} v^2)^2 \equiv 2^{38} v^6 \equiv 4v^6 \pmod{27}.$$

Since $v \equiv 1 \pmod{3}$, we have by Lemma 2.11 that $B^2 \equiv A + 1 \pmod{27}$. Lastly, note that $s_3 \equiv v_3(d) \pmod{2}$. Thus, by Theorem 2.2, $3^{v_3(d)} \parallel \Delta_{K_v}$.

Now, since $\gcd(d/3^{v_3(d)}, 6) = 1$ and d is squarefree, we have that

$$\prod_{\substack{p>3 \\ s_p \equiv 1 \pmod{2}}} p = |d|/3^{v_3(d)}$$

and

$$\prod_{\substack{p>3 \\ 1 \leq v_p(B) \leq v_p(A)}} p^2 = F(v)^2.$$

Therefore, by Theorem 2.2 we have that

$$\Delta_{F_v} = \operatorname{sign}(d) \cdot 2^2 \cdot 3^{v_3(d)}(|d|/3^{v_3(d)})F(v)^2 = 2^2 dF(v)^2.$$

Note that since distinct values of $v \in V$ gives distinct values of $F(v)$, each value of Δ_{F_v} is distinct. Consequently, each of the cubic fields F_v are distinct.

Set $q_v(x) = \dfrac{p_v(3x+v)}{27}$. Then by Lemma 2.12, we have

$$q_v(x) = x^3 + vx^2 + \left(\frac{3v^2 - A}{9}\right)x + \left(\frac{v^3 - Av + B}{27}\right).$$

Observe that

$$v^2 - A/3 \equiv v^2 - 2^{1+v_2(I)} \cdot 2^{11-v_2(I)}v^2 \equiv (1 - 2^{12})v^2 \equiv 0 \pmod{3}$$

and

$$\begin{aligned} v^3 - Av + B &\equiv v^3 - 3 \cdot 2^{1+v_2(I)} \cdot 2^{11-v_2(I)} v^2 \cdot v + 2^{1+v_2(I)} \cdot 2^7 v \cdot 2^{11-v_2(I)} v^2 \\ &\equiv (1 - 3 \cdot 2^{12} + 2^{19}) v^3 \equiv 0 \pmod{27}. \end{aligned}$$

Thus $q_v(x) \in \mathbb{Z}[x]$.

Since $p_v(x) = 27 q_v \left(\frac{x-v}{3} \right)$, we have that $q_v(x)$ is irreducible over $\mathbb{Q}$ since $p_v(x)$ is irreducible over $\mathbb{Q}$. Moreover, $q_v(x)$ and $p_v(x)$ generate the same cubic extension F_v of $\mathbb{Q}$. Finally, if θ_v is a root of $q_v(x)$, then by Corollary 2.6.1 we have that

$$\begin{aligned} 2^2 d I^2 F(v)^2 &= \frac{\operatorname{disc}(p_v(x))}{3^6} \\ &= \operatorname{disc}(q_v(x)) \\ &= \operatorname{ind}(\theta_v)^2 \Delta_{F_v} \\ &= \operatorname{ind}(\theta_v)^2 \cdot 2^2 d F(v)^2, \end{aligned}$$

which gives $I = \operatorname{ind}(\theta_v)$. Therefore $I \in S_{d, \mathcal{Q}_1^3}$ and is the index of an algebraic integer in $F_v \in C(d, \mathcal{Q}_1^3)$ for each $v \in V$.

Case 2b: $(2) = \mathcal{Q}_1 \mathcal{Q}_2$.

Since $d \equiv 5 \pmod 8$, we may write $d \equiv 5 + 8j \pmod{64}$, for some $j \in \{0, 1, ..., 7\}$. It is easy to check that

$$3^3 d \left(3^{13+6j} d + 1 \right) \equiv 32 \pmod{64}$$

for each $j \in \{0, 1, ..., 7\}$. Therefore $v_2(3^3 d (3^{13+6j} d + 1)) = 5$.

For any j, define

$$F(x) = \begin{cases} 2^{23}x^2 + 2^{10} \cdot 3^{8+3j} dIx + \dfrac{3^3 dI^2 \left(3^{13+6j}d+1\right)}{32} & \text{if } v_2(I) = 0, \\ 2^{24-12v_2(I)}x^2 + 2^{26-13v_2(I)} \cdot 3^3 dIx & \\ \qquad +3^3 d\left(1 + 2^{28-14v_2(I)} \cdot 3^3 d\right)(I/2)^2 & \text{if } v_2(I) = 1, 2, \end{cases}$$

and observe that $F(x) \in \mathbb{Z}[x]$.

Again, we will apply Theorem 2.14 to obtain congruence conditions on x for which $F(x)$ is squarefree infinitely often.

First, suppose $v_2(I) = 0$. Since $v_2(3^3 d\left(3^{13+6j}d+1\right)) = 5$, the constant term of $F(x)$ is not divisible by 2, whereas the leading coefficient is a power of 2. Thus $F(x)$ is primitive. Moreover,

$$\begin{aligned} \operatorname{disc}(F(x)) &= \left(2^{10} \cdot 3^{8+3j} dI\right)^2 - 4 \cdot 2^{23} \frac{3^3 dI^2 \left(3^{13+6j}d+1\right)}{32} \\ &= 2^{20} \cdot 3^{16+6j} d^2 I^2 - 2^{20} \cdot 3^{16+6j} d^2 I^2 - 2^{20} \cdot 3^3 dI^2 \\ &= -2^{20} \cdot 3^3 dI^2 \neq 0. \end{aligned}$$

Now suppose $v_2(I) \in \{1, 2\}$. When $v_2(I) = 1$, the constant term of $F(x)$ is not divisible by 2 whereas the leading coefficient is a power of 2. When $v_2(I) = 2$, the leading coefficient is 1. Therefore, $F(x)$ is primitive in these cases as well. Moreover,

$$\begin{aligned} \operatorname{disc}(F(x)) &= \left(2^{26-13v_2(I)} \cdot 3^3 dI\right)^2 - 4 \cdot 2^{24-12v_2(I)} \cdot 3^3 d\left(1 + 2^{28-14v_2(I)} \cdot 3^3 d\right)(I/2)^2 \\ &= 2^{52-26v_2(I)} \cdot 3^6 d^2 I^2 - 2^{24-12v_2(I)} \cdot 3^3 dI^2 - 2^{52-26v_2(I)} \cdot 3^6 d^2 I^2 \\ &= -2^{24-12v_2(I)} \cdot 3^3 dI^2 \neq 0. \end{aligned}$$

Let $n = 6d/3^{v_3(d)}$, where $v_3(d) \in \{0,\ 1\}$. Observe that n is squarefree. Also note that for each $v_2(I) \in \{0, 1, 2\}$, we have $F(1) \not\equiv 0 \pmod{p}$ for any prime $p \mid n$. Hence, for any prime p such that $p \mid n$, we have that $p \nmid F(1)$. Thus, with $r = 1$ and $q = 1$, we may apply Theorem 2.14 to conclude that there exist infinitely many positive integers $v \equiv 1 \pmod{n}$ such that $F(v)$ is squarefree.

Let V denote the same set as in the previous case so that $F(v) > 1$ for all $v \in V$ and no two distinct values of v in V give the same value to $F(v)$. Since $v \equiv 1 \pmod{n}$ for all $v \in V$, we have $F(v) \equiv F(1) \not\equiv 0 \pmod{p}$ for every prime $p \mid n$. Thus $\gcd(F(v), 6d) = 1$ for each $v \in V$.

For each $v \in V$ and $v_2(I) \in \{0,\ 1,\ 2\}$, set $p_v(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where

$$A = \begin{cases} 6F(v) & \text{if } v_2(I) = 0, \\ 3F(v) & \text{if } v_2(I) = 1,\ 2, \end{cases}$$

and

$$B = \begin{cases} (2^{14}v + 3^{8+3j}dI)\, F(v) & \text{if } v_2(I) = 0, \\ 2^{13-6v_2(I)} \left(v + 3^3 d(I/2^{v_2(I)-1})\right) F(v) & \text{if } v_2(I) = 1,\ 2. \end{cases}$$

We will show that $p_v(x)$ is an Eisenstein polynomial for each $v \in V$.

First, suppose $v_2(I) = 0$. In this case, we will show that

$$\gcd(2^{14}v + 3^{8+3j}dI, F(v)) = 1.$$

Suppose there exists some prime p such that $p \mid (2^{14}v + 3^{8+3j}dI)$ and $p \mid F(v)$.

Observe

$$\begin{aligned}
32F(v) \quad &- \quad \left(2^{14}v + 3^{8+3j}dI\right)^2 \\
&= \quad [2^{28}v^2 + 2^{15}\cdot 3^{8+3j}dIv + 3^3dI^2\left(3^{13+6j}d+1\right)] - \left(2^{14}v + 3^{8+3j}dI\right)^2 \\
&= \quad 2^{28}v^2 + 2^{15}\cdot 3^{8+3j}dIv + 3^{16+6j}d^2I^2 + 3^3dI^2 - 2^{28}v^2 \\
&\quad\quad -2^{15}\cdot 3^{8+3j}dIv - 3^{16+6j}d^2I^2 \\
&= \quad 3^3dI^2.
\end{aligned}$$

Thus $p \mid 3^3dI^2$. But since $\gcd(F(v), 6d) = 1$ and $p \mid F(v)$, we must have that $p \nmid 6d$. Thus $p \mid I^2$ so that $p^2 \mid 3^3dI^2$. Since $p^2 \mid (2^{14}v + 3^{8+3j}dI)^2$, this gives that $p^2 \mid 32F(v)$. Since $p \neq 2$, we have $p^2 \mid F(v)$. But this contradicts that $F(v)$ is squarefree.

Next, suppose $v_2(I) \in \{1, 2\}$. In this case, we will show that

$$\gcd\left(2^{13-6v_2(I)}(v + 3^3d(I/2^{v_2(I)-1})), F(v)\right) = 1.$$

Suppose there exists some prime p such that $p \mid 2^{13-6v_2(I)}\left(v + 3^3d(I/2^{v_2(I)-1})\right)$ and $p \mid F(v)$. Observe

$$\begin{aligned}
4F(v) \quad &- \quad \left[2^{13-6v_2(I)}\left(v + 3^3d(I/2^{v_2(I)-1})\right)\right]^2 \\
&= \quad \left[2^{26-12v_2(I)}v^2 + 2^{28-13v_2(I)}\cdot 3^3dIv + 3^3dI^2\left(1 + 3^3\cdot 2^{28-14v_2(I)}d\right)\right] \\
&\quad\quad - \left[2^{13-6v_2(I)}\left(v + 3^3d(I/2^{v_2(I)-1})\right)\right]^2 \\
&= \quad 2^{26-12v_2(I)}v^2 + 2^{28-13v_2(I)}\cdot 3^3dIv + 3^3dI^2 + 3^6\cdot 2^{28-14v_2(I)}d^2I^2 \\
&\quad\quad -2^{26-12v_2(I)}v^2 - 2^{28-13v_2(I)}\cdot 3^3dIv - 2^{28-14v_2(I)}\cdot 3^6d^2I^2 \\
&= \quad 3^3dI^2.
\end{aligned}$$

Thus $p \mid 3^3dI^2$. This contradicts that $F(v)$ is squarefree for the same reason as before.

Since $2 \nmid F(v)$ and $F(v) > 1$, the previous results show that for any prime $p \mid F(v)$, we have that $p \mid A, B$ and $p^2 \nmid B$ in both cases. Thus $p_v(x)$ is p-Eisenstein for any prime $p \mid F(v)$. Therefore $p_v(x)$ is irreducible over $\mathbb{Q}$ for each $v \in V$. Thus, the field generated by $p_v(x)$, call it F_v, is a cubic field.

We now show that $F_v \in C(d, \mathcal{Q}_1\mathcal{Q}_2)$ for each $v \in V$. First, suppose $v_2(I) = 0$. Observe that

$$\begin{aligned}
\operatorname{disc}(p_v(x)) &= 4A^3 - 27B^2 \\
&= 4(6F(v))^3 - 27\left[\left(2^{14}v + 3^{8+3j}dI\right)F(v)\right]^2 \\
&= 3^3F(v)^2\left[32F(v) - \left(2^{14}v + 3^{8+3j}dI\right)^2\right] \\
&= 3^3F(v)^2(3^3dI^2) \\
&= d(3^3IF(v))^2.
\end{aligned}$$

Thus, by Corollary 2.1.1 we have that $F_v \in C(d)$ for each $v \in V$. Since $F(v)$ is squarefree and $2, 3 \nmid F(v)$, we have that $v_p(A) < 2$ for all primes p. Also, A is even and B is odd, since $2^{14}v + 3^{8+3j}dI \equiv 1 \pmod 2$. So by Theorem 2.4, we have that $(2)\mathcal{O}_{F_v} = \mathcal{Q}_1\mathcal{Q}_2$.

Now suppose $v_2(I) \in \{1, 2\}$. Observe that

$$\begin{aligned}
\operatorname{disc}(p_v(x)) &= 4A^3 - 27B^2 \\
&= 4(3F(v))^3 - 27\left[2^{13-6v_2(I)}\left(v + 3^3d(I/2^{v_2(I)-1})\right)F(v)\right]^2 \\
&= 3^3F(v)^2\left(4F(v) - \left[2^{13-6v_2(I)}\left(v + 3^3d(I/2^{v_2(I)-1})\right)\right]^2\right) \\
&= 3^3F(v)^2(3^3dI^2) \\
&= d(3^3IF(v))^2.
\end{aligned}$$

Thus by Corollary 2.1 we have that $F_v \in C(d)$ for each $v \in V$. Since $F(v)$ is squarefree and $3 \nmid F(v)$, we have that $v_p(A) < 2$ for all primes p. Also, A is odd, B is even, s_2 is even, and

$$\Delta_2 = d\left(3^3(I/2^{v_2(I)})F(v)\right)^2 \equiv d \equiv 5 \pmod 8.$$

So by Theorem 2.4, we have that $(2)\mathcal{O}_{F_v} = \mathcal{Q}_1\mathcal{Q}_2$.

Next, we compute Δ_{F_v} for each $v_2(I) \in \{0,1,2\}$ by using Theorem 2.2. First, since $(2)\mathcal{O}_{F_v} = \mathcal{Q}_1\mathcal{Q}_2$ for all $v \in V$, 2 is unramified in F_v. Thus $2 \nmid \Delta_{F_v}$ in both cases.

Suppose $v_2(I) = 0$. Then for each $j \in \{0,1,...,7\}$ we have

$$\begin{aligned} A = 6F(v) &= 6\left[2^{23}v^2 + 2^{10}\cdot 3^{8+3j}dIv + \frac{3^3dI^2\left(3^{13+6j}d+1\right)}{32}\right] \\ &\equiv 3\cdot 2^{24}v^2 \equiv 3v^2 \pmod{27}. \end{aligned}$$

This gives $A+1 \equiv 3v^2+1 \pmod{27}$. Also, since $v \equiv 1 \pmod 3$, we get $A \equiv 3 \pmod 9$. Lastly,

$$\begin{aligned} B^2 &= \left[\left(2^{14}v + 3^{8+3j}dI\right)F(v)\right]^2 \\ &\equiv (2^{14}v^2\cdot 2^{23}v^2)^2 \equiv 4v^6 \pmod{27}. \end{aligned}$$

Now suppose $v_2(I) \in \{1,2\}$. Then for each $j \in \{0,1,...,7\}$ we have

$$\begin{aligned} A = 3F(v) &= 3\left[2^{24-12v_2(I)}v^2 + 2^{26-13v_2(I)}\cdot 3^3dIv + 3^3d\left(1+2^{28-14v_2(I)}\cdot 3^3d\right)(I/2)^2\right] \\ &\equiv 3\cdot 2^{24-12v_2(I)}v^2 \equiv 3v^2 \pmod{27}. \end{aligned}$$

Again, this gives that $A+1 \equiv 3v^2+1 \pmod{27}$ and $A \equiv 3 \pmod 9$. Lastly,

$$\begin{aligned} B^2 &= \left[2^{13-6v_2(I)}\left(v+3^3d(I/2^{v_2(I)-1})\right)F(v)\right]^2 \\ &\equiv (2^{13-6v_2(I)}v \cdot 2^{24-12v_2(I)}v^2)^2 \equiv 4v^6 \pmod{27}. \end{aligned}$$

Therefore, since $v \equiv 1 \pmod 3$ for all $v \in V$, we have by Lemma 2.11 that $B^2 \equiv A+1 \pmod{27}$ in both cases. Lastly, note that $s_3 \equiv v_3(d) \pmod 2$. Hence, by Theorem 2.2, $3^{v_3(d)} \,\|\, \Delta_{F_v}$ in both cases.

Now since $\gcd(d/3^{v_3(d)},6)=1$ and d is squarefree, in both cases we have that

$$\prod_{\substack{p>3 \\ s_p \equiv 1 \pmod 2}} p = |d|/3^{v_3(d)}$$

and

$$\prod_{\substack{p>3 \\ 1 \le v_p(B) \le v_p(A)}} p^2 = F(v)^2.$$

Therefore, by Theorem 2.2 we have

$$\Delta_{F_v} = \operatorname{sign}(d) \cdot 3^{v_3(d)}\left(|d|/3^{v_3(d)}\right)F(v)^2 = dF(v)^2.$$

Note that since distinct values of $v \in V$ gives distinct values of $F(v)$, each value of Δ_{F_v} is distinct. Consequently, each of the cubic fields F_v are distinct.

In both cases, set $q_v(x) = \dfrac{p_v(3x+v)}{27}$. Then by Lemma 2.12, we have

$$q_v(x) = x^3+vx^2+\left(\frac{3v^2-A}{9}\right)x+\left(\frac{v^3-Av+B}{27}\right).$$

When $v_2(I) = 0$, we have $v^2 - A/3 \equiv v^2 - 2^{24}v^2 \equiv 0 \pmod 3$ and

$$v^3 - Av + B \equiv v^3 - 3 \cdot 2^{24}v^3 + 2^{14}v \cdot 2^{23}v^2 \equiv (1 - 3 \cdot 2^{24} + 2^{37})v^3 \equiv 0 \pmod{27}.$$

When $v_2(I) \in \{1, 2\}$, we have $v^2 - A/3 \equiv v^2 - 2^{24-12v_2(I)}v^2 \equiv 0 \pmod 3$ and

$$\begin{aligned} v^3 - Av + B &\equiv v^3 - 3 \cdot 2^{24-12v_2(I)}v^3 + 2^{13-6v_2(I)}v \cdot 2^{24-12v_2(I)}v^2 \\ &\equiv (1 - 3 \cdot 2^{24-12v_2(I)} + 2^{37-18v_2(I)})v^3 \equiv 0 \pmod{27}. \end{aligned}$$

Thus in both cases, we have that $q_v(x) \in \mathbb{Z}[x]$.

Since $p_v(x) = 27q_v\left(\dfrac{x-v}{3}\right)$, we have that $q_v(x)$ is irreducible over $\mathbb{Q}$ since $p_v(x)$ is irreducible over $\mathbb{Q}$. Moreover, $q_v(x)$ and $p_v(x)$ generate the same cubic extension F_v of $\mathbb{Q}$. Finally, if θ_v is a root of $q_v(x)$, then by Corollary 2.6.1 we have that

$$\begin{aligned} dI^2F(v)^2 &= \frac{\mathrm{disc}(p_v(x))}{3^6} \\ &= \mathrm{disc}(q_v(x)) \\ &= \mathrm{ind}(\theta_v)^2\Delta_{F_v} \\ &= \mathrm{ind}(\theta_v)^2 dF(v)^2, \end{aligned}$$

which gives that $I = \mathrm{ind}(\theta_v)$. Therefore $I \in S_{d,\mathcal{Q}_1\mathcal{Q}_2}$ and is an index of an algebraic integer in $F_v \in C(d, \mathcal{Q}_1\mathcal{Q}_2)$ for each $v \in V$.

Case 3: $d \equiv 1 \pmod 8$.

By Corollary 2.5.1, there are 2 possible factorizations of (2) in $C(d)$ for any $d \equiv 1 \pmod 8$, namely, $\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''$ or $\mathcal{Q}_3$. So, we break Case 3 into two subcases.

Case 3a: $(2) = \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''$.

For each $v_2(I) \in \{1,2,3\}$, define $F(x) \in \mathbb{Z}[x]$ by

$$F(x) = \begin{cases} 2^{12}x^2 + 2^9 \cdot 3^3 dIx + 3^3 d\,(1 + 2^6 \cdot 3^3 d)\,(I/2)^2 & \text{if } v_2(I) = 1, \\ 2^{12}x^2 + 2^{7-v_2(I)} \cdot 3^3 dIx + 3^3 d\left(2^{2v_2(I)-2} + 3^3 d\right)(I/2^{v_2(I)})^2 & \text{if } v_2(I) = 2, 3. \end{cases}$$

Again, we will apply Theorem 2.14 to obtain congruence conditions on x for which $F(x)$ is squarefree infinitely often.

First, notice for each $v_2(I) \in \{1,2,3\}$ that the leading coefficient of $F(x)$ is a power of 2, whereas the constant term is not divisible by 2. Hence, $F(x)$ is primitive in both cases. If $v_2(I) = 1$, then

$$\begin{aligned} \operatorname{disc}(F(x)) &= \left(2^9 \cdot 3^3 dI\right)^2 - 4 \cdot 2^{12} \cdot 3^3 d\left(1 + 2^6 \cdot 3^3 d\right)(I/2)^2 \\ &= 2^{18} \cdot 3^6 d^2 I^2 - 2^{12} \cdot 3^3 dI^2 - 2^{18} \cdot 3^6 d^2 I^2 \\ &= -2^{12} \cdot 3^3 dI^2 \neq 0. \end{aligned}$$

If $v_2(I) \in \{2,3\}$, then

$$\begin{aligned} \operatorname{disc}(F(x)) &= \left(2^{7-v_2(I)} \cdot 3^3 dI\right)^2 - 4 \cdot 2^{12} \cdot 3^3 d\left(2^{2v_2(I)-2} + 3^3 d\right)(I/2^{v_2(I)})^2 \\ &= 2^{14-2v_2(I)} \cdot 3^6 d^2 I^2 - 2^{12} \cdot 3^3 dI^2 - 2^{14-2v_2(I)} \cdot 3^6 d^2 I^2 \\ &= -2^{12} \cdot 3^3 dI^2 \neq 0. \end{aligned}$$

Thus $\operatorname{disc}(F(x)) \neq 0$ in both cases.

Now, let $n = 6d/3^{v_3(d)}$, where $v_3(d) \in \{0, 1\}$. Observe $F(1) \not\equiv 0 \pmod{p}$ for each $p \mid n$. Hence, for any prime p such that $p \mid n$, we have that $p \nmid F(1)$. Thus, with $r = 1$ and $q = 1$, we may apply Theorem 2.14 in both cases to conclude that there exist infinitely many positive integers $v \equiv 1 \pmod{n}$ such that $F(v)$ is squarefree.

For each case, let V denote the same set as before so that $F(v) > 1$ for all $v \in V$ and no two distinct values of v in V can give the same value to $F(v)$. Observe that since $v \equiv 1 \pmod{n}$ for all $v \in V$, we have that $F(v) \equiv F(1) \not\equiv 0 \pmod{p}$ for each $p \mid n$. Thus $\gcd(F(v), 6d) = 1$ for each $v \in V$.

For each $v \in V$, set $p_v(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where $A = 3F(v)$ and

$$B = \begin{cases} 2^4(2^3v + 3^3d(I/2))F(v) & \text{if } v_2(I) = 1, \\ 2(2^6v + 3^3d(I/2^{v_2(I)}))F(v) & \text{if } v_2(I) = 2, 3. \end{cases}$$

We will show $p_v(x)$ is an Eisenstein polynomial for each $v \in V$.

First, suppose $v_2(I) = 1$. In this case, we will show that

$$\gcd\left(2^4(2^3v + 3^3d(I/2)), F(v)\right) = 1.$$

Suppose there exists some prime p such that $p \mid 2^4(2^3v + 3^3d(I/2))$ and $p \mid F(v)$. Observe

$$\begin{aligned} 4F(v) - \left[2^4(2^3v + 3^3d(I/2))\right]^2 &= 2^{14}v^2 + 2^{11} \cdot 3^3dIv + 3^3dI^2 + 2^6 \cdot 3^6d^2I^2 - 2^{14}v^2 \\ &\quad -2^{11} \cdot 3^3dIv - 2^6 \cdot 3^6d^2I^2 \\ &= 3^3dI^2. \end{aligned}$$

So $p \mid 3^3 dI^2$. But since $\gcd(F(v), 6d) = 1$ and $p \mid F(v)$, we must have that $p \nmid 6d$. Thus $p \mid I^2$ so that $p^2 \mid 3^3 dI^2$. Since $p^2 \mid \left(2^4(2^3 v + 3^3 d(I/2))\right)^2$, we have $p^2 \mid 4F(v)$. Since $p \neq 2$, this gives $p^2 \mid F(v)$. But this contradicts that $F(v)$ is squarefree.

Next, suppose $v_2(I) \in \{2, 3\}$. In this case, we will show that

$$\gcd\left(2(2^6 v + 3^3 d(I/2^{v_2(I)})), F(v)\right) = 1.$$

Suppose there exists some prime p such that $p \mid 2(2^6 v + 3^3 d(I/2^{v_2(I)}))$ and $p \mid F(v)$. Observe

$$\begin{aligned} 4F(v) \quad & - \quad \left[2(2^6 v + 3^3 d(I/2^{v_2(I)}))\right]^2 \\ & = \quad 2^{14} v^2 + 2^{9-v_2(I)} \cdot 3^3 dIv + 2^2 \cdot 3^3 dI \cdot 2^{2v_2(I)-2}(I/2^{v_2(I)})^2 + 2^2 \cdot 3^6 d^2 (I/2^{v_2(I)})^2 \\ & \quad\quad -2^{14} v^2 - 2^{9-v_2(I)} \cdot 3^3 dIv - 2^2 \cdot 3^6 d^2 (I/2^{v_2(I)})^2 \\ & = \quad 3^3 dI^2. \end{aligned}$$

So $p \mid 3^3 dI^2$, which contradicts that $F(v)$ is squarefree by the same reasoning as before.

So by the above arguments, along with the fact that $F(v) > 1$ for all $v \in V$ and $2 \nmid F(v)$, we have for any prime $p \mid F(v)$ that $p \mid A, B$ and $p^2 \nmid B$. Thus $p_v(x)$ is p-Eisenstein for each prime $p \mid F(v)$. Therefore $p_v(x)$ is irreducible over $\mathbb{Q}$ for each $v \in V$. Thus, the field generated by $p_v(x)$, call it F_v, is a cubic field.

We now show that $F_v \in C(d, \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1'')$ for each $v \in V$. First, suppose $v_2(I) = 1$. Observe that

$$\begin{aligned}\mathrm{disc}(p_v(x)) &= 4A^3 - 27B^2 \\ &= 4(3F(v))^3 - 27\left[2^4(2^3v + 3^3d(I/2))F(v)\right]^2 \\ &= 3^3F(v)^2\left(4F(v) - \left[2^4(2^3v + 3^3d(I/2))\right]^2\right) \\ &= 3^3F(v)^2(3^3dI^2) \\ &= d\left(3^3IF(v)\right)^2.\end{aligned}$$

Now suppose $v_2(I) \in \{2, 3\}$. Observe that

$$\begin{aligned}\mathrm{disc}(p_v(x)) &= 4A^3 - 27B^2 \\ &= 4(3F(v))^3 - 27\left[2(2^6v + 3^3d(I/2^{v_2(I)}))F(v)\right]^2 \\ &= 3^3F(v)^2\left(4F(v) - \left[2(2^6v + 3^3d(I/2^{v_2(I)}))\right]^2\right) \\ &= 3^3F(v)^2(3^3dI^2) \\ &= d\left(3^3IF(v)\right)^2.\end{aligned}$$

Thus, by Corollary 2.1.1 we have that $F_v \in C(d)$ for each $v \in V$ in both cases.

Since $F(v)$ is squarefree and $3 \nmid F(v)$, we have in both cases that $v_p(A) < 2$ for all primes p. We also have that A is odd, B is even, s_2 is even, and

$$\Delta_2 = d\left(3^3(I/2^{v_2(I)})F(v)\right)^2 \equiv d \equiv 1 \pmod{8}.$$

So by Theorem 2.4, we have that $(2)\mathcal{O}_{F_v} = \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''$.

Next, we compute Δ_{F_v} for each $v_2(I) \in \{1, 2, 3\}$ by using Theorem 2.2. Since (2) is completely split in $\mathcal{O}_{F_v}$, 2 does not ramify in F_v. Thus $2 \nmid \Delta_{F_v}$ in both cases. Next, observe in both cases that

$$A = 3F(v) \equiv 3 \cdot 2^{12}v^2 \equiv 3v^2 \pmod{27}.$$

This gives $A+1 \equiv 3v^2+1 \pmod{27}$. Also, since $v \equiv 1 \pmod 3$, we get $A \equiv 3 \pmod 9$. Furthermore,

$$B^2 \equiv (2^7v \cdot 2^{12}v^2)^2 \equiv 4v^6 \pmod{27}.$$

Since $v \equiv 1 \pmod 3$, we have by Lemma 2.11 that $B^2 \equiv A + 1 \pmod{27}$. Finally, note that $s_3 \equiv v_3(d) \pmod 2$. Thus by Theorem 2.2, $3^{v_3(d)} \parallel \Delta_{F_v}$ in both cases.

Now since $\gcd(d/3^{v_3(d)}, 6) = 1$ and d is squarefree, we have in both cases that

$$\prod_{\substack{p>3 \\ s_p \equiv 1 \pmod 2}} p = |d|/3^{v_3(d)}$$

and

$$\prod_{\substack{p>3 \\ 1 \le v_p(B) \le v_p(A)}} p^2 = F(v)^2.$$

Therefore, by Theorem 2.2 we have that

$$\Delta_{F_v} = \operatorname{sign}(d) \cdot 3^{v_3(d)} \left(|d|/3^{v_3(d)}\right) F(v)^2 = dF(v)^2.$$

Note that since distinct values of $v \in V$ give distinct values of $F(v)$, each value of Δ_{F_v} is distinct. Consequently, each of the cubic fields F_v are distinct.

In both cases, let $q_v(x) = \dfrac{p_v(3x+v)}{27}$. Then by Lemma 2.12, we have

$$q_v(x) = x^3 + vx^2 + \left(\frac{3v^2 - A}{9}\right)x + \left(\frac{v^3 - Av + B}{27}\right).$$

Observe that

$$v^2 - A/3 \equiv (1 - 2^{12})v^2 \equiv 0 \pmod{3}$$

and

$$v^3 - Av + B \equiv (1 - 3 \cdot 2^{12} + 2^{19})v^3 \equiv 0 \pmod{27}.$$

Thus, in both cases, we have that $q_v(x) \in \mathbb{Z}[x]$.

Since $p_v(x) = 27q_v\left(\dfrac{x-v}{3}\right)$, we have that $q_v(x)$ is irreducible over $\mathbb{Q}$ since $p_v(x)$ is irreducible over $\mathbb{Q}$. Moreover, $q_v(x)$ and $p_v(x)$ generate the same cubic extension F_v of $\mathbb{Q}$. Finally, if θ_v is a root of $q_v(x)$, then by Corollary 2.6.1 we have that

$$\begin{aligned} dI^2F(v)^2 &= \frac{\operatorname{disc}(p_v(x))}{3^6} \\ &= \operatorname{disc}(q_v(x)) \\ &= \operatorname{ind}(\theta_v)^2\Delta_{K_v} \\ &= \operatorname{ind}(\theta_v)^2 dF(v)^2, \end{aligned}$$

which gives $I = \operatorname{ind}(\theta_v)$. Therefore $I \in S_{d,\mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1''}$ and is an index of an algebraic integer in $F_v \in C(d, \mathcal{Q}_1\mathcal{Q}_1'\mathcal{Q}_1'')$ for each $v \in V$.

Case 3b: $(2) = \mathcal{Q}_3$.

Since $d \equiv 1 \pmod 8$, we have that $3^5d + 1 \equiv 4 \pmod 8$ so that $v_2(3^5d + 1) = 2$. Now set

$$F(x) = x^2 + 3^4dIx + 3^3dI^2\left(\frac{3^5d+1}{4}\right) \in \mathbb{Z}[x].$$

Again, we will apply Theorem 2.14 to obtain congruence conditions on x for which $F(x)$ is squarefree infinitely often.

Observe that $F(x)$ is clearly primitive. Next,

$$\begin{aligned} \operatorname{disc}(F(x)) &= \left(3^4dI\right)^2 - 4\cdot 3^3dI^2\left(\frac{3^5d+1}{4}\right) \\ &= 3^8d^2I^2 - 3^8d^2I^2 - 3^3dI^2 \\ &= -3^3dI^2 \neq 0. \end{aligned}$$

Now, let $n = 6d/3^{v_3(d)}$ for each $v_3(d) \in \{0, 1\}$. Again observe that n is squarefree. Furthermore, $F(1) \equiv 1 \pmod p$ for each $p \mid n$. Hence, for any prime p such that $p \mid n$, we have that $p \nmid F(1)$. Thus, with $r = 1$ and $q = 1$, we may apply Theorem 2.14 to conclude that there exist infinitely many positive integers $v \equiv 1 \pmod n$ such that $F(v)$ is squarefree.

For each case, we let V denote the same set as in previous cases so that $F(v) > 1$ for all $v \in V$ and no two distinct values of v in V can give the same value to $F(v)$. Since $v \equiv 1 \pmod n$ for all $v \in V$, we have $F(v) \equiv F(1) \equiv 1 \pmod p$ for each $p \mid n$. Thus $\gcd(F(v), 6d) = 1$ for each $v \in V$.

For each $v \in V$, set $p_v(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where

$$\begin{aligned} A &= 3F(v), \\ B &= (2v + 3^4 dI)F(v). \end{aligned}$$

We will show $p_v(x)$ is an Eisenstein polynomial for each $v \in V$.

First, we show that

$$\gcd(2v + 3^4 dI, F(v)) = 1.$$

Suppose there exists some prime p such that $p \mid 2v + 3^4 dI$ and $p \mid F(v)$. Observe

$$\begin{aligned} 4F(v) - (2v + 3^4 dI)^2 &= 4v^2 + 4 \cdot 3^4 dIv + 3^8 d^2 I^2 + 3^3 dI^2 - 4v^2 - 4 \cdot 3^4 dIv - 3^8 d^2 I^2 \\ &= 3^3 dI^2. \end{aligned}$$

Thus $p \mid 3^3 dI^2$. But since $\gcd(F(v), 6d) = 1$ and $p \mid F(v)$, we have $p \nmid 6d$. Thus $p \mid I^2$ so that $p^2 \mid 3^3 dI^2$. Since $p^2 \mid (2v + 3^4 dI)^2$, we have $p^2 \mid 4F(v)$. Since $p \neq 2$, this gives $p^2 \mid F(v)$. But this contradicts that $F(v)$ is squarefree.

Since $\gcd(2v + 3^4 dI, F(v)) = 1$, $3 \nmid F(v)$, and $F(v) > 1$, we have for any prime $p \mid F(v)$ that $p \mid A, B$ and $p^2 \nmid B$. Thus $p_v(x)$ is p-Eisenstein for each prime $p \mid F(v)$. Therefore $p_v(x)$ is irreducible over $\mathbb{Q}$ for each $v \in V$. Thus, the field generated by $p_v(x)$, call it F_v, is a cubic field.

We now show that $F_v \in C(d, \mathcal{Q}_3)$ for each $v \in V$. First, observe that

$$\begin{aligned} \operatorname{disc}(p_v(x)) &= 4A^3 - 27B^2 \\ &= 4(3F(v))^3 - 27\left[(2v + 3^4 dI)F(v)\right]^2 \\ &= 3^3 F(v)^2 \left[4F(v) - (2v + 3^4 dI)^2\right] \\ &= 3^3 F(v)^2 (3^3 dI^2) \\ &= d\left(3^3 I F(v)\right)^2. \end{aligned}$$

Thus by Corollary 2.1.1 we have that $F_v \in C(d)$ for each $v \in V$. Since $F(v)$ is squarefree and $3 \nmid F(v)$, we have that $v_p(A) < 2$ for all primes p. Since $2 \nmid I$, we also have that A and B are odd. So by Theorem 2.4, we have that $(2)\mathcal{O}_{F_v} = \mathcal{Q}_3$.

Next, we compute Δ_{F_v} by using Theorem 2.2. Since $(2)\mathcal{O}_{F_v} = \mathcal{Q}_3$, 2 is unramified in F_v. Thus we have that $2 \nmid \Delta_{F_v}$. Furthermore we have

$$A = 3F(v) \equiv 3v^2 \pmod{27}.$$

This gives $A + 1 \equiv 3v^2 + 1 \pmod{27}$. Also, since $v \equiv 1 \pmod{3}$, we have that $A \equiv 3 \pmod{9}$. Furthermore,

$$B^2 \equiv (2v \cdot v^2)^2 \equiv 4v^6 \pmod{27}.$$

Since $v \equiv 1 \pmod{3}$, we have by Lemma 2.11 that $B^2 \equiv A + 1 \pmod{27}$. Lastly, note that $s_3 \equiv v_3(d) \pmod{2}$. Thus, by Theorem 2.2, $3^{v_3(d)} \parallel \Delta_{F_v}$.

Now since $\gcd(d/3^{v_3(d)}, 6) = 1$ and d is squarefree, we have that

$$\prod_{\substack{p > 3 \\ s_p \equiv 1 \pmod 2}} p = |d|/3^{v_3(d)}$$

and

$$\prod_{\substack{p > 3 \\ 1 \leq v_p(B) \leq v_p(A)}} p^2 = F(v)^2.$$

Therefore, by Theorem 2.2 we have that

$$\Delta_{F_v} = \operatorname{sign}(d) \cdot 3^{v_3(d)}(|d|/3^{v_3(d)})F(v)^2 = dF(v)^2.$$

Note that since distinct values of $v \in V$ gives distinct values of $F(v)$, each value of Δ_{F_v} is distinct. Consequently, each of the cubic fields F_v are distinct.

Set $q_v(x) = \dfrac{p_v(3x+v)}{27}$. Then by Lemma 2.12, we have

$$q_v(x) = x^3 + vx^2 + \left(\frac{3v^2 - A}{9}\right)x + \left(\frac{v^3 - Av + B}{27}\right).$$

Observe that $v^2 - F(v) \equiv 0 \pmod 3$ and

$$v^3 - Av + B \equiv v^3 - 3v^2 \cdot v + 2v \cdot v^2 \equiv 0 \pmod{27}.$$

Thus $q_v(x) \in \mathbb{Z}[x]$.

Since $p_v(x) = 27q_v\left(\dfrac{x-v}{3}\right)$, we have that $q_v(x)$ is irreducible over $\mathbb{Q}$ since $p_v(x)$ is irreducible over $\mathbb{Q}$. Moreover, $q_v(x)$ and $p_v(x)$ generate the same cubic extension

F_v of $\mathbb{Q}$. Finally, if θ_v is a root of $q_v(x)$, then by Corollary 2.6.1 we have that

$$\begin{aligned} dI^2F(v)^2 &= \frac{\operatorname{disc}(p_v(x))}{3^6} \\ &= \operatorname{disc}(q_v(x)) \\ &= \operatorname{ind}(\theta_v)^2\Delta_{K_v} \\ &= \operatorname{ind}(\theta_v)^2 dF(v)^2, \end{aligned}$$

which gives $I = \operatorname{ind}(\theta_v)$. Therefore $I \in S_{d,\mathcal{Q}_3}$ and is an index of an algebraic integer in $F_v \in C(d, \mathcal{Q}_3)$ for each $v \in V$.

□

The following corollary is immediate.

Corollary 2.15.1. *For each squarefree $d \in \mathbb{Z}$ and $\mathcal{J} \in \mathcal{A}$, there exist infinitely many cubic fields $F \in C(d, \mathcal{J})$ whose ring of integers has a power basis.*

Since the natural numbers represented by an indicial form are quite irregular, so are the indices in any given cubic field. Hence, our choice to look at indices for the families of cubic fields $C(d, \mathcal{J})$ was essential for obtaining the well-structured sets in our result.

A natural way to extend our result is to generalize to factorizations of (p) for any prime p. Llorente and Nart expand the result of Theorem 2.4 to give conditions on a cubic field F for the factorizations of primes $p = 3$ and $p > 3$ in $\mathcal{O}_F$. Theorem 2.2 suggests that a result like ours for $p = 3$ might have a similar proof due to the potential wild ramification of 3. However, since $i(F)$ has no relationship with the prime ideal factorization of (3) like that of (2) according to Theorem 1.5, it is unclear how the index sets might change. One could do the same for any prime $p > 3$ or a combination of any finite number of primes.

3 Unbounded Minimal Indices

In this chapter, we will work towards proving the second of our two main results. Given an $N \in \mathbb{N}$ and a squarefree $d \in \mathbb{Z}$, we will show that there exist infinitely many $F \in C(d)$ such that $m(F) > N$. This will show that the minimal index is unbounded as we run through all cubic fields in $C(d)$.

3.1 An Indicial Form for Cubic Fields

The proofs of Hall and of Dummit and Kisilevsky on the unboundedness of the minimal index in the pure cubics and cyclic cubics, respectively, rely on convenient indicial forms. Both results are proved by showing that for each $N \in \mathbb{N}$, there exists a cubic field F in the cubic family such that $m(F) \notin \{1, ..., N\}$. This is accomplished by providing an indicial form for F and showing that it cannot assume any of these values. We aim to do this as well. However, in order to obtain an indicial form for a number field, we need an integral basis for its ring of integers. Hall and Dummit and Kisilevsky construct explicit integral bases for $C(-3)$ and $C(1)$, respectively. Since we want to extend their results to $C(d)$ for $d \neq -3, 1$, our first task will be to find integral bases for these families.

We provide a way to determine an integral basis for any cubic field by using the concept of *p-integral bases* for any prime p. Let F be a number field of degree n, $\mathcal{P}$ be a prime $\mathcal{O}_F$-ideal, and $\alpha \in F$. Write

$$\alpha \mathcal{O}_F = \prod_{\mathcal{P} \in I_{\mathcal{O}_F}} \mathcal{P}^{e_{\mathcal{P}}}$$

where $e_{\mathcal{P}} \in \mathbb{Z}$. For any prime ideal $\mathcal{P}$ dividing $p\mathcal{O}_K$ recall that $v_{\mathcal{P}}(\alpha) = e_P$. If $v_{\mathcal{P}}(\alpha) \geq 0$, then α is called a *$\mathcal{P}$-integral element* of F. If α is $\mathcal{P}$-integral for each prime ideal $\mathcal{P}$ of F such that $\mathcal{P} \mid p\mathcal{O}_F$, then α is called a *p-integral element* of F. Let $\{\beta_1, \beta_2, ..., \beta_n\}$ be a basis for F over $\mathbb{Q}$ where each β_i is a p-integral element of F. If every p-integral element α of F is given by $\alpha = a_1\beta_1 + ... + a_n\beta_n$, where the a_i are p-integral elements of $\mathbb{Q}$, then $\mathcal{B} = \{\beta_1, \beta_2, ..., \beta_n\}$ is called a *p-integral basis* for F.

The set of all p-integral elements of $\mathbb{Q}$ is the localization of $\mathbb{Z}$ at the prime ideal (p), given by

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

Since the elements of $\mathbb{Z}_{(p)}$ are the scalars for linear combinations of p-integral basis elements, a p-integral basis for F in θ-standard form need only have denominators that are powers of p.

Alaca [1] gives p-integral bases for cubic fields of the form $F = \mathbb{Q}(\theta)$, where θ is a root of the irreducible polynomial $x^3 - Ax + B$, with $A, B \in \mathbb{Z}$ and $v_p(A) < 2$ or $v_p(B) < 3$ for every prime p. The p-integral bases are provided in tables which we will not replicate here; the tables are subdivided according to $p = 2$, $p = 3$, and $p > 3$, and then further subdivided according to conditions on A and B.

By synthesizing the information encoded by the p-integral bases found within the tables, Alaca is able to produce an integral basis for any cubic field.

Theorem 3.1 (Alaca, Theorem 2.2 [1]). *Let $F = \mathbb{Q}(\theta)$ be a cubic field, where θ is a root of the irreducible polynomial $x^3 - Ax + B \in \mathbb{Z}[x]$ with $v_p(A) < 2$ or $v_p(B) < 3$ for every prime p. Suppose for any prime p that a p-integral basis of F is given by*

$$\mathcal{B}_p = \left\{1, \theta, (R_p + S_p\theta + \theta^2)/p^{T_p}\right\},$$

where $R_p, S_p, T_p \in \mathbb{Z}_{\geq 0}$*. Let* R *and* S *be integers such that*

$$R \equiv R_p \ (mod\, p^{T_p}), \ \ and \ \ S \equiv S_p \ (mod\, p^{T_p})$$

for all primes p*. Let* T *be the positive integer* $T = \prod_p p^{T_p}$*. Then*

$$\mathcal{B} = \left\{1, \theta, (R + S\theta + \theta^2)/T\right\}$$

is an integral basis for $\mathcal{O}_F$*, except in the case that* $v_3(B) = 0$*,* $A \equiv 3 \ (mod\, 9)$*, and* $B^2 \equiv A + 1 \ (mod\, 27)$*, in which an integral basis is given by*

$$\mathcal{B} = \left\{1, (B + \theta)/3, (R + S\theta + \theta^2)/T\right\}.$$

Hence, by knowing a p-integral basis for F for every prime p, we can determine an integral basis for $\mathcal{O}_F$. In the case of a pure cubic field $F = \mathbb{Q}(\sqrt[3]{ab^2})$, where $a, b \in \mathbb{N}$, squarefree, and relatively prime, we have an integral basis whose elements are determined explicitly by a and b. We do not have this luxury for the integral basis given in Theorem 3.1 for an arbitrary cubic field. In fact, the third basis element involves variables R and S whose exact values are unknown. However, the congruence conditions on R and S provided in the theorem will suffice for the proof of the main result of this chapter.

Given an integral basis for $\mathcal{O}_F$ of the form given in Theorem 3.1, we now compute the corresponding indicial form.

Lemma 3.2. *Let* $F = \mathbb{Q}(\theta)$ *be a cubic field with* θ *a root of* $x^3 - Ax + B \in \mathbb{Z}[x]$*. Suppose* $\mathcal{O}_F$ *has an integral basis of the form* $\mathcal{B} = \left\{1, \theta, \dfrac{R + S\theta + \theta^2}{T}\right\}$ *for some*

$R, S, T \in \mathbb{Z}_{\geq 0}$. Then an indicial form for $\mathcal{O}_F$ is given by

$$I_F(x, y) = Tx^3 + 3Sx^2y + \left(\frac{3S^2 - A}{T}\right) xy^2 + \left(\frac{S^3 - AS + B}{T^2}\right) y^3$$

for any $x, y \in \mathbb{Z}$.

Proof. Let $F = \mathbb{Q}(\beta)$, where $\beta \in \mathcal{O}_F$. By Proposition 1.3, $\text{ind}(\beta) = \text{ind}(\beta + c)$ for any $c \in \mathbb{Z}$. Thus we may assume without loss of generality that

$$\beta = x\theta + y\left(\frac{R + S\theta + \theta^2}{T}\right)$$

for some $x, y \in \mathbb{Z}$. In order to compute an indicial form for $\mathcal{O}_F$, we need to compute the determinant of the change-of-basis matrix from $\{1, \beta, \beta^2\}$ to $\mathcal{B}$. First, note

$$\begin{aligned}
\beta^2 &= \left[\theta x + \left(\frac{R + S\theta + \theta^2}{T}\right) y\right]^2 \\
&= \theta^2x^2 + 2\left(\frac{R\theta + S\theta^2 + \theta^3}{T}\right) xy + \left(\frac{R^2 + S^2\theta^2 + \theta^4 + 2RS\theta + 2R\theta^2 + 2S\theta^3}{T^2}\right) y^2 \\
&= \theta^2x^2 + 2\left(\frac{S\theta^2 + (R + A)\theta - B}{T}\right) xy \\
&\quad + \left(\frac{(S^2 + A + 2R)\theta^2 + (-B + 2RS + 2SA)\theta - 2SB + R^2}{T^2}\right) y^2 \\
&= \left(-\frac{2Bxy}{T} + \frac{(R^2 - 2BS)y^2}{T^2}\right) + \left(\frac{2(R + A)xy}{T} + \frac{(-B + 2RS + 2SA)y^2}{T^2}\right)\theta \\
&\quad + \left(x^2 + \frac{2Sxy}{T} + \frac{(S^2 + A + 2R)y^2}{T^2}\right)\theta^2 \\
&= \left(-Rx^2 - \frac{2(RS + B)xy}{T} - \frac{(R^2 + AR + 2SB + RS^2)y^2}{T^2}\right) \\
&\quad + \left(-Sx^2 + \frac{2(R + A - S^2)xy}{T} - \frac{(S^3 - AS + B)y^2}{T^2}\right)\theta \\
&\quad + \left(Tx^2 + 2Sxy + \frac{(S^2 + A + 2R)y^2}{T}\right)\left(\frac{R + S\theta + \theta^2}{T}\right).
\end{aligned}$$

Let

$$\begin{aligned}
C &= -Rx^2 - \frac{2(RS+B)xy}{T} - \frac{(R^2+AR+2SB+RS^2)y^2}{T^2},\\
D &= -Sx^2 + \frac{2(R+A-S^2)xy}{T} - \frac{(S^3-AS+B)y^2}{T^2},\\
E &= Tx^2 + 2Sxy + \frac{(S^2+A+2R)y^2}{T}.
\end{aligned}$$

Then

$$\begin{aligned}
I_F(x,y) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & x & y \\ C & D & E \end{vmatrix} &= Ex - Dy \\
&= Tx^3 + 3Sx^2y + \left(\frac{3S^2-A}{T}\right)xy^2 + \left(\frac{S^3-AS+B}{T^2}\right)y^3.
\end{aligned}$$

□

For a given $N \in \mathbb{N}$ and squarefree $d \in \mathbb{Z}$ with $d \neq -3, 1$, our goal will be to construct a cubic field F so that $I_F(x,y) \notin \{1, 2, ..., N\}$ for any $x, y \in \mathbb{Z}$. We will do this by using cubic nonresidues just as Hall [5] does. For each $n \in \{1, 2, ..., N\}$ we will find a prime p_n so that $I_F(x,y) \not\equiv \pm n \pmod{p_n}$. To use the technique of cubic nonresidues, we must eliminate the first three terms of the indicial form whenever we pass over to congruences modulo p_n. Thus, our goal will be to construct F according to an irreducible polynomial of the form $x^3 - Ax + B$, with $A, B \in \mathbb{Z}$ and $v_p(A) < 2$ or $v_p(B) < 3$ for every prime p, so that the values of A and B (along with R, S, and T, which are derived from A and B) make the coefficients of these terms congruent to zero modulo p_n.

3.2 The Main Result

Theorem 3.3. *Let $d \in \mathbb{Z}$ be squarefree with $d \neq -3, 1$. Let $N \in \mathbb{N}$. Then there exists a cubic field $F \in C(d)$ such that $m(F) > N$.*

Proof. Let

$$\begin{aligned} C &= 2^{v_2(d)} \cdot 3^{v_3(d)+1} \\ D &= d/(2^{v_2(d)} \cdot 3^{v_3(d)}) \end{aligned} \tag{2}$$

First, observe that since $d \neq -3, 1$, we have that $[\mathbb{Q}(\sqrt{-3}, \sqrt{-3d}) : \mathbb{Q}] = 4$. Now, by the Cheboratev Density Theorem, the primes that are completely split in $\mathbb{Q}(\sqrt{-3d})$ have density $1/2$ and are exactly those primes p for which $\left(\frac{-3d}{p}\right) = 1$. Likewise, the primes that are completely split in the cyclotomic field $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ have density $1/2$ and are exactly those primes p for which $p \equiv 1 \pmod 3$. Therefore the primes p for which both $p \equiv 1 \pmod 3$ and $\left(\frac{-3d}{p}\right) = 1$ are exactly those primes that are completely split in the compositum field $\mathbb{Q}(\sqrt{-3}, \sqrt{-3d})$ and have density $1/4$. Hence, there are infinitely many of them. So, we may choose distinct primes $p_0 = u$, p_1, ..., p_N such that $\gcd(p_n, N!D) = 1$, $p_n \equiv 1 \pmod 3$, and $\left(\frac{-3d}{p_n}\right) = 1$ for each $n \in \{0, 1, ..., N\}$.

Note $CD = 3d$. So, since $\left(\frac{-3d}{p_n}\right) = 1$ for each $n \in \{0, 1, ..., N\}$, each congruence equation $x^2 \equiv -CD \pmod{p_n}$ is solvable. Consequently, the congruence equations $Dx^2 \equiv -C \pmod{p_n}$ are also solvable for each n. Say

$$Da_n^2 \equiv -C \pmod{p_n}, \tag{3}$$

where $a_n \in \mathbb{Z}$.

Let $f(x) = Dx^2 + C + u^2 \in \mathbb{Z}[x]$. Observe

$$f(a_0) \equiv Da_0^2 + C + u^2 \equiv -C + C + u^2 \equiv 0 \pmod{u}.$$

Since $\gcd(u, D) = 1$ and $u \equiv 1 \pmod{3}$, we have $u \nmid 6D$. Thus $Da_0^2 \equiv -C \pmod{u}$ gives $a_0 \not\equiv 0 \pmod{u}$. Moreover, $f'(a_0) = 2Da_0 \not\equiv 0 \pmod{u}$. Therefore, by Hensel's Lemma there exists $\alpha \in \mathbb{Z}$ such that $f(\alpha) \equiv 0 \pmod{u^3}$ and $\alpha \equiv a_0 \pmod{u}$.

Define

$$t = \begin{cases} 0 & \text{if } d \equiv 1, 2 \pmod{4}, \\ 1 & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Since $\gcd(p_n, N!D) = 1$, we have that $p_n \nmid n$ for all $n \in \{1, 2, ..., N\}$. Note also that $p_n \equiv 1 \pmod{3}$. So, for each n, we may choose $r_n \in \mathbb{Z}$ relatively prime to p_n that satisfy two simultaneous conditions. The first is that $-2^{2t+2} \cdot 3^{1-v_3(d)} Dur_n^2$ is in a different cubic residue class than n modulo p_n; the second is that $\left(\frac{-2Cr_n}{p_n}\right) = 1$. These choices are possible since exactly $2/3$ of the elements of the set $(\mathbb{Z}/p_n\mathbb{Z})^*$ are in a different cubic residue class than n modulo p_n, and exactly $1/2$ of the elements in the set $(\mathbb{Z}/p_n\mathbb{Z})^*$ are quadratic residues modulo p_n. Therefore, at least $2/3 - 1/2 = 1/6$ of the elements of the set $(\mathbb{Z}/p_n\mathbb{Z})^*$ satisfy both conditions. Hence there are infinitely many choices for $r_n \in \mathbb{Z}$.

Note that the integers in the set $\{2, 3D, u, p_1, ..., p_N\}$ are pairwise relatively prime. Thus, we may apply the Chinese Remainder Theorem to conclude that the congruence equations

$$\begin{aligned}
&y \equiv 4 \pmod{8},\\
&y \equiv 1 \pmod{3D},\\
&y \equiv 1 \pmod{u^3},\\
&y \equiv -(2C)^{-1} r_1 \pmod{p_1},\\
&\quad\vdots\\
&y \equiv -(2C)^{-1} r_N \pmod{p_N} \qquad (4)
\end{aligned}$$

have a unique solution modulo $E = 24Du^3 p_1 \cdots p_N$. Observe that since $\left(\frac{-2Cr_n}{p_n}\right) = 1$ for each $n \in \{1, 2, ..., N\}$, each value on the right-hand side of these congruence equations is a perfect square with respect to its modulus. Thus, any particular solution y_0 that simultaneously satisfies all of these congruence equations is a quadratic residue modulo E. So, the arithmetic progression $\{y_0 + Ej\}_{j \in \mathbb{Z}_{\geq 0}}$ contains a perfect square, say $r^2 = y_0 + Ei$, where $i \in \mathbb{Z}_{\geq 0}$. Note that since $r^2 \equiv 4 \pmod{8}$, we have $2 \,\|\, r$. Furthermore, since $r^2 \equiv 1 \pmod{3D}$, we have $3 \nmid r$.

Now, let $g(x) = Dx^2 + Cr^2 \in \mathbb{Z}[x]$. We will apply Theorem 2.14 to obtain congruence conditions on x for which $g(x)$ is of the form $u^2 z$, where z is squarefree and $u \nmid z$.

Since $r^2 \equiv 1 \pmod{D}$ and $\gcd(C, D) = 1$, we have that $\gcd(D, Cr^2) = 1$. Hence, $g(x)$ is primitive. In addition, we have that $\operatorname{disc}(g(x)) = -4DCr^2 \neq 0$.

Since $6D, u^3, p_1 \cdots p_n$ are pairwise relatively prime, we may apply the Chinese Remainder Theorem to conclude there exists $R \in \mathbb{Z}$ such that

$$R \equiv 1 \pmod{6D},$$
$$R \equiv \alpha \pmod{u^3},$$
$$R \equiv a_n r \pmod{p_n},$$

for each $n \in \{1, 2, ..., N\}$. Since $3 \mid C$ and $3 \nmid DR$, observe

$$g(R) \equiv DR^2 + Cr^2 \equiv D \not\equiv 0 \pmod{3}.$$

This gives $g(R) \neq 0$.

Let $M = 6Dp_1 \cdots p_N u^2$. Note that $u \nmid 6Dp_1 \cdots p_N$ and $6Dp_1 \cdots p_N$ is squarefree. Thus M is the product of a power of u and a squarefree integer relatively prime to u. Moreover,

$$g(R) = DR^2 + Cr^2 \equiv D\alpha^2 + C \equiv -u^2 (\text{mod } u^3),$$

since $r^2 \equiv 1 \pmod{u^3}$ and α is a root of the polynomial $f(x) = Dx^2 + C + u^2$ modulo u^3. Therefore, we have that $u^2 \parallel DR^2 + Cr^2$.

Recall that $p_n \nmid 2Da_n$ and $r^2 \equiv -(2C)^{-1} r_n \not\equiv 0 \pmod{p_n}$ for each $n \in \{1, 2, ..., N\}$.

Thus,

$$
\begin{aligned}
&g'(R) = 2DR \equiv 2Da_n r \not\equiv 0 \pmod{p_n},\\
&g(R) \not\equiv 0 \pmod{3},\\
&g(R) \equiv DR^2 + Cr^2 \equiv D \equiv 1 \pmod{2},\\
&g(R) \equiv Cr^2 \equiv C \not\equiv 0 \pmod{p}
\end{aligned}
$$

for any $n \in \{1, 2, ..., N\}$ and for any prime $p \mid D$. Hence, $p_n \nmid g'(R)$ and $2^2, 3^2, p^2 \nmid g(R)$ for any prime $p \mid D$. Therefore, by Theorem 2.14 there exist infinitely many positive integers $v \equiv R \pmod{M}$ such that $g(v)$ is of the form $u^2 z$, where z is squarefree and $u \nmid z$.

Fix one such v. Then

$$
\begin{aligned}
&v \equiv 1 \pmod{6D},\\
&v \equiv \alpha \pmod{u^3},\\
&v \equiv a_n r \pmod{p_n}, \qquad (5)
\end{aligned}
$$

for each $n \in \{1, 2, ..., N\}$. Furthermore, $g(v) \equiv -u^2 \pmod{u^3}$. This gives that $u^2 \parallel g(v) = Dv^2 + Cr^2$.

Let $k, w \in \mathbb{Z}$ be given by

$$
k = \frac{Dv^2 + Cr^2}{u^2} \ \text{ and } \ w = Dv^2 - Cr^2.
$$

For each $n \in \{1, 2, ..., N\}$, recall $Da_n^2 \equiv -C \pmod{p_n}$ and $r^2 \equiv -(2C)^{-1} r_n \pmod{p_n}$.

Thus

$$w \equiv Dv^2 - Cr^2 \equiv D(a_n r)^2 - Cr^2 \equiv -Cr^2 - Cr^2 \equiv -2Cr^2 \equiv r_n \pmod{p_n}. \tag{6}$$

By the same reasoning, we have

$$k \equiv \frac{Dv^2 + Cr^2}{u^2} \equiv \frac{-Cr^2 + Cr^2}{u^2} \equiv 0 \pmod{p_n} \tag{7}$$

for each $n \in \{1, 2, ..., N\}$. Hence k is squarefree, and contains $p_1, ..., p_N$ as distinct prime factors.

Next, observe

$$\begin{aligned} u^2k + w &= (Dv^2 + Cr^2) + (Dv^2 - Cr^2) = 2Dv^2, \\ u^2k - w &= (Dv^2 + Cr^2) - (Dv^2 - Cr^2) = 2Cr^2. \end{aligned}$$

This gives

$$u^4k^2 - w^2 = (u^2k + w)(u^2k - w) = (2Dv^2)(2Cr^2) = 4DCv^2r^2 = 12dv^2r^2. \tag{8}$$

Since $v \equiv 1 \pmod 2$ and $2 \parallel r$, we have that

$$\begin{aligned} w = Dv^2 - Cr^2 &\equiv D \equiv 1 \pmod 2, \\ u^2k \equiv Dv^2 + Cr^2 &\equiv D \equiv 1 \pmod 2. \end{aligned}$$

Thus $2 \nmid kw$. Furthermore, since $v \equiv 1 \pmod 3$ and $3 \mid C$, we have

$$\begin{aligned} w &\equiv Dv^2 - Cr^2 \equiv D \not\equiv 0 \pmod 3, \\ u^2k &\equiv Dv^2 + Cr^2 \equiv D \not\equiv 0 \pmod 3, \end{aligned}$$

so that $3 \nmid kw$.

Since $u^2 \parallel Dv^2 + Cr^2$, we have that $u \nmid k$. Note that $w = u^2k - 2Cr^2$ so that if $u \mid w$, then $u \mid r^2$ since $u \neq 2, 3$. However, $r^2 \equiv 1 \pmod{u^3}$. Thus $u \nmid w$.

We now show that $\gcd(k, w) = 1$. Suppose to the contrary that $p \mid \gcd(k, w)$ for some prime p. Since $2, 3 \nmid k$, we have that $p \neq 2, 3$. Note that $p \mid u^2k \pm w$. We saw earlier that $u^2k + w = 2Dv^2$ and $u^2k - w = 2Cr^2$, so that $p \mid 2Dv^2$ and $p \mid 2Cr^2$. Since $p \neq 2, 3$, we have that $p \mid r^2$. So since $\gcd(r^2, D) = 1$, we have that $p \mid v^2$. Thus $p^2 \mid Dv^2 + Cr^2$. However, $k = \dfrac{Dv^2 + Cr^2}{u^2}$ is squarefree. Hence $p = u$. Then since $p \mid r$, we have that $u \mid r$. But $r^2 \equiv 1 \pmod{u^3}$, a contradiction. Therefore $\gcd(k, w) = 1$.

Now let $h(x) = x^3 - Ax + B \in \mathbb{Z}[x]$, where

$$\begin{aligned} A &= 3k^2u^2, \\ B &= 2k^2wu. \end{aligned} \tag{9}$$

From the previous arguments, we have for any prime p that $v_p(A) < 2$ or $v_p(B) < 3$. Since $u \mid A, B$ and $u^2 \nmid B$, we have that $h(x)$ is u-Eisenstein and thus irreducible over $\mathbb{Q}$. Thus, if θ is a root of $h(x)$, then $F = \mathbb{Q}(\theta)$ is a cubic field.

Observe that

$$\begin{aligned}\mathrm{disc}(h(x)) &= 4A^3 - 27B^2\\ &= 4(3k^2u^2)^3 - 27(2k^2wu)^2\\ &= 4\cdot 27k^4u^2(u^4k^2 - w^2)\\ &= 4\cdot 27k^4u^2(12dv^2r^2)\\ &= d(2^2\cdot 3^2k^2uvr)^2.\end{aligned}$$

Thus, by Corollary 2.1.1, we have that $F \in C(d)$.

We now show that the integers in the set $\{2, 3, u, k, w, v, r/2, D\}$ are pairwise relatively prime. So far, we have seen that $2 \nmid 3ukwvD$, $2 \parallel r$, $3 \nmid 2ukwvrD$, $u \nmid 6kwvrD$, $\gcd(k, w) = 1$, $v \equiv 1 \pmod{D}$, and $r^2 \equiv 1 \pmod{D}$.

First, we show that $\gcd(k, v) = 1$. Suppose to the contrary that $p \mid k$ and $p \mid v$ for some prime p. Since $2 \nmid v$ and $3 \nmid v$, we have $p \neq 2, 3$. Since $k = \dfrac{Dv^2 + Cr^2}{u^2}$, we have that $p \mid r$. Thus $p^2 \mid Dv^2 + Cr^2 = u^2k$. But since $v \equiv \alpha \not\equiv 0 \pmod{u}$ and $p \mid v$, we have that $p \neq u$. Therefore $p^2 \mid k$, which contradicts the fact that k is squarefree.

Similarly, we have that $\gcd(k, r) = 1$. Suppose to the contrary that $p \mid k$ and $p \mid r$ for some prime p. Since $r^2 \equiv 1 \pmod{D}$, we must have $p \nmid D$. So since $k = \dfrac{Dv^2 + Cr^2}{u^2}$, we have that $p \mid v$. Thus $p^2 \mid Dv^2 + Cr^2 = u^2k$. But again we have that $p \neq u$. Therefore $p^2 \mid k$, which contradicts the fact that k is squarefree.

Next, we show that $\gcd(w, r) = 1$. Suppose $p \mid w$ and $p \mid r$ for some prime p. Since $w = u^2k - 2Cr^2$, we have that $p \mid u^2k$. But $r \equiv 1 \pmod{u^3}$, so that $p \nmid u$. Therefore $p \mid k$. But then $p \mid w$ and $p \mid k$, whereas we have already shown that $\gcd(k, w) = 1$, a contradiction. Thus $\gcd(w, r) = 1$. Since $w = 2Dv^2 - u^2k$, the same argument shows that $\gcd(w, v) = 1$.

We also have that $\gcd(D,k)=1$. Suppose to the contrary that $p \mid D$ and $p \mid k$ for some prime p. Then $p \neq 2,3$. Since $k = \dfrac{Dv^2+Cr^2}{u^2}$, we have that $p \mid r$. But $r^2 \equiv 1 \pmod{D}$ so that $p \nmid D$, a contradiction. Similar reasoning shows that $\gcd(D,w)=1$.

Finally, we have that $\gcd(v,r)=1$. For if there exists some prime p such that $p \mid v$ and $p \mid r$, then $p^2 \mid k = \dfrac{Dv^2+Cr^2}{u^2}$, which contradicts that k is squarefree.

Therefore, the integers in the set $\{2,3,u,k,w,v,r/2,D\}$ are pairwise relatively prime, as desired. Now, by referring to the values $A=3k^2u^2$, $B=2k^2wu$, and $\operatorname{disc}(h(x)) = d(2^2\cdot 3^2k^2uvr)^2$, and partitioning the set of all primes by which, if any, of $\{2,3,u,k,w,vr/2,D\}$ they divide, we may easily compute $v_p(A)$, $v_p(B)$ and s_p for all primes p. Since $v_p(A)<2$ or $v_p(B)<3$ for any prime p, we may then apply Alaca's tables [1] to determine the corresponding p-integral bases for $\mathcal{O}_F$.

Most cases are easy to verify, but the cases $p=2$ and $p=3$ require some explanation. Observe

$$\begin{aligned}
&A \equiv 3k^2u^2 \equiv 3 \pmod{4},\\
&B \equiv 2k^2wu \equiv 2 \pmod{4},\\
&\Delta_2 \equiv d/2^{v_2(d)} \equiv 1,3 \pmod{4},\\
&s_2 = 6+v_2(d).
\end{aligned}$$

Thus, according to Alaca's table for $p=2$, this leaves us with three cases. We will determine the form of a 2-integral basis in each case.

First, suppose $v_2(d)=1$. Then $s_2=7$ and $s_2\equiv 1 \pmod{2}$. Hence, $\mathcal{O}_F$ has a 2-integral basis of the form $\{1,\theta,(R_2+S_2\theta+\theta^2)/2^2\}$, where $R_2,S_2\in\mathbb{Z}$ are determined according to the table. Second, suppose $v_2(d)=0$ and $\Delta_2\equiv 3 \pmod{4}$. Then $s_2=6$ and $\mathcal{O}_F$ has a 2-integral basis of the form $\{1,\theta,(R_2+S_2\theta+\theta^2)/2^2\}$. Third, suppose

$v_2(d) = 0$ and $\Delta_2 \equiv 1 \pmod 4$. Then $s_2 = 6$ and $\mathcal{O}_F$ has a 2-integral basis of the form $\{1, \theta, (R_2 + S_2\theta + \theta^2)/2^3\}$. Recall

$$t = \begin{cases} 0 & \text{if } d \equiv 1, 2 \pmod 4, \\ 1 & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

Thus, all three cases may be summarized by a 2-integral basis of the form

$$\left\{1, \theta, (R_2 + S_2\theta + \theta^2)/2^{3-v_2(d)-t}\right\}.$$

Note that since $ku \not\equiv 0 \pmod 3$, we have

$$A \equiv 3k^2u^2 \equiv 3(ku)^2 \equiv 3 \pmod 9.$$

Thus $v_3(A) = 1$. Moreover, it is clear that $v_3(B) = 0$ and $s_3 = 4+v_2(d) \in \{4, 5\}$. Now, according to Alaca's table for $p = 3$, this leaves us with two cases. If $B^2 \equiv 4 \pmod 9$, then $\mathcal{O}_F$ has a 3-integral basis of the form $\{1, \theta, (1 - B\theta + \theta^2)/3\}$. If $B^2 \not\equiv 4 \pmod 9$, then $\mathcal{O}_F$ has a 3-integral basis of the form $\{1, \theta, \theta^2\}$. Both cases may be summarized by a 3-integral basis of the form

$$\left\{1, \theta, (R_3 + S_3\theta + \theta^2)/3^{v_3(d)}\right\},$$

where $R_3, S_3 \in \mathbb{Z}$.

The information for all primes p is summarized in the table below. Note that all p-integral bases are given in the form $\left\{1, \theta, (R_p + S_p\theta + \theta^2)/p^{T_p}\right\}$, where $R_p, S_p, T_p \in \mathbb{Z}$ and are determined according to Alaca's tables.

prime p	$v_p(A)$	$v_p(B)$	s_p	p-integral basis
2	0	1	$6+v_2(d)$	$\left\{1,\theta,(R_2+S_2\theta+\theta^2)/2^{3-v_2(d)-t}\right\}$
3	1	0	$4+v_3(d)$	$\left\{1,\theta,(R_3+S_3\theta+\theta^2)/3^{v_3(d)}\right\}$
u	2	1	2	$\{1,\theta,\theta^2\}$
$p \mid k$	2	2	4	$\{1,\theta,\theta^2/p\}$
$p \mid w$	0	$v_p(w)$	0	$\{1,\theta,\theta^2\}$
$p \mid (vr/2)$	0	0	$2v_p(vr/2)$	$\left\{1,\theta,(R_p+S_p\theta+\theta^2)/p^{v_p(vr/2)}\right\}$
$p \mid D$	0	0	1	$\{1,\theta,\theta^2\}$
otherwise	0	0	0	$\{1,\theta,\theta^2\}$

We now show $B^2 \not\equiv A+1 \pmod{27}$. Suppose otherwise. Since $ku \not\equiv 0 \pmod 3$, we have by Lemma 2.11 that

$$A+1 \equiv 3k^2u^2+1 \equiv 3(ku)^2+1 \equiv 4(ku)^6 \equiv 4k^6u^6 \pmod{27}.$$

On the other hand,

$$B^2 \equiv 4k^4w^2u^2 \pmod{27}.$$

Hence $B^2 \equiv A+1 \pmod{27}$ gives $w^2 \equiv u^4k^2 \pmod{27}$. However, $u^4k^2 - w^2 = 12dv^2r^2$ by (8). Since $v_3(d) \in \{0,1\}$ and $3 \nmid vr$, this is a contradiction.

Therefore, by Theorem 3.1 an integral basis for $\mathcal{O}_F$ is given by

$$\mathcal{B} = \left\{1,\theta,(R+S\theta+\theta^2)/T\right\},$$

where $R \equiv R_p \pmod{p^{T_p}}$ and $S \equiv S_p \pmod{p^{S_p}}$ for all primes p, and

$$T = 2^{3-v_2(d)-t} \cdot 3^{v_3(d)} k(vr/2) = 2^{2-v_2(d)-t} \cdot 3^{v_3(d)} kvr.$$

Note that $p_n \parallel k$ for each $n \in \{1, ..., N\}$ by (7). Hence $R, S \equiv 0 \pmod{p_n}$.

By Lemma 3.2, an indicial form for $\mathcal{O}_F$ is given by

$$I_F(x,y) = Tx^3 + 3Sx^2y + \left(\frac{3S^2 - A}{T}\right)xy^2 + \left(\frac{S^3 - AS + B}{T^2}\right)y^3,$$

where $x, y \in \mathbb{Z}$. Since $p_n \parallel k$, we have by (9) that $p_n^2 \mid A$ and $p_n^2 \mid B$ for each n. Thus, the coefficients of the x^3, x^2y and xy^2 terms have p_n as a factor for all n. Set $k_n = k/p_n$ for each n. Then, with reference to (2), (3), (4), (5), (6), and (9), we have for each $n \in \{1, ..., N\}$ that

$$\begin{aligned}
I_F(x,y) &\equiv \left(\frac{T}{p_n}\right)^{-2} \frac{B}{p_n^2} y^3 \\
&\equiv (2^{2-v_2(d)-t} \cdot 3^{v_3(d)} k_n vr)^{-2} (2k_n^2 wu) y^3 \\
&\equiv 2^{2v_2(d)+2t-3} \cdot 3^{-2v_3(d)} wu(vr)^{-2} y^3 \\
&\equiv 2^{2v_2(d)+2t-3} \cdot 3^{-2v_3(d)} r_n u(a_n r^2)^{-2} y^3 \\
&\equiv 2^{2v_2(d)+2t-3} \cdot 3^{-2v_3(d)} r_n u a_n^{-2} r^{-4} y^3 \\
&\equiv 2^{2v_2(d)+2t-3} \cdot 3^{-2v_3(d)} r_n u(-DC^{-1})(4C^2 r_n^{-2}) y^3 \\
&\equiv -2^{2v_2(d)+2t-1} \cdot 3^{-2v_3(d)} r_n^{-1} u(DC) y^3 \\
&\equiv -2^{3v_2(d)+2t-1} \cdot 3^{1-v_3(d)} D u r_n^{-1} y^3 \\
&\not\equiv \pm n \pmod{p_n},
\end{aligned}$$

since $-2^{2t+2} \cdot 3^{1-v_3(d)} D u r_n^2$ is in a different cubic residue class than n modulo p_n.

Now, if $I_F(x, y) = \pm n$ for some $x, y \in \mathbb{Z}$, then $I_F(x, y) \equiv \pm n \pmod{p_n}$. Therefore, $I_F(x, y) \neq \pm n$ for any $n \in \{1, 2, ..., N\}$. This gives $m(F) > N$.

□

While this result shows that the minimal index is unbounded as F varies in $C(d)$, it does not tell us anything about which natural numbers occur as minimal indices. A natural generalization of our result would be a result like that of Spearman, Yang, and Yoo [12], in which we determine the minimal index sets for each squarefree $d \in \mathbb{Z}$. Showing that they are infinite for each d would immediately imply our result. Spearman, Yang, and Yoo show that any cubefree natural number is the index of an algebraic integer in infinitely many pure cubics. Thus, the minimal index set in this case at least includes the set of all cubefree natural numbers. However, they are only able to do this because of the explicit nature of the indicial form they use for the pure cubics. Since we do not know the exact coefficients of the indicial form we develop in Lemma 3.2, a result like theirs which uses our integral basis does not seem possible.

The following corollary of the previous result is immediate.

Corollary 3.3.1. *Let $d \in \mathbb{Z}$ be squarefree. Then there exist infinitely many cubic fields $F \in C(d)$ whose ring of integers does not have a power basis.*

In tandem with Corollary 2.15.1, this gives us a connection between the two main results proved in this dissertation. While neither corollary conveys the full power of our results, they nevertheless reiterate the relationship between indices and monogenic number fields.

References

[1] Şaban Alaca, *P-integral bases of a cubic field*, Proc. Amer. Math. Soc. 126 (1998), no. 7, 1949-1953.

[2] R. Dedekind, *Über der Zussamenhang zwischen der Theorie der Ideals und der Theorie der höheren Kongruenzen*, Abh. Akad. Wiss. Göttigen, Math.-Phys. Kl. 23 (1878), 1-23.

[3] D. S. Dummit and H. Kisilevsky, *Indices in Cyclic Cubic Fields*, pp. 29-42 of ”Number Theory and Algebra” (H. Zassenhaus, ed.), Academic Press, New York, 1977.

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

[5] Marshall Hall, Jr., *Indices in cubic fields*, Bull. Amer. Math. Soc. 43 (1937), 104-108.

[6] James G. Huard, *Cyclic cubic fields that contain an integer of a given index*, Lecture Notes in Math, 751 (1979), 195-199.

[7] Pascual Llorente and Enric Nart, *Effective Determination of the Decomposition of the Rational Primes in a Cubic Field*, Proceedings of the Amer. Math. Soc. 87 (1983) no. 4, 579-585.

[8] T. Nagel, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Hamburg 1 (1922), 179-194.

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

[10] Blair K. Spearman and Kenneth S. Williams, *Cubic fields with a power basis*, Rocky Mountain Journal of Mathematics 31 (2001), no. 3, 1103-1109.

[11] Blair K. Spearman and Kenneth S. Williams, *Indices of integers in cyclic cubic fields*, International Mathematical Forum 3 (2008), no. 32, 1595-1606.

[12] Blair K. Spearman, Qiduan Yang, and Jeewon Yoo, *Minimal Indices of Pure Cubic Fields*, Archiv der Mathematik 106 (2016), no. 1, 35-40.

VITA

Jeremy Taylor Smith was born April 1, 1991, in Alexandria, Louisiana. He is the son of Brian and Shannon Smith. A 2009 graduate of Caddo Mills High School, in Caddo Mills, Texas, he received a Bachelor of Science degree with a major in Mathematics from University of Dallas, in Irving, Texas, in 2012.

In August 2012, he enrolled at Texas Christian University where he received his Master of Science degree in Mathematics in 2014 and his Doctor of Philosophy degree in Mathematics in 2018. While working on his doctorate, he worked as a Graduate Assistant for the Department of Mathematics.

ABSTRACT

INDICES OF ALGEBRAIC INTEGERS IN CUBIC FIELDS

by Jeremy Taylor Smith, Ph.D., 2018
Department of Mathematics
Texas Christian University

Dissertation Advisor: George Gilbert, Associate Professor and Chair of Mathematics

Let $F = \mathbb{Q}(\theta)$ be a cubic field with $\theta \in \mathcal{O}_F$. The index of θ in $\mathcal{O}_F$ is the $\mathbb{Z}$-module index $\mathrm{ind}(\theta) := [\mathcal{O}_F : \mathbb{Z}[\theta]] \in \mathbb{N}$. The minimal index of F is given by $m(F) = \min\limits_{\theta \in \mathcal{O}_F} \mathrm{ind}(\theta)$. Let $d \in \mathbb{Z}$ be squarefree. If $d \neq 1$, let $C(d)$ denote the set of all non-cyclic cubic fields whose normal closure contains the unique quadratic subfield $\mathbb{Q}(\sqrt{d})$. Let $C(1)$ denote the set of all cyclic cubic fields.

For a given squarefree $d \in \mathbb{Z}$, we determine the set of all index values assumed by algebraic integers in cubic fields in each subfamily of $C(d)$ with a given factorization of the prime ideal (2). We also determine that each index assumed is assumed by infinitely many algebraic integers in distinct cubics fields within this subfamily. Moreover, for each $N \in \mathbb{N}$, we show that there exists a cubic field $F \in C(d)$ with $m(F) > N$.