Indices of Integers in Cyclic Cubic Fields

Blair K. Spearman

Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, British Columbia, Canada V1V 1V7
blair.spearman@ubc.ca

Kenneth S. Williams

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
kwilliam@connect.carleton.ca

Abstract

The field index $i(K)$ of a cyclic cubic field $K$ is 1 or 2. For $i \in \{1, 2\}$ we determine explicitly the set

$L_i := \{ n \in \mathbb{N} \mid n = \text{ind}(\theta), \text{ where } \theta \text{ is an algebraic integer such that } \mathbb{Q} (\theta) \text{ is a cyclic cubic field with field index } i \}.$

Moreover for each $\ell \in L_i$ we show that there exist infinitely many cyclic cubic fields $K$ with field index $i$ such that $O_K$ possesses an element of index $\ell$.

Mathematics Subject Classification: 11R16, 11S05

Keywords: cyclic cubic field, index, field index, discriminant

1 Introduction

Let $I \in \mathbb{N}$. Huard [1, Theorem B, p. 189] has proved that there exist infinitely many cyclic cubic fields that contain an integer of index $I$. It is known that
the field index of a cyclic cubic field is 1 or 2 [3, p. 585]. For \( i \in \{1, 2\} \) we set

\[
C_i := \{ K \mid K \text{ is a cyclic cubic field with field index } i(K) = i \}.
\]

In this paper we investigate the indices of integers in \( C_i \). To do this we define for \( i \in \{1, 2\} \)

\[
L_i := \{ n \in \mathbb{N} \mid n = \text{ind}(\theta), \text{ where } \theta \text{ is an algebraic integer such that } Q(\theta) \text{ is a cyclic cubic field with field index } i \}.
\]

We determine the set \( L_i \) explicitly and show that each element of \( L_i \) occurs as an index for infinitely many \( K \) in \( C_i \). We prove the following theorem in Section 3 after some preliminary results are proved in Section 2.

**Theorem 1.1.**

(i) \( L_1 = \{ 8^a n \mid a \in \mathbb{N} \cup \{0\}, n \in 2\mathbb{N} - 1 \} \).

(ii) \( L_2 = \{ 2n \mid n \in \mathbb{N} \} \).

(iii) For each \( i \in \{1, 2\} \) and each \( \ell \in L_i \) there exist infinitely many cyclic cubic fields \( K \) in \( C_i \) such that \( O_K \) possesses an element of index \( \ell \).

Although every positive integer is an index of some cyclic cubic field, Theorem 1.1 shows that the density of indices is \( 4/7 = 0.56 \ldots \) in the field index one case and \( 1/2 = 0.5 \) in the field index two case.

## 2 Preliminary Results

If \( K \) is a cubic field, the cubic trinomial \( x^3 + Ax + B \) \((A, B \in \mathbb{Z})\) is said to be a defining polynomial for \( K \) if \( x^3 + Ax + B \) possesses a root \( \theta \in \mathbb{C} \) such that \( K = \mathbb{Q}(\theta) \).

A cubic trinomial \( x^3 + Ax + B \) \((A, B \in \mathbb{Z})\) is said to satisfy the simplifying assumption if

\[
R^2 \mid A, \quad R^3 \mid B \quad (R \in \mathbb{N}) \implies R = 1.
\]

**Lemma 2.1.** Let \( K \) be a cyclic cubic field. Let \( x^3 + Ax + B \) be a defining polynomial for \( K \) satisfying (2.1). Then

\[
i(K) = \begin{cases} 
1, & \text{if } B \text{ is odd,} \\
2, & \text{if } B \text{ is even.}
\end{cases}
\]
Proof. If $B$ is odd then the discriminant $-4A^3 - 27B^2$ of $x^3 + Ax + B$ is also odd and thus $i(K) = 1$.

If $B$ is even we suppose that $i(K) = 1$ and obtain a contradiction so that $i(K) = 2$. Let $\theta \in \mathbb{C}$ be a root of $x^3 + Ax + B$. As $x^3 + Ax + B$ is a defining polynomial for $K$ and $K$ is a normal extension of $\mathbb{Q}$ we have $K = \mathbb{Q}(\theta)$. Let $\langle \theta \rangle = P_1P_2 \cdots P_r$ be the prime ideal factorization of the principal ideal $\langle \theta \rangle$ in $O_K$. As $\theta^3 + A\theta + B = 0$ we have $N(\theta) = -B$ so that

$$N(P_1)N(P_2) \cdots N(P_r) = N(\langle \theta \rangle) = |N(\theta)| = |B| \equiv 0 \pmod{2}.$$ 

Hence $2 \mid N(P_j)$ for some $j \in \{1, 2, \ldots, r\}$. Thus $N(P_j) = 2^t$ for some $t \in \mathbb{N}$. Since $2$ does not divide the discriminant of any cyclic cubic field [2, Theorem, p. 4], $2$ does not ramify in $K$. Thus, as $K/\mathbb{Q}$ is a normal extension of degree 3, either $\langle 2 \rangle$ is a prime ideal of $O_K$ or $\langle 2 \rangle = \wp_1\wp_2\wp_3$ for distinct prime ideals $\wp_1, \wp_2, \wp_3$ of $O_K$. If $\langle 2 \rangle = \wp_1\wp_2\wp_3$ then by [5, Corollary, p. 180] we have $i(K) = 2$, contradicting $i(K) = 1$. Thus $\langle 2 \rangle$ is a prime ideal of $O_K$ so $\langle 2 \rangle = P_j$. Hence $\langle 2 \rangle \mid \langle \theta \rangle$ and so $2 \mid \theta$ in $O_K$. Thus $\theta/2 \in O_K$. As $(\theta/2)^3 + (A/4)(\theta/2) + (B/8) = 0$ and $A/4$, $B/8 \in \mathbb{Q}$, the monic irreducible cubic polynomial in $\mathbb{Z}[x]$ satisfied by $\theta/2$ is $x^3 + (A/4)x + (B/8)$. Thus $A/4 \in \mathbb{Z}$ and $B/8 \in \mathbb{Z}$. This contradicts (2.1). \qed

Lemma 2.2. Let $K \in C_1$. If $\theta \in O_K$ has even index then $(\theta + k)/2 \in O_K$ for some $k \in \mathbb{Z}$.

Proof. Suppose that $\theta \in O_K$ has even index. As $\theta \in O_K$, there exist $a, b, c \in \mathbb{Z}$ such that $\theta$ is a root of $g(x) = x^3 + ax^2 + bx + c$. Then $3\theta + a \in O_K$ is a root of $h(x) = x^3 + Ax + B$, where $A = -3a^2 + 9b \in \mathbb{Z}$ and $B = 2a^3 - 9ab + 27c \in \mathbb{Z}$. We note that $\text{disc}(h(x)) = 3^6\text{disc}(g(x))$. As $\text{ind}(\theta) \equiv 0 \pmod{2}$, we have $\text{disc}(g) \equiv 0 \pmod{2}$ and so $-4A^3 - 27B^2 = \text{disc}(h) \equiv 0 \pmod{2}$. Thus $B \equiv 0 \pmod{2}$. If either $2^2 \nmid A$ or $2^3 \nmid B$ then by Lemma 2.1, we have $i(K) = 2$, contradicting $K \in C_1$. Thus $2^2 \mid A$ and $2^3 \mid B$ so $(3\theta + a)/2 \in O_K$. Hence $(\theta + a)/2 = (3\theta + a)/2 - \theta \in O_K$ as required. \qed

Lemma 2.3. Let $K \in C_1$. Let $\theta \in O_K$ be such that $K = \mathbb{Q}(\theta)$. Then

$$\text{ind}(\theta) = 8^an$$

for some $a \in \mathbb{N} \cup \{0\}$ and $n \in 2\mathbb{N} - 1$.

Proof. Suppose that there exists $\theta \in O_K$ and $K = \mathbb{Q}(\theta)$ with $2^t \parallel \text{ind}(\theta)$ for some $t \in \mathbb{N} \cup \{0\}$ with $t \not\equiv 0 \pmod{3}$. Let $\theta^* \in O_K$ have the least
such value of $t$, say $t^\ast$. Then, by Lemma 2.2, there exists $k \in \mathbb{Z}$ such that $(\theta^\ast + k)/2 \in O_K$ and $K = \mathbb{Q}((\theta^\ast + k)/2)$. Hence $2^{t^\ast - 3} \parallel \text{ind}((\theta^\ast + k)/2)$ so $t^\ast - 3 \geq 0$. As $t^\ast - 3 \not\equiv 0 \pmod{3}$ this contradicts the minimality of $t^\ast$. Hence, for every $\theta \in O_K$ with $K = \mathbb{Q}(\theta)$ we have $2^t \parallel \text{ind}((\theta + k)/2)$ so $t^\ast - 3 \geq 0$. As $t^\ast - 3 \not\equiv 0 \pmod{3}$ this contradicts the minimality of $t^\ast$. Hence, for every $\theta \in O_K$ with $K = \mathbb{Q}(\theta)$ we have $2^t \parallel \text{ind}((\theta + k)/2)$ with $t \equiv 0 \pmod{3}$.

Thus $\text{ind}((\theta + k)/2) = 2^n$ for some $a \in \mathbb{N} \cup \{0\}$ and $n \in 2\mathbb{N} - 1$.

We next state a theorem of Nagel [6] in the case of a quadratic polynomial.

**Proposition 2.1.** Let $f(x) \in \mathbb{Z}[x]$ be a quadratic polynomial which is primitive and has a nonzero discriminant. Then there exist infinitely many $x \in \mathbb{N}$ such that $f(x)$ is squarefree.

In [7] the following extension of Proposition 2.1 was proved.

**Proposition 2.2.** Let $d \neq 0$, $e$, $f \in \mathbb{Z}$ be such that $\gcd(d, e, f) = 1$ and $e^2 - 4df \neq 0$. Let $m$ be a positive squarefree integer. Let $r$ be an integer such that $dr^2 + er + f \neq 0$ and for every prime $p$ dividing $m$, $p^2 \nmid dr^2 + er + f$ we have $p \nmid 2dr + e$. Then there exist infinitely many positive integers $x \equiv r \pmod{m}$ such that $dx^2 + ex + f$ is squarefree.

We need the following special cases of Proposition 2.2.

**Lemma 2.4.** (a) Let $d, e, f \in \mathbb{N}$ be such that $\gcd(d, e, f) = 1$, $e^2 - 4df \neq 0$ and $3 \parallel e^2 - 4df$. Then for any $r \in \mathbb{Z}$ there exist infinitely many positive integers $v \equiv r \pmod{3}$ such that $dv^2 + ev + f$ is squarefree.

(b) Let $e, f \in \mathbb{N}$ be such that $e^2 - 4f \neq 0$, $e \equiv 0 \pmod{3}$ and $f \equiv 2 \pmod{3}$. Then there exist infinitely many positive integers $v \not\equiv 0 \pmod{3}$ such that $v^2 + ev + f$ is squarefree.

(c) Let $d, f \in \mathbb{N}$ be such that $\gcd(d, f) = 1$. Then there exist infinitely many positive integers $v \not\equiv 0 \pmod{3}$ such that $dv^2 + f$ is squarefree.

## 3 Proof of Theorem 1.1.

We first examine $L_1$. By Lemma 2.3 the only possible integers in $L_1$ are those of the form $8^an$, where $a \in \mathbb{N} \cup \{0\}$ and $n \in 2\mathbb{N} - 1$. We show that all such integers are in $L_1$ and occur as indices of infinitely many cyclic cubic
fields of index 1. It is enough to do this for the odd positive integers since
\( \text{ind}(2^a\theta) = 8^a\text{ind}(\theta) \) for \( \mathbb{Q}(\theta) \in C_1 \). As \( \text{ind}(3^b\theta) = 3^{3b}\text{ind}(\theta) \) for \( \mathbb{Q}(\theta) \in C_1 \) we can further restrict \( n \) to satisfy \( 3^3 \nmid n \).

Let \( I \in 2\mathbb{N} - 1 \) be such that \( 3^3 \nmid I \). We show that \( I \in L_1 \) and that there
exist infinitely many cyclic cubic fields \( K \) such that \( \mathcal{O}_K \) possesses an element of index \( I \). Define \( F(x) \in \mathbb{Z}[x] \) by

\[
F(x) = \begin{cases} 
x^2 + Ix + I^2, & \text{if } 3 \nmid I, \\
3x^2 + Ix + (I^2/9), & \text{if } 3 \parallel I, \\
x^2 + 9Ix + 27I^2, & \text{if } 3^2 \parallel I.
\end{cases}
\]

If \( 3 \nmid I \) by Lemma 2.4(a) there exist infinitely many positive integers \( v \equiv I + 1 \) (mod 3) such that \( F(v) \) is squarefree. If \( 3 \parallel I \) again by Lemma 2.4(a) there exist infinitely many positive integers \( v \equiv (I/3) + 1 \) (mod 3) such that \( F(v) \) is squarefree. If \( 3^2 \parallel I \) by Lemma 2.4(b) there exist infinitely many positive integers \( v \not\equiv 0 \) (mod 3) such that \( F(v) \) is squarefree. We denote the
set of such \( v \) by \( V \) in each of the three cases \( 3 \nmid I \), \( 3 \parallel I \) and \( 3^2 \parallel I \).

We show that \( 2 \nmid F(v) \) for \( v \in V \). Suppose \( 2 \mid F(v) \). Then by (3.1) we have \( 2 \mid v \) and \( 2 \mid I \), contradicting that \( 2 \nmid I \).

Next we note that it is easy to check using (3.1) and the congruences modulo 3 satisfied by \( v \in V \) that \( F(v) \equiv 1 \) (mod 3) for \( v \in V \).

For \( v \in V \) we have

\[
F(v) = \begin{cases} 
\frac{1}{4}((2v + I)^2 + 3I^2), & \text{if } 3 \nmid I, \\
\frac{1}{12}((6v + I)^2 + 3(I/3)^2), & \text{if } 3 \parallel I, \\
\frac{1}{4}((2v + 9I)^2 + 27I^2), & \text{if } 3^2 \parallel I.
\end{cases}
\]

As \( 2 \nmid F(v) \), \( 3 \nmid F(v) \) and \( F(v) \) is squarefree, we see that the only primes \( p \)
dividing \( F(v) \) satisfy \( p \equiv 1 \) (mod 3).

We now show that for \( v \in V \)

\[
\begin{cases} 
gcd(F(v), 2v + I) = 1, & \text{if } 3 \nmid I, \\
gcd(F(v), 6v + I) = 1, & \text{if } 3 \parallel I, \\
gcd(F(v), 2v + 9I) = 1, & \text{if } 3^2 \parallel I.
\end{cases}
\]
Let $p$ be a prime divisor of

$$
\begin{cases}
\gcd(F(v), 2v + I), & \text{if } 3 \nmid I, \\
\gcd(F(v), 6v + I), & \text{if } 3 \mid I, \\
\gcd(F(v), 2v + 9I), & \text{if } 3^2 \mid I.
\end{cases}
$$

As $p \mid F(v)$ and $F(v) \equiv 1 \pmod{3}$ we see that $p \neq 3$. From the identities

$$
\begin{cases}
4F(v) - (2v + I)^2 = 3I^2, & \text{if } 3 \nmid I, \\
9F(v) - (6v + I)^2 = \frac{1}{3}I^2, & \text{if } 3 \mid I, \\
4F(v) - (2v + 9I)^2 = 27I^2, & \text{if } 3^2 \mid I,
\end{cases}
$$

we deduce that $p \mid \gcd(I, v)$. Then, by (3.1), $p^2 \mid F(v)$, contradicting that $F(v)$ is squarefree. This completes the proof of (3.3).

From the congruences (mod 3) satisfied by $v \in V$ we have

$$
\begin{cases}
2v + I \equiv 2 \pmod{3}, & \text{if } 3 \nmid I, \\
6v + I \equiv 3I + 6 \equiv 6 \pmod{9}, & \text{if } 3 \mid I, \\
2v + 9I \not\equiv 0 \pmod{3}, & \text{if } 3^2 \mid I.
\end{cases}
$$

(3.4)

To summarize we have shown that for each $v \in V$ we have $F(v) \in \mathbb{N}$, $F(v) > 1$, $2 \nmid F(v)$, $3 \nmid F(v)$, $F(v)$ is squarefree, and that (3.3) and (3.4) hold.

For $v \in V$ we define a cubic polynomial $p(x) \in \mathbb{Z}[x]$ by

$$
p(x) = \begin{cases}
x^3 - 3F(v)x + (2v + I)F(v), & \text{if } 3 \nmid I, \\
x^3 - 9F(v)x + 3(6v + I)F(v), & \text{if } 3 \mid I, \\
x^3 + vx^2 + \left(\frac{v^2 - F(v)}{3}\right)x + \left(\frac{v^3 - F(v)v + 9IF(v)}{27}\right), & \text{if } 3^2 \mid I.
\end{cases}
$$

(3.5)

We have

$$
\text{disc}(p(x)) = \begin{cases}
3^4I^2F(v)^2, & \text{if } 3 \nmid I, \\
3^4I^2F(v)^2, & \text{if } 3 \mid I, \\
I^2F(v)^2, & \text{if } 3^2 \mid I.
\end{cases}
$$

(3.6)
We observe that
\[(3.7) \quad q(x) = 3^3 p \left( \frac{x - v}{3} \right) = x^3 - 3F(v)x + (2v + 9I)F(v), \text{ if } 3^2 \parallel I.\]

We set
\[A = \begin{cases} 
-3F(v), \quad &\text{if } 3 \nmid I, \\
-9F(v), \quad &\text{if } 3 \mid I, \\
-3F(v), \quad &\text{if } 3^2 \parallel I,
\end{cases}\]

and
\[B = \begin{cases} 
(2v + I)F(v), \quad &\text{if } 3 \nmid I, \\
3(6v + I)F(v), \quad &\text{if } 3 \mid I, \\
(2v + 9I)F(v), \quad &\text{if } 3^2 \parallel I,
\end{cases}\]

so that
\[x^3 + Ax + B = \begin{cases} 
p(x), \quad &\text{if } 3 \nmid I \text{ or } 3 \mid I, \\
q(x), \quad &\text{if } 3^2 \parallel I,
\end{cases}\]

and
\[-4A^3 - 27B^2 = C^2,\]

where
\[C = \begin{cases} 
3^2 IF(v), \quad &\text{if } 3 \nmid I \text{ or } 3 \mid I, \\
3^3 IF(v), \quad &\text{if } 3^2 \parallel I.
\end{cases}\]

We show that \(x^3 + Ax + B\) satisfies (2.1). Suppose \(R \in \mathbb{N}\) is such that \(R^2 \mid A\) and \(R^3 \mid B\). If \(3 \nmid I\) or \(3^2 \mid I\) then \(A\) is squarefree so \(R = 1\). If \(3 \mid I\) then the only square dividing \(A\) is \(3^2\) so \(R \mid 3\). Moreover, as \(F(v) \equiv 1 \pmod{3}\) and \(v \equiv I/3 + 1 \pmod{3}\) in this case we have
\[B = 3(6v + I)F(v) \equiv 3(6v + I) \equiv 3(3I + 6) \equiv 18 \pmod{27},\]

so that \(R \neq 3\). Thus \(R = 1\).

We show next that \(p(x)\) is irreducible over \(\mathbb{Q}\) for \(v \in V\). In the case \(3^2 \parallel I\) it suffices to prove that \(q(x)\) is irreducible in view of (3.7). We can choose a prime \(p \neq 2, 3\) with \(p \mid F(v)\). Clearly \(p \mid A\) and \(p \mid B\). From (3.3) we deduce that \(p \mid B\). Hence \(x^3 + Ax + B\) is \(p\)-Eisenstein and so irreducible over \(\mathbb{Q}\).
Next we show that
\[ \text{Gal} \left( p(x) \right) \simeq \mathbb{Z}/3\mathbb{Z}, \quad v \in V. \]

This is clear as \( p(x) \) is irreducible over \( \mathbb{Q} \) and \( \text{disc}(p(x)) \in \mathbb{Z}^2 \) by (3.6).

Our next goal is to show that if \( v \in V \) and \( K = \mathbb{Q}(\theta) \), where \( \theta \) is a root of \( p(x) \), then
\[
d(K) = \begin{cases} 
3^4 F(v)^2, & \text{if } 3 \nmid I \text{ or } 3 \parallel I, \\
F(v)^2, & \text{if } 3^2 \parallel I.
\end{cases}
\]

To do this we appeal to the following result, see [4, p. 831] and [2, Theorem, p. 4].

**Proposition 3.1.** If \( K \) is a cyclic cubic field given by \( K = \mathbb{Q}(\phi) \), where \( \phi^3 + A\phi + B = 0 \) and \( A \) and \( B \) are integers satisfying (2.1), then the discriminant of \( K \) is given by
\[
d(K) = f(K)^2,
\]
where
\[
f(K) = 3^\alpha \prod_{\substack{p \equiv 1 \pmod{3} \\text{or} \quad p \mid A, \; p \mid B}} p
\]
where \( p \) runs through primes and
\[
\alpha = \begin{cases} 
0, & \text{if } 3 \nmid A \text{ or } 3 \parallel A, \; 3 \nmid B, \; 3^3 \mid C, \\
2, & \text{if } 3^2 \parallel A, \; 3^2 \parallel B \text{ or } 3 \parallel A, \; 3 \nmid B, \; 3^2 \parallel C,
\end{cases}
\]
where \( C \in \mathbb{N} \) is given by \( C^2 = -4A^3 - 27B^2 \).

We have
\[
\begin{cases} 
3 \parallel A, & 3 \nmid B, \; 3^2 \parallel C, \; \text{if } 3 \nmid I, \\
3^2 \parallel A, & 3^2 \parallel B, \; \text{if } 3 \parallel I, \\
3 \parallel A, & 3 \nmid B, \; 3^3 \mid C, \; \text{if } 3^2 \parallel I,
\end{cases}
\]
so that
\[
\alpha = \begin{cases} 
0, & \text{if } 3^2 \parallel I, \\
2, & \text{if } 3 \nmid I \text{ or } 3 \parallel I.
\end{cases}
\]
In all three cases \(3 \nmid I, 3 \parallel I\) and \(3^2 \parallel I\) we have

\[
\prod_{p \equiv 1 \pmod{3}, p \mid A, p \mid B} p = F(v).
\]

Hence

\[
d(K) = \begin{cases} 
3^4 F(v)^2, & \text{if } 3 \nmid I \text{ or } 3 \parallel I, \\
F(v)^2 & \text{if } 3^2 \parallel I.
\end{cases}
\]

Finally in all three cases we have

\[
\text{ind}(\theta) = \sqrt{\frac{\text{disc}(p(x))}{d(K)}} = I.
\]

As \(F(v) = F(v')\) has at most two solutions for \(v'\), we can find an infinite subset of \(V\) for which the values of \(F(v)\) are distinct thus ensuring that the corresponding field discriminants are distinct. This gives an infinite set of cyclic cubic fields \(K\) possessing an integer of index \(I\). As \(B\) is odd, by Lemma 2.1 each \(K \in C_1\).

We now turn to the determination of \(L_2\). If \(K \in C_2\) the index of any \(\theta \in O_K\) such that \(K = \mathbb{Q}(\theta)\) is even. Thus we may suppose that \(I\) is even. As \(\text{ind}(3^b \theta) = 3^{3b} \text{ind}(\theta)\) for \(\mathbb{Q}(\theta) \in C_2\) we can further restrict \(I\) to satisfy \(3^3 \nmid I\). Define \(F(x) \in \mathbb{Z}[x]\) by

\[
F(x) = \begin{cases} 
x^2 + (3I^2/4), & \text{if } 3 \nmid I, \\
3x^2 + (I/6)^2 & \text{if } 3 \parallel I, \\
x^2 + 27(I/2)^2 & \text{if } 3^2 \parallel I.
\end{cases}
\]

By Lemma 2.4(c) there exist infinitely many positive integers \(v \equiv 0 \pmod{3}\) such that \(F(v)\) is squarefree. We denote the set of such \(v\) by \(V\). Moreover \(F(v) \equiv 1 \pmod{3}\) for \(v \in V\). We show next that \(\gcd(v, F(v)) = 1\). Suppose there exists a prime \(p\) with \(p \mid v\) and \(p \mid F(v)\). As \(3 \nmid v\) we have \(p \neq 3\). Suppose \(p = 2\). As \(F(v)\) is squarefree we have \(2 \parallel F(v)\). By (3.8) \(F(v) = a^2 + 3b^2\) for some integers \(a\) and \(b\). Hence \(2 \parallel a^2 + 3b^2\), contradicting \(a^2 + 3b^2 \equiv 0, 1\) or \(3\) (mod 4). Hence \(p \neq 2\). Then, from (3.8), we see that as \(p \mid F(v)\) and \(p \mid v\) we have \(p \mid I\) so \(p^2 \mid F(v)\), a contradiction.

As \(2 \nmid F(v), 3 \nmid F(v)\) and \(F(v)\) is squarefree, we see that the only primes \(p\) dividing \(F(v)\) satisfy \(p \equiv 1 \pmod{3}\).
For \( v \in V \) we define a cubic polynomial \( p(x) \in \mathbb{Z}[x] \) by
\[
(3.9) \quad p(x) = \begin{cases} 
    x^3 - 3F(v)x + 2vF(v), & \text{if } 3 \nmid I, \\
    x^3 - 9F(v)x + 18vF(v), & \text{if } 3 \parallel I, \\
    x^3 + vx^2 - 9(I/2)x - v(I/2)^2, & \text{if } 3^2 \parallel I.
\end{cases}
\]

Let \( \theta \) be a root of \( p(x) \) and set \( K = \mathbb{Q}(\theta) \). We have
\[
(3.10) \quad \text{disc}(p(x)) = \begin{cases} 
    3^4I^2F(v)^2, & \text{if } 3 \nmid I \text{ or } 3 \parallel I, \\
    I^2F(v)^2, & \text{if } 3 \parallel I.
\end{cases}
\]

We observe that
\[
q(x) = 3^3p \left( \frac{x - v}{3} \right) = x^3 - 3F(v)x + 2vF(v), \text{ if } 3^2 \parallel I.
\]

We set
\[
A = \begin{cases} 
    -3F(v), & \text{if } 3 \nmid I, \\
    -9F(v), & \text{if } 3 \parallel I, \\
    -3F(v), & \text{if } 3^2 \parallel I,
\end{cases}
\]
and
\[
B = \begin{cases} 
    2vF(v), & \text{if } 3 \nmid I, \\
    18F(v), & \text{if } 3 \parallel I, \\
    2vF(v), & \text{if } 3^2 \parallel I,
\end{cases}
\]
so that
\[
x^3 + Ax + B = \begin{cases} 
    p(x), & \text{if } 3 \nmid I \text{ or } 3 \parallel I, \\
    q(x), & \text{if } 3^2 \parallel I,
\end{cases}
\]
and
\[-4A^3 - 27B^2 = C^2,\]
where
\[
C = \begin{cases} 
    3^2IF(v), & \text{if } 3 \nmid I \text{ or } 3 \parallel I, \\
    3^3IF(v), & \text{if } 3^2 \parallel I.
\end{cases}
\]

Clearly, as \( 3 \nmid v, 3 \nmid F(v) \) and \( F(v) \) is squarefree, the polynomial \( x^3 + Ax + B \) satisfies the simplifying assumption (2.1). We show next that the polynomial
$x^3 + Ax + B$ is irreducible over $\mathbb{Q}$. For $v \in V$ we have $F(v) > 1$. Let $p$ be a prime divisor of $F(v)$. As $2 \nmid F(v)$ and $3 \nmid F(v)$ we have $p \neq 2, 3$. As $\gcd(v, F(v)) = 1$ we see that $p \parallel A$ and $p \parallel B$. Hence $x^3 + Ax + B$ is $p$–Eisenstein and so is irreducible over $\mathbb{Q}$. Thus $p(x)$ is irreducible over $\mathbb{Q}$.

As $p(x)$ is irreducible over $\mathbb{Q}$ and $\text{disc}(p(x)) \in \mathbb{Z}^2$, we have

$$\text{Gal}(K) \simeq \mathbb{Z}/3\mathbb{Z}, \quad v \in V.$$  

We have

$$\begin{cases} 3 \parallel A, & 3 \nmid B, & 3^2 \parallel C, & \text{if } 3 \nmid I, \\ 3^2 \parallel A, & 3^2 \parallel B, & 3^3 \parallel C, & \text{if } 3 \parallel I, \\ 3 \parallel A, & 3 \nmid B, & 3^5 \mid C, & \text{if } 3^2 \parallel I, \end{cases}$$

so that

$$\alpha = \begin{cases} 0, & \text{if } 3^2 \parallel I, \\ 2, & \text{if } 3 \nmid I \text{ or } 3 \parallel I. \end{cases}$$

In all three cases ($3 \nmid I$, $3 \parallel I$ and $3^2 \parallel I$) we have

$$\prod_{p \equiv 1 \pmod{3} \atop p \mid A, p \mid B} p = F(v).$$

Hence

$$d(K) = \begin{cases} 3^4 F(v)^2, & \text{if } 3 \nmid I \text{ or } 3 \parallel I, \\ F(v)^2, & \text{if } 3^2 \parallel I. \end{cases}$$

Finally, in all three cases ($3 \nmid I$, $3 \parallel I$ and $3^2 \parallel I$), we have

$$\text{ind}(\theta) = \sqrt{\frac{\text{disc}(p(x))}{d(K)}} = I.$$ 

As before there exists an infinite set of cyclic cubic fields $K$ possessing an integer of index $I$. As $B$ is even, by Lemma 2.1 each of these $K \in C_2$.

**References**


Received: January 9, 2008