Monatsh. Math. 134, 331–336 (2002)

Monatshefte für
Mathematik

Cubic Fields with Index 2

By

Blair K. Spearman[1] and **Kenneth S. Williams**[2]

[1] Okanagan University College, Kelowna, B.C., Canada
[2] Carleton University, Ottawa, Ontario, Canada

(Received 23 May 2001)

Abstract. Let d be a squarefree integer with $d = 1$ allowed. If $d \not\equiv 1 \pmod 8$ it is shown that there do not exist any cubic fields with index 2 whose splitting field contains $\mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \pmod 8$ it is shown that there exist infinitely many cubic fields with index 2 and minimal index 2 whose splitting field contains $\mathbb{Q}(\sqrt{d})$.

2000 Mathematics Subject Classification: 11R16
Key words: Cubic fields, power basis, index, minimal index, common index divisor, discriminant

1. Introduction

Let K be an algebraic number field of degree n over $\mathbb{Q}$. We denote the ring of integers of K by O_K. An element $\alpha \in O_K$ is called a generator of K if $K = \mathbb{Q}(\alpha)$. If $\alpha \in K$ we denote the minimal polynomial of α over $\mathbb{Q}$ by f_α and set $d(\alpha) = \operatorname{disc}(f_\alpha)$.

The field K is said to possess a power basis if it has an integral basis of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for some $\alpha \in O_K$. Not all algebraic number fields K have a power basis. Dedekind [1] gave the first example of a field K without a power basis, namely $K = \mathbb{Q}(\theta)$, where $\theta^3 - \theta^2 - 2\theta - 8 = 0$. A necessary and sufficient condition for K to have a power basis is the existence of a generator α of K with $d(\alpha) = d(K)$. In Dedekind's example $d(K) = -503$ and $d(\alpha) \equiv 0 \pmod 4$ for every generator α of K.

For a generator α of K, the index of α, written $i(\alpha)$, is the positive integer given by

$$d(\alpha) = d(K)i(\alpha)^2. \tag{1}$$

Clearly if $i(\alpha) \neq 1$ for all generators α of K then K does not have a power basis. We also define the minimal index of K by

$$m(K) = \min\{i(\alpha) | \alpha \text{ a generator of } K\} \tag{2}$$

Both authors were supported by research grants from the Natural Sciences and Engineering Research Council of Canada.

and the index of K by

$$i(K) = \gcd\{i(\alpha) | \alpha \text{ a generator of } K\}. \tag{3}$$

Any divisor of $i(K)$ is called a common index divisor of K. In Dedekind's example $m(K) = i(K) = 2$. Clearly if $m(K) \geqslant 2$ then K does not have a power basis. It is known that for a cubic field $i(K) = 1$ or 2 [3, p. 234], [5, p. 585].

Dummit and Kisilevsky [2] have shown that there exist infinitely many cyclic cubic fields which have a power basis and Gras [4] has shown that there are infinitely many which do not. Spearman and Williams [7] have shown that there exist infinitely many cubic fields K with a power basis such that the splitting field M of K contains a given quadratic field. In this paper we prove the following theorem.

Theorem. *Let d be a squarefree integer (with $d = 1$ allowed).*

(a) *If $d \not\equiv 1 \pmod 8$ then there do not exist any cubic fields K with $i(K) = 2$ whose splitting field contains $\mathbb{Q}(\sqrt{d})$.*

(b) *If $d \equiv 1 \pmod 8$ then there exist infinitely many cubic fields K with $i(K) = m(K) = 2$ whose splitting field contains $\mathbb{Q}(\sqrt{d})$.*

2. Proof of the Theorem

Throughout this section p denotes a prime. For m a nonzero integer we let $v_p(m)$ denote the largest nonnegative integer k such that $p^k | m$, and we write $p^{v_p(m)} \| m$.

Let $x^3 - ax + b \in \mathbb{Z}[x]$. The cubic polynomial $x^3 - ax + b$ is said to satisfy the simplifying assumption if the following condition holds:

$$\text{there does not exist a prime } p \text{ with } p^2 | a,\ p^3 | b. \tag{4}$$

The discriminant Δ of $x^3 - ax + b$ is given by

$$\Delta = 4a^3 - 27b^2. \tag{5}$$

If $\Delta \neq 0$ we let

$$s_p = v_p(\Delta), \quad \Delta_p = \Delta / p^{s_p}. \tag{6}$$

If $x^3 - ax + b$ satisfies the simplifying assumption (4) and is irreducible (so that $\Delta \neq 0$) with root θ then $K = \mathbb{Q}(\theta)$ is a cubic field and Llorente and Nart [5, Theorem 2] have given the exact power of p in the discriminant D of K.

Theorem 1 (Llorente and Nart). *For $p = 2$,*

$$\begin{aligned} v_2(D) = 3 &\Leftrightarrow\ s_2 \text{ odd}, \\ v_2(D) = 2 &\Leftrightarrow \begin{cases} 1 \leqslant v_2(b) \leqslant v_2(a), \text{ or} \\ s_2 \text{ even and } \Delta_2 \equiv 3 \pmod 4, \end{cases} \\ v_2(D) = 0 &\quad \text{otherwise}. \end{aligned}$$

For $p = 3$,

$$\begin{aligned} v_3(D) = 5 &\Leftrightarrow\ 1 \leqslant v_3(b) < v_3(a), \\ v_3(D) = 4 &\Leftrightarrow \begin{cases} v_3(a) = v_3(b) = 2, \text{ or} \\ a \equiv 3 \pmod 9, 3 \nmid b \text{ and } b^2 \not\equiv 4 \pmod 9, \end{cases} \end{aligned}$$

$$v_3(D) = 3 \Leftrightarrow \begin{cases} v_3(a) = v_3(b) = 1, \text{ or} \\ 3 \mid a, 3 \nmid b, a \not\equiv 3 \pmod 9 \text{ and } b^2 \not\equiv a+1 \pmod 9, \text{ or} \\ a \equiv 3 \pmod 9, b^2 \equiv 4 \pmod 9 \text{ and } b^2 \not\equiv a+1 \pmod{27}, \end{cases}$$

$$v_3(D) = 1 \Leftrightarrow \begin{cases} 1 = v_3(a) < v_3(b), \text{ or} \\ 3 \mid a,\ a \not\equiv 3 \pmod 9 \text{ and } b^2 \equiv a+1 \pmod 9, \text{ or} \\ a \equiv 3 \pmod 9,\ b^2 \equiv a+1 \pmod{27} \text{ and } s_3 \text{ odd}, \end{cases}$$

$$v_3(D) = 0 \Leftrightarrow \begin{cases} 3 \nmid a, \text{ or} \\ a \equiv 3 \pmod 9,\ b^2 \equiv a+1 \pmod{27} \text{ and } s_3 \text{ even}. \end{cases}$$

For $p > 3$,

$$\begin{aligned} v_p(D) = 2 &\Leftrightarrow\ 1 \leqslant v_p(b) \leqslant v_p(a), \\ v_p(D) = 1 &\Leftrightarrow\ s_p \text{ odd}, \\ v_p(D) = 0 &\qquad \text{otherwise}. \end{aligned}$$

Llorente and Nart [5, Theorem 4] have also given a necessary and sufficient condition for the index of K to be 2.

Theorem 2 (Llorente and Nart).

$$i(K) = 2 \Leftrightarrow a \text{ odd},\ b \text{ even},\ s_2 \text{ even and } \Delta_2 \equiv 1 \pmod 8.$$

Proof of Theorem. (a) Suppose that there exists a cubic field K with $i(K) = 2$ whose splitting field contains $\mathbb{Q}(\sqrt{d})$. Then $K = \mathbb{Q}(\theta)$ for some generator θ, which is a root of an irreducible cubic polynomial of the form $x^3 - ax + b \in \mathbb{Z}[x]$ satisfying the simplifying assumption (4). As the splitting field of K contains $\mathbb{Q}(\sqrt{d})$ we have $\Delta = df^2$ for some integer f. Set $f = 2^t g$, where g is odd. By Theorem 2, s_2 is even and so d (being squarefree) is odd. Thus $s_2 = 2t$ and $\Delta_2 = dg^2$. Further, by Theorem 2, we have $\Delta_2 \equiv 1 \pmod 8$ so that $d \equiv 1 \pmod 8$.

(b) Suppose that d is squarefree and

$$d \equiv 1 \pmod 8. \tag{7}$$

In (8), (9), (11) and (12) below we construct a parametric family of cubics $x^3 - ax + b$ in each of the five cases:

$$\begin{aligned} &\text{Case 1} : d \not\equiv 0 \pmod 3. \\ &\text{Case 2} : d \equiv 3 \pmod 9, \quad d \not\equiv 12 \pmod{27}. \\ &\text{Case 3} : d \equiv 12 \pmod{27}. \\ &\text{Case 4} : d \equiv 6 \pmod 9, \quad d \not\equiv 15 \pmod{27}. \\ &\text{Case 5} : d \equiv 15 \pmod{27}. \end{aligned}$$

The parametric families were constructed by starting with the parametric solution

$$a = 12m^2 + 9dn^2, \quad b = 16m^3 + 12dmn^2, \quad c = 72m^2n + 54dn^3,$$

of

$$4a^3 - 27b^2 = dc^2$$

and then imposing congruence restrictions on the parameters m and n so that a, b and $4a^3 - 27b^2$ contain powers of primes suitable for our purposes. We define for any positive integer k

$$p(k) = \begin{cases} 36d^2k^2 + 24dk + (3d+4), & \text{case 1,} \\ 324d^2k^2 + 72dk + ((d/3)+4), & \text{case 2,} \\ 576d^2k^2 + 384dk + ((d/3)+64), & \text{case 3,} \\ 36d^2k^2 + 24dk + ((d/3)+4), & \text{case 4,} \\ 144d^2k^2 + 96dk + ((d/3)+16), & \text{case 5,} \end{cases} \tag{8}$$

and

$$q(k) = \begin{cases} 3dk+1, & \text{case 1,} \\ 9dk+1, & \text{case 2,} \\ 12dk+4, & \text{case 3,} \\ 3dk+1, & \text{case 4,} \\ 6dk+2, & \text{case 5.} \end{cases} \tag{9}$$

Clearly $p(k) \in \mathbb{Z}^+$ and $q(k) \in \mathbb{Z}^+$. Moreover

$$\begin{aligned} &\gcd(p(k),\ 6dq(k)) = 1, && \text{cases 1, 2, 3,} \\ &\gcd(p(k)/3,\ 6dq(k)) = 1, && \text{cases 4, 5.} \end{aligned} \tag{10}$$

It is easily checked that the quadratic polynomials $p(k)$ in cases 1, 2 and 3, and $p(k)/3$ in cases 4 and 5, are primitive, have nonzero discriminants and no fixed divisors. Hence, by Nagel's theorem [6] (see also [7]), there are infinitely many positive integers k such that $p(k)$ in cases 1, 2 and 3, and $p(k)/3$ in cases 4 and 5, is squarefree. In each case we denote the set of such k by S. For $k \in S$ clearly $p(k) > 4$.

For $k \in S$ we define

$$f_k(x) = x^3 - ax + b, \tag{11}$$

where

$$a = a(k) = 3p(k), \quad b = b(k) = 4p(k)q(k). \tag{12}$$

By (10), (11) and (12), $f_k(x)$ $(k \in S)$ is p–Eisenstein for any prime $p|p(k)$. Thus $f_k(x)$ is irreducible. Let $\theta = \theta_k$ be a root of $f_k(x)$ and set $K = \mathbb{Q}(\theta)$ so that $[K : \mathbb{Q}] = 3$. Clearly there are no primes p such that $p^2|a$ and $p^3|b$ so that the simplifying assumption (4) holds.

Next

$$\Delta = \Delta(k) = 4a^3 - 27b^2 = \begin{cases} 2^2 3^4 d\ p(k)^2, & \text{case 1,} \\ 2^2 3^2 d\ p(k)^2, & \text{cases 2, 3, 4, 5,} \end{cases} \tag{13}$$

so that

$$s_2 = 2, \quad \Delta_2 \equiv 1 \pmod 8. \tag{14}$$

Clearly from (10) and (12) we have

$$a \equiv 1 \pmod 2, \quad b \equiv 0 \pmod 2. \tag{15}$$

Hence, by Theorem 2, (14) and (15), we have $i(K) = 2$.

Next we show that $m(K) = 2$. As $i(K) = 2$ we have $m(K) \geqslant 2$. We show that $i(\theta) = 2$ proving $m(K) = 2$. As $i(K) = 2$ we have $2|i(\theta)$. Since $2^2 \| \Delta$ and $\Delta = d(K)i(\theta)^2$, we deduce that $d(K) \equiv 1 \pmod 2$ and $2 \| i(\theta)$. It remains to show that $p \nmid i(\theta)$ for every prime $p \neq 2$.

From (7), (8), (9) and (12), we deduce that

$a \equiv 3 \pmod 9,\ b \not\equiv 0 \pmod 3,\ b \equiv 3d - 2 \pmod 9,$
$b^2 \equiv 6d + 4 \not\equiv 4 \pmod 9,$ case 1,

$a \equiv 0 \pmod 3,\ a \equiv 6 \pmod 9,\ b \not\equiv 0 \pmod 3,\ b \equiv 4e - 2 \pmod 9,$
$b^2 \equiv -2e + 6 \pmod 9,\ b^2 - a - 1 \equiv -2e - 1 \not\equiv 0 \pmod 9,$ as $e = d/3 \equiv 1 \pmod 3$,
$e \not\equiv 4 \pmod 9,$ case 2,

$a \equiv 0 \pmod 3,\ a \equiv 6 \pmod 9,\ b \not\equiv 0 \pmod 3,\ b \equiv -1 \pmod 9,$
$b^2 \equiv 1 \pmod 9,\ b^2 - a - 1 \equiv 3 \not\equiv 0 \pmod 9,$ case 3,

$3^2 \| a, 3 \| b.$ cases 4, 5.

By Theorem 1 we have

$$\begin{aligned} 3^4 &\parallel d(K), \quad \text{case 1,} \\ 3^3 &\parallel d(K), \quad \text{cases 2, 3,} \\ 3^5 &\parallel d(K), \quad \text{cases 4, 5.} \end{aligned}$$

By (10) and (13) we have

$$\begin{aligned} 3^4 &\parallel \Delta, \quad \text{case 1,} \\ 3^3 &\parallel \Delta, \quad \text{cases 2, 3,} \\ 3^5 &\parallel \Delta, \quad \text{cases 4, 5.} \end{aligned}$$

Hence

$$3 \nmid i(\theta).$$

Now let p be a prime with $p \neq 2, 3$. If $p \nmid \Delta$ then $p \nmid i(\theta)$. If $p|\Delta$ then by (10) and (13) $p|d$ or $p|p(k)$ but not both by (10). If $p|d$ then by (10) and (13) we have $p \| \Delta$, and by Theorem 1 we have $p \| d(K)$, so $p \nmid i(\theta)$. If $p|p(k)$ then by (10) and (13) we have $p^2 \| \Delta$, and by (10) and (12) $p \| a$, $p \| b$, so by Theorem 1 we have $p^2 \| d(K)$, and so $p \nmid i(\theta)$. This completes the proof that $i(\theta) = 2$ and $m(K) = 2$.

Finally for $k_1, k_2 \in S$ we have $p(k_1) \neq p(k_2)$ for $k_1 \neq k_2$ and a fixed polynomial $p(k)$. As $p(k_1) > 0$, $p(k_2) > 0$, we have $p(k_1)^2 \neq p(k_2)^2$. Thus, by (13), $\Delta(k_1) \neq \Delta(k_2)$ and so

$$d(\mathbb{Q}(\theta_{k_1})) = \frac{\Delta(k_1)}{4} \neq \frac{\Delta(k_2)}{4} = d(\mathbb{Q}(\theta_{k_2})).$$

This shows that the fields $\mathbb{Q}(\theta_k)$ $(k \in S)$ are all distinct. As $\Delta(k)/d$ is a perfect square for each $k \in S$, the splitting field of $\mathbb{Q}(\theta_k)$ $(k \in S)$ contains $\mathbb{Q}(\sqrt{d})$.

We close by remarking that an integral basis for $\mathbb{Q}(\theta_k)$ $(k \in S)$ is

$$\left\{1, \theta_k, \frac{\theta_k^2 + \theta_k}{2}\right\}.$$

References

[1] Dedekind R (1930) Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Abh Kgl Ges Wiss Göttingen **23**: 1–23 (Gesammelte Mathematische Werke I, pp 202–232, Vieweg)
[2] Dummit D, Kisilevsky H (1977) Indices in cyclic cubic fields. In Zassenhaus H (ed) Number Theory and Algebra, Collected papers dedicated to Henry B. Mann, Arnold E. Ross and Olga Taussky-Todd, pp 29–42, New York: Academic Press
[3] Engstrom HT (1930) On the common index divisors of an algebraic field. Trans Amer Math Soc **32**: 223–237
[4] Gras MN (1973) Sur les corps cubiques cycliques dont l'anneau des entiers est monogène. Ann Sci Univ Besancon (3) Fasc **6**: 26 pp
[5] Llorente P, Nart E (1983) Effective determination of the rational primes in a cubic field. Proc Amer Math Soc **87**: 579–585
[6] Nagel T (1922) Zur Arithmetik der Polynome. Abh Math Sem Hamburg **1**: 179–194
[7] Spearman BK, Williams KS, Cubic fields with a power basis. Rocky Mountain J Math (in press)

Authors' addresses: B. K. Spearman, Department of Mathematics and Statistics, Okanagan University College, Kelowna, B.C., Canada V1V 1V7, e-mail: bkspearm@okuc02.okanagan.bc.ca; K. S. Williams, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6, e-mail: williams@math.carleton.ca