ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 31, Number 3, Fall 2001

CUBIC FIELDS WITH A POWER BASIS

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT. It is shown that there exist infinitely many cubic fields L with a power basis such that the splitting field M of L contains a given quadratic field K.

1. Introduction. We prove the following result, which answers a question posed to the authors by James G. Huard.

Theorem. *Let K be a fixed quadratic field. Then there exist infinitely many cubic fields L with a power basis such that the splitting field M of L contains K.*

We remark that Dummit and Kisilevsky [**2**] have shown that there exist infinitely many cyclic cubic fields with a power basis.

2. Squarefree values of quadratic polynomials. The following result is due to Nagel [**5**]. We quote it in the form given by Huard [**3**].

Proposition 2.1. *Let $f(x)$ be a polynomial with integer coefficients such that*

(i) *the degree of $f(x) = k$,*

(ii) *the discriminant of $f(x)$ is not equal to zero,*

(iii) *$f(x)$ is primitive,*

(iv) *$f(x)$ has no fixed divisors which are kth powers of primes.*

Then infinitely many of $f(1), f(2), f(3), \dots$ are kth power free.

We recall that a positive integer $d > 1$ is called a fixed divisor of the primitive polynomial $f(x) \in \mathbf{Z}[x]$ if $f(k) \equiv 0 \pmod{d}$ for all

1991 AMS *Mathematics Subject Classification.* Primary 11R16.
Key words and phrases. Cubic fields, power bases.
Received by the editors on March 3, 2000, and in revised form on June 21, 2000.

Copyright ©2001 Rocky Mountain Mathematics Consortium

$k \in \mathbf{Z}$. Thus, for example, 2 is a fixed divisor of $x^2 + x$. Since the only possible fixed divisor of a primitive quadratic polynomial with integer coefficients is 2, the case $k = 2$ of Proposition 2.1 gives

Proposition 2.2. *Let a, b, c be integers such that*

$$a \neq 0, \; b^2 - 4ac \neq 0, \; \gcd(a, b, c) = 1.$$

Then

$$\{k \in \mathbf{Z}^+ : ak^2 + bk + c \text{ is squarefree}\}$$

is an infinite set.

If $a > 0$, then $ak^2 + bk + c \leq 1$ holds for only finitely many integers k so that Proposition 2.2 gives

Proposition 2.3. *Let a, b, c be integers such that*

$$a > 0, \; b^2 - 4ac \neq 0, \; \gcd(a, b, c) = 1.$$

Then

$$\{k \in \mathbf{Z}^+ : ak^2 + bk + c \text{ is squarefree and } > 1\}$$

is an infinite set.

3. The discriminant of a cubic field. Throughout this paper p denotes a prime. If m is a nonzero integer such that $p^k \mid m$, $p^{k+1} \nmid m$, we write $p^k \| m$ and set $v_p(m) = k$. The following result is due to Llorente and Nart [**4**], see also Alaca [**1**].

Proposition 3.1. *Let a and b be integers such that the cubic polynomial $x^3 - ax + b$ is irreducible 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 $K = \mathbf{Q}(\theta)$ so that $[K : \mathbf{Q}] = 3$. Let $s_p = v_p(4a^3 - 27b^2)$ and $\Delta_p = (4a^3 - 27b^2)/p^{s_p}$. Then the discriminant $d(K)$ of the cubic field K is given by*

$$d(K) = \operatorname{sgn}(4a^3 - 27b^2) 2^\alpha 3^\beta \prod_{\substack{p>3 \\ s_p \equiv 1 \pmod 2}} p \prod_{\substack{p>3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2,$$

where

$$\alpha = \begin{cases} 3, & \textit{if } s_2 \equiv 1 \pmod 2, \\ 2, & \textit{if } 1 \le v_2(b) \le v_2(a), \textit{ or} \\ & s_2 \equiv 0 \pmod 2 \textit{ and } \Delta_2 \equiv 3 \pmod 4, \\ 0, & \textit{otherwise,} \end{cases}$$

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

4. Proof of theorem. Let K be a quadratic field so that $K = \mathbf{Q}(\sqrt{d})$ for a unique squarefree integer $d \neq 1$. (We remark that our proof is also valid when $d = 1$ giving another proof that there are infinitely many cyclic cubic fields with a power basis, see Dummit and Kisilevsky [**2**].) We now describe briefly how our theorem is proved. We construct infinitely many cubic polynomials $\{f_k(x) : k \in S\}$ in such a way that the corresponding cubic fields $\{L_k = \mathbf{Q}(\theta_k) : k \in S\}$, where θ_k is a root of $f_k(x)$, are all distinct and satisfy $d(L_k) = \operatorname{disc}(f_k(x))$ and $d(L_k)/d =$ square. Thus $\{L_k : k \in S\}$ is an infinite set of cubic fields containing $Q(\sqrt{d})$, each of which has a power basis.

We consider the following ten cases:

$$\begin{array}{rll}
\text{Case } 1: & d \equiv 2 \pmod 4, & d \not\equiv 0 \pmod 3. \\
\text{Case } 2: & d \equiv 2 \pmod 4, & d \equiv 0 \pmod 3. \\
\text{Case } 3: & d \equiv 3 \pmod 4, & d \not\equiv 0 \pmod 3. \\
\text{Case } 4: & d \equiv 3 \pmod 4, & d \equiv 0 \pmod 3. \\
\text{Case } 5: & d \equiv 1 \pmod 8, & d \not\equiv 0 \pmod 3. \\
\text{Case } 6: & d \equiv 1 \pmod 8, & d \equiv 0 \pmod 3. \\
\text{Case } 7: & d \equiv 5 \pmod{16}, & d \not\equiv 0 \pmod 3. \\
\text{Case } 8: & d \equiv 5 \pmod{16}, & d \equiv 0 \pmod 3. \\
\text{Case } 9: & d \equiv 13 \pmod{16}, & d \not\equiv 0 \pmod 3. \\
\text{Case } 10: & d \equiv 13 \pmod{16}, & d \equiv 0 \pmod 3.
\end{array}$$

In cases 7 and 8 we let q be a prime such that

$$q \equiv 11 \pmod{16}, \quad q \nmid d.$$

We define

$$p(k) = \begin{cases}
36d^2k^2 + 12dk + (3d+1), & \text{case } 1, \\
81d^2k^2 + 54dk + (9 + (d/3)), & \text{case } 2, \\
36d^2k^2 + 24dk + (4+3d), & \text{case } 3, \\
324d^2k^2 + 216dk + (36 + (d/3)), & \text{case } 4, \\
36d^2k^2 + 6dk + ((1+3d)/4), & \text{case } 5, \\
324d^2k^2 + 54dk + ((27+d)/12), & \text{case } 6, \\
648d^2k^2 + 18qdk + ((q^2+3d)/8), & \text{case } 7, \\
72d^2k^2 + 18qdk + ((27q^2+d)/24), & \text{case } 8, \\
72d^2k^2 + 6dk + ((1+3d)/8), & \text{case } 9, \\
648d^2k^2 + 54dk + ((27+d)/24). & \text{case } 10.
\end{cases}$$

It is easily checked that in all cases the coefficients of $p(k)$ are integers so that $p(k) \in \mathbf{Z}$ for all $k \in \mathbf{Z}$. Moreover,

$$\gcd(p(k), 6d) = 1 \quad \text{for all } k \in \mathbf{Z}.$$

Further, the conditions stated in Proposition 2.3 are satisfied by the coefficients of $p(k)$ in every case. Thus, by Proposition 2.3, the set

$$S = \{k \in \mathbf{Z}^+ : p(k) \text{ is squarefree and } > 1\}$$

is infinite. Moreover, no two distinct values of k in S can give the same value to $p(k)$.

For $k \in S$, we set

$$f_k(x) = x^3 - ax + b,$$

where

$$(a,b) = (a(k), b(k)) = \begin{cases} (3p(k), 2(6dk+1)p(k)), & \text{case 1,} \\ (3p(k), 2(9dk+3)p(k)), & \text{case 2,} \\ (3p(k), 2(6dk+2)p(k)), & \text{case 3,} \\ (3p(k), 2(18dk+6)p(k)), & \text{case 4,} \\ (3p(k), (12dk+1)p(k)), & \text{case 5,} \\ (3p(k), (36dk+3)p(k)), & \text{case 6,} \\ (6p(k), 2(72dk+q)p(k)), & \text{case 7,} \\ (6p(k), 6(8dk+q)p(k)), & \text{case 8,} \\ (6p(k), 2(24dk+1)p(k)), & \text{case 9,} \\ (6p(k), 2(72dk+3)p(k)), & \text{case 10.} \end{cases}$$

It is easy to check that $\gcd(b(k)/p(k), p(k)) = 1$ in all cases so that $f_k(x)$ is p-Eisenstein for every prime $p \mid p(k)$. Thus $f_k(x)$ is irreducible. Let θ_k be a root of $f_k(x)$, and set $L_k = \mathbf{Q}(\theta_k)$ so that $[L_k : \mathbf{Q}] = 3$. Clearly there does not exist a prime p such that $v_p(a) \geq 2$ so that we can apply Proposition 3.1 to determine the discriminant $d(L_k)$ of the cubic field L_k. We note that

$$\operatorname{disc}(f_k(x)) = 4a^3 - 27b^2 = \begin{cases} 2^2 \cdot 3^4 p(k)^2 d, & \text{case 1,} \\ 2^2 \cdot 3^2 p(k)^2 d, & \text{case 2,} \\ 2^2 \cdot 3^4 p(k)^2 d, & \text{case 3,} \\ 2^2 \cdot 3^2 p(k)^2 d, & \text{case 4,} \\ 3^4 p(k)^2 d, & \text{case 5,} \\ 3^2 p(k)^2 d, & \text{case 6,} \\ 2^2 \cdot 3^4 p(k)^2 d, & \text{case 7,} \\ 2^2 \cdot 3^2 p(k)^2 d, & \text{case 8,} \\ 2^2 \cdot 3^4 p(k)^2 d, & \text{case 9,} \\ 2^2 \cdot 3^2 p(k)^2 d, & \text{case 10.} \end{cases}$$

We have

$$\begin{array}{ll} s_2 = 3, & \text{cases } 1,\ 2, \\ a \equiv 3 \pmod 4,\ b \equiv 0 \pmod 4, & \text{cases } 3,\ 4, \\ b \equiv 1 \pmod 2, & \text{cases } 5,\ 6, \\ a \equiv 0 \pmod 2,\ b \equiv 2 \pmod 4, & \text{cases } 7,\ 8,\ 9,\ 10, \end{array}$$

so that, by Proposition 3.1, we have

$$v_2(d(L_k)) = \begin{cases} 3, & \text{cases } 1,\ 2, \\ 2, & \text{cases } 3,\ 4,\ 7,\ 8,\ 9,\ 10, \\ 0, & \text{cases } 5,\ 6. \end{cases}$$

Next,

$$\begin{array}{ll} a \equiv 3 \pmod 9,\ b \not\equiv 0 \pmod 3, & \\ b \equiv 2-3d \pmod 9,\ b^2 \equiv 4-3d \not\equiv 4 \pmod 9, & \text{case } 1, \\ v_3(a) = v_3(b) = 1, & \text{cases } 2,\ 4,\ 6,\ 8,\ 10, \\ a \equiv 3 \pmod 9,\ b \not\equiv 0 \pmod 3, & \\ b \equiv 3d-2 \pmod 9,\ b^2 \equiv 4-3d \not\equiv 4 \pmod 9, & \text{cases } 3,\ 5,\ 9, \\ a \equiv 3 \pmod 9,\ b \not\equiv 0 \pmod 3, & \\ b \equiv 3qd-2q^3 \pmod 9,\ b^2 \equiv 4-3d \not\equiv 4 \pmod 9, & \text{case } 7, \end{array}$$

so that, by Proposition 3.1, we have

$$v_3(d(L_k)) = \begin{cases} 4, & \text{cases } 1,\ 3,\ 5,\ 7,\ 9, \\ 3, & \text{cases } 2,\ 4,\ 6,\ 8,\ 10. \end{cases}$$

Easy calculations show that in all cases

$$\prod_{\substack{p>3 \\ 1 \le v_p(b) \le v_p(a)}} p^2 = p(k)^2,$$

and

$$\operatorname{sgn}(4a^3 - 27b^2) \prod_{\substack{p>3 \\ s_p \equiv 1 \,(\mathrm{mod} 2)}} p = \frac{d}{\gcd(d,6)}.$$

Hence, by Proposition 3.1, we deduce that

$$d(L_k) = \text{disc}\,(f_k(x)), \quad \text{for all } k \in S.$$

Thus, L_k has a power basis for each $k \in S$. For $k_1, k_2 \in S$ with $k_1 \neq k_2$ we have $p(k_1) \neq p(k_2)$ and $p(k_1) > 1$, $p(k_2) > 1$, so that $p(k_1)^2 \neq p(k_2)^2$, and thus $d(L_{k_1}) \neq d(L_{k_2})$ proving that $L_{k_1} \neq L_{k_2}$. Thus, $\{L_k : k \in S\}$ is an infinite set of distinct cubic fields, each with a power basis. Since each $d(L_k)/d$ is a square, the splitting field M_k of L_k contains $Q(\sqrt{d})$.

REFERENCES

1. S. Alaca, *p-integral bases of algebraic number fields*, Ph.D. Thesis, Carleton University, 1994.

2. D.S. Dummit and H. Kisilevsky, *Indices in cyclic cubic fields*, Number theory and algebra, collected papers dedicated to Henry B. Mann, Arnold E. Ross and Olga Taussky-Todd (Hans Zassenhaus, ed.), Academic Press, New York, 1977, pp. 29–42.

3. J.G. Huard, *Index forms and power bases for cyclic cubic fields*, Ph.D. Thesis, Pennsylvania State University, 1978.

4. P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579–585.

5. T. Nagel, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 179–194.

Department of Mathematics and Statistics, Okanagan University College, Kelowna, B.C. Canada V1V 1V7
E-mail address: bkspearm@okuc02.okanagan.bc.ca

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6
E-mail address: williams@math.carleton.ca