Arch. Math. 106 (2016), 35–40
© 2015 Springer Basel
0003-889X/16/010035-6
published online August 30, 2015
DOI 10.1007/s00013-015-0812-z

Archiv der Mathematik

Minimal indices of pure cubic fields

Blair K. Spearman, Qiduan Yang and Jeewon Yoo

Abstract. The minimal index of a pure cubic field was shown to assume arbitrarily large values by M. Hall. In this paper we extend this result by showing that every cubefree integer occurs as the minimal index of infinitely many pure cubic fields.

Mathematics Subject Classification. Primary 11R16; Secondary 11D59.

Keywords. Pure cubic field, Minimal index, Chebotarev density theorem.

1. Introduction. Let K be an algebraic number field with discriminant $d(K)$. The ring of integers of K is denoted by O_K. Let $\alpha \in O_K$ be such that $K = \mathbb{Q}(\alpha)$. The minimal polynomial of α over $\mathbb{Q}$ is denoted by $irr_{\mathbb{Q}}(\alpha)$, and the discriminant of $irr_{\mathbb{Q}}(\alpha)$ by $D(\alpha)$. Using this notation, we define the index of α, $ind(\alpha)$ by

$$ind(\alpha) = \sqrt{\frac{D(\alpha)}{d(K)}}.$$

The quantity $ind(\alpha)$ is a positive integer (see for example [12, p. 53]). We may now define the field index $i(K)$ of K by

$$i(K) = \gcd_{\alpha \in O_K} (ind(\alpha)),$$

and the minimal index $m(K)$ of K by

$$m(K) = \min_{\alpha \in O_K} (ind(\alpha)).$$

In the case of cubic fields, it is known that $i(K) = 1$ or 2, [3]. On the other hand, the minimal index of a cubic field can be arbitrarily large. This was proved for pure cubic fields by Hall [7]. Gaál and Szabó [6] studied distributions of the minimal indices of pure cubic fields with bounded discriminant. Unboundedness of the minimal index for cyclic cubic fields was established by Dummit and Kisilevsky [2]. Nakahara, [10,11] proved the minimal index is

unbounded for bicyclic and cyclic quartic fields. More recently there has been a trend towards evaluation of the minimal index for families of number fields. The minimal index was evaluated for a class of pure quartic fields by Thunder and Wolfskill [13], and for a class of bicyclic quartic fields by Jadrijević [8]. The purpose of this paper is to return to pure cubic fields and evaluate the minimal index for infinitely many of these fields, showing that any cubefree positive integer occurs infinitely often as the minimal index of a pure cubic field. We prove the following theorem.

Theorem 1.1. *Let n be a cubefree positive integer. Then there exist infinitely many pure cubic fields with minimal index equal to n.*

2. Background and proof. First we recall some relevant facts about pure cubic fields, then we give the proof of our theorem. If K is a pure cubic field, then there exist squarefree relatively prime integers a and b such that

$$K = \mathbb{Q}\left(\sqrt[3]{ab^2}\right).$$

Set $\theta = \sqrt[3]{ab^2}$. Dedekind determined an integral basis for K in the following form [1, p. 340], [2].

Case 1. If $a^2 \not\equiv b^2 (\mathrm{mod}\ 9)$, then

$$\left\{1, \theta, \frac{\theta^2}{b}\right\}$$

is an integral basis.

Case 2. If $a^2 \equiv b^2 (\mathrm{mod}\ 9)$ and we choose the signs of a and b so that $a \equiv b \equiv 1 \pmod 3$, then

$$\left\{1, \theta, \frac{\theta^2 + ab^2\theta + b^2}{3b}\right\}$$

is an integral basis.

Hall [7] used these integral bases to compute index forms $I(x, y)$ for K. The set of nonzero values of $|I(x, y)|$ as x, y range over the integers is equal to the set of indices of K. These index forms are as follows.

Case 1. If $a^2 \not\equiv b^2 (\mathrm{mod}\ 9)$, then

$$I(x, y) = ax^3 - by^3 \tag{1}$$

Case 2. If $a^2 \equiv b^2 (\mathrm{mod}\ 9)$ and we have chosen $a \equiv b \equiv 1 (\mathrm{mod}\ 3)$, then

$$I(x, y) = \frac{a(3x + y)^3 - by^3}{9} \tag{2}$$

We are now ready to prove our theorem.

Proof. Let n be a cubefree positive integer. We construct infinitely many pure cubic fields K with

$$m(K) = n.$$

Suppose that $n = 1$. If $p > 3$ is any prime, then the pure cubic field

$$K = \mathbb{Q}\left(\sqrt[3]{3p}\right)$$

has minimal index $m(K) = 1$ since the index form of K is

$$I(x, y) = 3px^3 - y^3$$

by (1) and

$$I(x, y) = 1$$

is clearly solvable. Now, assuming that $n > 1$ and cubefree, it is easily shown using unique factorization that the set of integers

$$n^2k, \quad k = 1, 2, \ldots, n-1,$$

contains no perfect cubes. Thus the cubic polynomials

$$f_k(x) = x^3 - n^2k, \quad k = 1, 2, \ldots, n-1,$$

are irreducible over $\mathbb{Q}$. The Galois groups of the cubic polynomials $f_k(x)$ contain an element of order 3 so that by the Chebotarev density theorem [9] we may select prime numbers p_k, $k = 1, 2, \ldots, n-1$ such that $f_k(x)$ is irreducible modulo p_k. Clearly $p_k = 3$ is impossible. Furthermore, each p_k has the form $3e + 1$ where e is an integer since every integer is a cube modulo primes of the form $3e + 2$. This would imply that $f_k(x)$ is reducible modulo p_k contradicting our choice of p_k. Define the positive integer b to be the product of the distinct primes in the sequence

$$p_1, p_2, \ldots, p_{n-1}.$$

Clearly we have $\gcd(n, b) = 1$, and b is squarefree. Further, we have

$$b \equiv 1 (\mathrm{mod}\, 3). \tag{3}$$

Let z be an integer. We define the integer $a = a_z$ by

$$a = b(3z + 1)^3 + 9n. \tag{4}$$

We may apply a theorem of Erdös [4] on squarefree values of cubic polynomials to conclude that there exist infinitely many integers z such that a is squarefree. More information on this theorem is available in a paper of Filaseta [5]. From now on we assume that the integers $a = a_z$ have this property. By construction $\gcd(a, b) = 1$. We now have a family of pure cubic fields

$$K = \mathbb{Q}\left(\sqrt[3]{ab^2}\right).$$

We will show that these fields have the property that $m(K) = n$. Using (4) it is easy to check that

$$a \equiv b (\mathrm{mod}\ 9),$$

from which we deduce that we are in case 2 for pure cubic fields. From (3) and (4) we see that

$$a \equiv b \equiv 1 (\mathrm{mod}\ 3)$$

so that an index form for this field, given by (2) is

$$I(x,y) = \frac{(b(3z+1)^3 + 9n)(3x+y)^3 - by^3}{9}.$$

A calculation shows that

$$I(-z, 3z+1) = n.$$

If any of the equations

$$I(x,y) = \pm k, \quad k = 1, 2, \ldots, n-1$$

are solvable for integers x, y then at least one of the congruences

$$I(x,y) \equiv \pm k \pmod{p_k}, \quad k = 1, 2, \ldots, n-1$$

is solvable. These congruences reduce to

$$n(3x+y)^3 \equiv \pm k (\text{mod } p_k),$$

implying that the congruence

$$X^3 \equiv \pm n^2 k (\text{mod } p_k)$$

is solvable for X modulo p_k for some k, which contradicts the choice of the p_k. Thus each of the infinitely many pure cubic fields K in this case satisfy

$$m(K) = n,$$

completing the proof. □

We finish with two examples and a question.

Example. We use the method in the proof of our theorem to construct a pure cubic field K with

$$m(K) = 4.$$

Begin by choosing primes p_k, $k = 1, 2, 3$ such that the cubic polynomials

$$f_k(x) = x^3 - 4^2 k, \quad k = 1, 2, 3$$

are irreducible modulo p_k. We find that we may choose $p_1 = p_2 = 7$ and $p_3 = 13$. Thus $b = 7 \cdot 13$. Next we choose the positive integer z so that

$$7 \cdot 13 \cdot (3z+1)^3 + 4 \cdot 9$$

is squarefree. We find the value $z = 0$ yields the squarefree integer 127. As in the proof of our theorem, we have

$$a = 127 \qquad \text{and} \qquad b = 91.$$

The pure cubic field

$$K = \mathbb{Q}\left(\sqrt[3]{127 \cdot 91^2}\right)$$

has index form

$$I(x,y) = \frac{127(3x+y)^3 - 91y^3}{9}.$$

The cubic Thue equations

$$I(x,y) = \pm k, \quad k = 1, 2, 3$$

are insolvable by construction, but

$$I(0,1) = 4,$$

so that

$$m(K) = 4.$$

Next we consider an example which is not covered by our theorem.

Example. We give a pure cubic field K with $m(K) = 8$. Set

$$K = \mathbb{Q}\left(\sqrt[3]{23 \cdot 15^2}\right).$$

The index form for K is

$$I(x,y) = 23x^3 - 15y^3.$$

Using Magma, we find that the Thue equations

$$I(x,y) = \pm k, \quad k = 1, 2, \ldots, 7$$

are all insolvable. However

$$I(1,1) = 8,$$

so that

$$m(K) = 8.$$

We finish by asking the following question: For a fixed positive integer n, do there exist infinitely many pure cubic fields with minimal index equal to n?

References

[1] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag (2000).

[2] D. S. Dummit and H. Kisilevsky, Indices in cyclic cubic fields, in "Number Theory and Algebra", Academic Press, 1977, 29–42.

[3] H. T. Engstrom, On the common index divisors of an algebraic field, Transactions of the American Mathematical Society, vol. **32**, pp. 223–237, 1930.

[4] P. Erdös, Arithmetic properties of polynomials, J. London Math. Soc. **28** (1953), 416–425.

[5] M. Filaseta, Squarefree values of polynomials, Acta Arith. **60** (1992), 21–231.

[6] I. Gaál and T. Szabó, A note on the minimal indices of pure cubic fields, JP Journal of Algebra, Number Theory and Applications, **19** (2010), 129–139.

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

[8] B. Jadrijević, Establishing the minimal index in a parametric family of bicyclic biquadratic fields, Periodica Mathematica Hungarica, Volume **58**, Number 2, 155–180.

[9] H. W. Lenstra, and P. Stevenhagen, Chebotarev and his density theorem, The Mathematical Intelligencer **18** (1966), 26–37.

[10] T. Nakahara, On the indices and integral bases of non-cyclic but abelian biquadratic fields, Arch. Math. (Basel) **41** (1983), 504–508.

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

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

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

Blair K. Spearman, Qiduan Yang and Jeewon Yoo
Mathematics and Statistics
University of British Columbia Okanagan
Kelowna
BC V1V 1V7
Canada
e-mail: blair.spearman@ubc.ca

Qiduan Yang
e-mail: qiduan.yang@ubc.ca

Jeewon Yoo
e-mail: Jeewon.Yoo@ubc.ca

Received: 7 July 2015