Chad T. DAVIS, Blair K. SPEARMAN† et Jeewon YOO

Cubic polynomials defining monogenic fields with the same discriminant
Tome 30, no 3 (2018), p. 991-996.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_3_991_0>
Cubic polynomials defining monogenic fields with the same discriminant

par CHAD T. DAVIS, BLAIR K. SPEARMAN† et JE EWON YOO

Abstract. Let $K$ be a number field with ring of integers $\mathcal{O}_K$. $K$ is said to be monogenic if $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$. Monogeneity of a number field is not always guaranteed. Furthermore, it is rare for two number fields to have the same discriminant, thus finding fields with these two properties is an interesting problem. In this paper we show that there exist infinitely many triples of polynomials defining distinct monogenic cubic fields with the same discriminant.

1. Introduction

Let $K$ be a number field with ring of integers $\mathcal{O}_K$ and discriminant $d(K)$. $K$ is called monogenic if there exists an element $\theta \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbb{Z}[\theta]$. The properties of monogeneity and sharing the same discriminant are uncommon (see for instance [4], and [5, p. 80, Remark 2.4]) thus, finding fields that have both properties is an interesting problem. The following three polynomials provide an example of this phenomenon (see [2, p. 94, Exercise 21])

\begin{align*}
p_1(X) &= X^3 - 18X - 6, \\
p_2(X) &= X^3 - 36X - 78, \\
p_3(X) &= X^3 - 54X - 150.
\end{align*}
Note that the coefficients of these polynomials are in arithmetic progression. The purpose of this paper is to give three infinite families of polynomials \( f_1(X), f_2(X), \) and \( f_3(X) \), defining cubic monogenic fields over \( \mathbb{Q} \) of the same discriminant. In particular we prove the following

**Theorem 1.** There exists infinitely many pairs of relatively prime integers \((k, e)\) satisfying \( k \equiv \pm 1 \pmod{3} \), \( e \equiv \pm 1 \pmod{3} \), and

\[
k(3k^4 - 6k^2e^2 - e^4)
\]

is squarefree. For each such pair \((k, e)\), the polynomials

\[
\begin{align*}
f_1(X) &= X^3 - 9k(k + e)X - 3k(3k^2 + 6ke + e^2), \\
f_2(X) &= X^3 - 9k^2X - 3k(3k^2 + e^2), \\
f_3(X) &= X^3 - 9k(k - e)X - 3k(3k^2 - 6ke + e^2),
\end{align*}
\]

define distinct monogenic cubic fields with the same discriminant. Furthermore, the set of integers defined in equation (1.1) is infinite.

2. Preliminaries

In this section, we provide some preliminary results. Throughout this section, \( k \) and \( e \) will be as in the statement of Theorem 1.

**Lemma 1.** The polynomials \( f_1, f_2, \) and \( f_3 \) of equation (1.2) are irreducible over \( \mathbb{Q} \) and each have the same polynomial discriminant.

**Proof.** Since \( 3 \nmid k, e \) it is clear that \( 3 \) exactly divides the constant coefficients of \( f_1, f_2, \) and \( f_3, \) hence they are 3-Eisenstein. Verifying that they have the same discriminant is strictly computational. \( \square \)

**Lemma 2.** Let \( f_1, f_2, \) and \( f_3 \) be the polynomials from equation (1.2). Let \( \theta_i \) be a root of \( f_i \), and set \( K_i = \mathbb{Q}(\theta_i) \) for \( i \in \{1, 2, 3\} \). Then \( K_1, K_2, \) and \( K_3 \) are monogenic.

**Proof.** If the discriminant of \( f_i \) is equal to \( d(K_i) \) for each \( i \in \{1, 2, 3\} \) then each \( K_i \) is monogenic. Thus, it suffices to show that for each prime \( p \), the exact power of \( p \) in the discriminant of \( f_i \) is equal to the exact power of \( p \) dividing \( d(K_i) \). This can be determined using a result due to Llorente and Nart ([3, Theorem 2]), or alternatively, by Tables A, B, and C on p. 4–7 of [1]. The discriminant of each \( f_i \), which we denote by \( \Delta \), is equal to

\[
\Delta = 3^5k^2(3k^4 - 6k^2e^2 - e^4).
\]

Following the notation of [3] and [1], let \( v_p(x) \) denote the exact power of a prime \( p \) dividing an integer \( x \) and let \( s_p = v_p(\Delta) \). We show that \( s_p = v_p(d(K_i)), \ i = 1, 2, 3, \) for all primes \( p \). We give the proof for the field \( K_1 \) and note that the other cases are done similarly. Let \( a_1 \) and \( b_1 \) denote the coefficients on \( X \) and the constant coefficient of \( f_1 \) respectively. We break into cases when \( p = 2, p = 3, \) and \( p > 3. \)
Case 1: \( p = 2 \). The assumption that \( k(3k^4 - 6k^2e^2 - e^4) \) is squarefree implies that \( k \) and \( e \) have opposite parity. If \( k \) is even, then \( k \equiv 2 \pmod{4} \) lest equation (1.1) is divisible by a square. In this case, we have \( a_1 \equiv 0 \pmod{2} \) and \( b_1 \equiv 2 \pmod{4} \). Then line 2 of Table A in [1] implies that \( s_2 = v_2(d(K_1)) = 2 \) as desired. If \( k \) is odd and \( e \) is even, then \( b_1 \equiv 1 \pmod{2} \), so that line 1 of Table A of [1] implies that \( s_2 = v_2(d(K_1)) = 0 \) as desired.

Case 2: \( p = 3 \). Since neither \( k \) nor \( e \) is divisible by 3, it is easily verified that \( a_1 \equiv 0 \pmod{9} \) and \( b_1 \equiv 0 \pmod{3} \) but \( b_1 \not\equiv 0 \pmod{9} \). Thus line 3 of Table B of [1] implies that \( s_3 = v_3(d(K_1)) = 5 \) as desired.

Case 3: \( p > 3 \). First suppose that \( p \) does not divide \( k \) nor \( e \). Then

\[
\begin{align*}
a_1 & \equiv -9k(k + e) \pmod{p} \\
(2.1) \quad b_1 & \equiv -3k(3k^2 + 6ke + e^2) \pmod{p} \\
\Delta & \equiv -4a_1^3 + 27b_1^2 \pmod{p}.
\end{align*}
\]

If \( k \equiv -e \pmod{p} \), then from equation (2.1) we have

\[
a_1 \equiv 0 \pmod{p} \quad \text{and} \quad b_1 \equiv -6e^3 \not\equiv 0 \pmod{p}
\]

so that \( p \nmid \Delta \). Consequently \( p \nmid d(K_1) \) and \( s_p = v_p(d(K_1)) \). If \( k \not\equiv -e \pmod{p} \), then from equation (2.1) we have \( a_1 \not\equiv 0 \pmod{p} \). If \( b_1 \equiv 0 \pmod{p} \) then \( \Delta \not\equiv 0 \pmod{p} \) so \( s_p = v_p(d(K_1)) \). If \( b_1 \not\equiv 0 \pmod{p} \), then recalling that \( 3k^4 - 6k^2e^2 - e^4 \) is squarefree, we see that \( s_p = 0 \) or 1. From line 5 of Table C of [1], we get that \( s_p = v_p(d(K_1)) \) as required.

Now suppose \( p \) divides \( k \) but does not divide \( e \). Then using the assumption that equation (1.1) is squarefree, it is easily checked that \( v_p(a_1) = v_p(b_1) = 1 \). Using line 2 of Table C of [1], we have \( s_p = v_p(d(K_1)) = 2 \) as desired. Finally, if \( p \) divides \( e \) but does not divide \( k \), then \( p \nmid \Delta \) so that \( s_p = v_p(d(K_1)) = 0 \) as required.

In all cases, it has been verified that \( v_p(d(K_1)) = s_p = v_p(\Delta) \) for all primes \( p \geq 2 \). Thus \( d(K_1) = \Delta \) and \( K_1 \) is monogenic. \( \Box \)

**Lemma 3.** Let everything be as in Lemma 2. Then \( K_1, K_2, \) and \( K_3 \) are distinct.

**Proof.** Towards a contradiction, suppose that two of the fields are not distinct. Without loss of generality, suppose that \( \mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2) \) (noting that the other two cases are done similarly). Then \( \theta_1 \in K_2 \). Since \( K_2 \) is monogenic by Lemma 2, there exist \( a, b, c \in \mathbb{Z} \) such that

\[
\theta_1 = a + b\theta_2 + c\theta_2^2.
\]
Since the trace of \( \theta_1 \) is zero, it follows that \( a = -6ck^2 \). Making this substitution, we calculate the minimal polynomial of the above element as

\[
F(X) = X^3 + uX + v
\]

where

\[
u = -3k((3k^2 + e^2)3 + 18k^3b^2c + (27k^4 + 9k^2e^2)bc^2 + (3ke^4 + 18k^3e^2 + 9k^5)e^3).
\]

Since the minimal polynomial of \( \theta_1 \) is \( f_1(X) \), we see that the coefficients of \( f_1 \) and \( F \) must be equal. Thus, from the constant term

\[
0 \equiv \frac{v}{3} + k(3k^2 + 6ke + e^2) \equiv 2ke^2(b + 2)^3 \pmod{3}.
\]

Since 3 does not divide \( k \) nor \( e \), this congruence forces \( b \equiv 1 \pmod{3} \).

Substituting \( b = 1 + 3m \) for some integer \( m \) into the equations for \( u \) and \( v \) yields two congruences

\[
0 \equiv \frac{u}{9} + k(k + e) \equiv 2ke(ec + 2) \pmod{3},
\]

\[
0 \equiv \frac{1}{3} \left( \frac{v}{3} + k(3k^2 + 6ke + e^2) \right) \equiv 2k^2e(ec + 1)^3 \pmod{3}
\]

which is impossible as these two congruences can not simultaneously hold. Thus \( K_1 \) and \( K_2 \) must be distinct fields. \( \square \)

3. Proof of Theorem

Proof. By Lemma 1, each \( f_i \) is irreducible over \( \mathbb{Q} \) and have the same polynomial discriminant. Lemma 2 implies that the fields \( K_i \) are monogenic for each \( i \in \{1,2,3\} \) and Lemma 3 implies that the fields \( K_i \) are all distinct. The only thing left to verify is that there are infinitely many integer pairs \((k,e)\) such that the result holds. In order for this to happen, we need only show that equation \((1.1)\) is squarefree for infinitely many pairs of integers \((k,e)\). This follows from Theorem 1 on p. 950–951 of [6] with \( A = \pm 1, B = \pm 1, M = 3, m = 4, w = 1, r = 5, k = 2, F = k(3k^4 - 6k^2e^2 - e^4) \) and letting \( x \to \infty \). The statement that there are infinitely many integers as in equation \((1.1)\) follows immediately from this argument. Finally, note that this implies there are infinitely many field discriminants that satisfy the property given in the theorem. \( \square \)

4. Examples

Let \( \theta_i \) be a root of \( f_i \) for each \( i = 1,2,3 \). The following table gives some numerical examples of polynomials \( f_1, f_2, f_3 \) that define distinct monogenic fields over \( \mathbb{Q} \) of the same discriminant. Notice that when \((k,e) = (2,1)\) we recover the example from [2] cited at the beginning of this paper.
Monogenic cubic fields with the same discriminant

$(k, e) \quad f_i(X) \quad \Delta f_i \quad \text{Integral Basis for } K_i = \mathbb{Q}(\theta_i)$

| $(k, e)$ | $f_1(X)$ | $\Delta f_i$ | Integral Basis for $K_i = \mathbb{Q}(\theta_i)$ |
|----------|----------|----------------|---------------------------------------------|
| $(2, 1)$ | $f_1(X) = X^3 - 54X - 150$ | $22356 = 2^2 \cdot 3^3 \cdot 23$ | $\{1, \theta_i, \theta_i^2\}$ |
|          | $f_2(X) = X^3 - 36X - 78$ | | |
|          | $f_3(X) = X^3 - 18X - 6$ | | |
| $(1, 2)$ | $f_1(X) = X^3 - 27X - 57$ | $-8991 = -3^5 \cdot 37$ | $\{1, \theta_i, \theta_i^2\}$ |
|          | $f_2(X) = X^3 - 9X - 21$ | | |
|          | $f_3(X) = X^3 + 9X + 15$ | | |
| $(1, 4)$ | $f_1(X) = X^3 - 45X - 129$ | $-84807 = -3^5 \cdot 349$ | $\{1, \theta_i, \theta_i^2\}$ |
|          | $f_2(X) = X^3 - 9X - 57$ | | |
|          | $f_3(X) = X^3 + 27X + 15$ | | |
| $(1, 10)$ | $f_1(X) = X^3 - 99X - 489$ | $-2575071 = -3^5 \cdot 10597$ | $\{1, \theta_i, \theta_i^2\}$ |
|         | $f_2(X) = X^3 - 90X - 309$ | | |
|         | $f_3(X) = X^3 + 81X - 129$ | | |

Table 1. Integral Bases and discriminants for $K = \mathbb{Q}(\theta_i)$ defined by $f_i$ for $i \in \{1, 2, 3\}$.

We end with a numerical example of an extension of Theorem 1 to four polynomials that define distinct monogenic fields with the same discriminant. Let $\theta_i$ be a root of $f_i$ and set $K_i = \mathbb{Q}(\theta_i)$ for $i \in \{1, 2, 3, 4\}$.

| $f_i(X)$ | $\Delta f_i$ | Integral Basis for $K_i = \mathbb{Q}(\theta_i)$ |
|----------|-------------|---------------------------------------------|
| $f_1(X) = X^3 - 990X - 10830$ | | |
| $f_2(X) = X^3 - 900X - 9030$ | $714395700 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 29399$ | $\{1, \theta_i, \theta_i^2\}$ |
| $f_3(X) = X^3 - 810X - 7230$ | | |
| $f_4(X) = X^3 - 720X + 5370$ | | |

Table 2. Integral Bases and discriminants for $K = \mathbb{Q}(\theta_i)$ defined by $f_i$ for $i \in \{1, 2, 3, 4\}$.

References

[1] S. Alaca, “$p$-integral bases of a cubic field”, Proc. Am. Math. Soc. 126 (1998), no. 7, p. 1949-1953.
[2] Z. I. Borevich & I. R. Shafarevich, Number Theory, Academic Press Inc., 1966.
[3] P. Llorente & E. Nart, “Effective determination of the decomposition of the rational primes in a cubic field”, Proc. Am. Math. Soc. 87 (1983), no. 4, p. 579-585.
[4] D. C. Mayer, “How many fields share a common discriminant? (Multiplicity problem)”, Algebra and Algebraic Number Theory, http://www.algebra.at/index_e.htm.
[5] R. A. Mollin, Algebraic Number Theory, 2nd revised ed., Discrete Mathematics and its Applications, CRC Press, 2011.
[6] C. L. Stewart & J. Top, “On ranks of twists of elliptic curves and power-free values of binary forms”, *J. Am. Math. Soc.* 8 (1995), no. 4, p. 943-973.

Chad T. Davis
3333 University Way
University of British Columbia - Okanagan
Kelowna, BC, Canada, V1V 1V7.
E-mail: chad.davis@ubc.ca

Blair K. Spearman†

Jeewon Yoo
3333 University Way
University of British Columbia - Okanagan
Kelowna, BC, Canada, V1V 1V7
E-mail: j.yoo1026@gmail.com