NEW ZEALAND JOURNAL OF MATHEMATICS
Volume 26 (1997), 293–299

QUADRATIC SUBFIELDS OF THE SPLITTING FIELD OF A DIHEDRAL QUINTIC TRINOMIAL x^5+ax+b

BLAIR K. SPEARMAN, LAURA Y. SPEARMAN AND KENNETH S. WILLIAMS

(Received November 1995)

Abstract. It is known that every quadratic field K is a subfield of the splitting field of a dihedral quintic polynomial. In this paper it is shown that K is a subfield of the splitting field of a dihedral quintic trinomial $x^5 + ax + b$ if and only if the discriminant of K is of the form $-4q$ or $-8q$, where q is the (possibly empty) product of distinct primes congruent to 1 modulo 4.

1. Introduction

The quintic polynomial $f(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \in Q[x]$ is said to be dihedral if its Galois group is D_5 (the dihedral group of order 10). We denote the splitting field of $f(x)$ by $SF(f(x))$. Jensen and Yui [**3**, Theorem 1.2.1] have shown (as a special case of a more general result) that if K is a quadratic field then there exists a dihedral quintic polynomial $f(x)$ such that $K \subseteq SF(f(x))$. In this paper we characterize those quadratic fields K for which there exist a dihedral quintic trinomial $x^5 + ax + b \in Q[x]$ such that $K \subseteq SF(x^5 + ax + b)$. We remark that if $x^5 + ax + b$ is dihedral then $x^5 + ax + b$ is irreducible, $a \neq 0$, and $b \neq 0$.

After a number of preliminary results, we prove –

Theorem 1.1. *Let K be a quadratic field. Let d denote the discriminant of K. Then there exists a dihedral quintic trinomial $x^5 + ax + b \in Q[x]$ such that $K \subseteq SF(x^5 + ax + b)$ if and only if $d = -4q$ or $-8q$ where q is a (possibly empty) product of distinct primes congruent to* 1 *modulo* 4.

In the course of the proof of Theorem 1.1, we establish the following result.

Theorem 1.2. *Let K be a quadratic field with discriminant $d = -4q$ or $-8q$, where q is a (possibly empty) product of distinct primes* $\equiv 1 \pmod 4$. *Then there exist integers r and s such that*

$$q = r^2 + s^2, \quad r \equiv 1 \pmod 2, \quad s \equiv 0 \pmod 2. \tag{1.1}$$

1991 *AMS Mathematics Subject Classification:* 11R04, 11R09, 11R11, 11R21.
Key words and phrases: quadratic field, dihedral quintic trinomial $x^5 + ax + b$, splitting field.
Research of the third author supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

Set
$$a = \begin{cases} \frac{4(r^2+11rs-s^2)(r^2+rs-s^2)}{(r^2+s^2)^2}, & \text{if } 4\|d, \\ \frac{(11r^2-4rs-11s^2)(r^2-4rs-s^2)}{(r^2+s^2)^2}, & \text{if } 8\|d, \end{cases} \tag{1.2}$$

and
$$b = \begin{cases} \frac{16(3r+4s)(4r-3s)(r^2+rs-s^2)}{5(r^2+s^2)^2}, & \text{if } 4\|d, \\ \frac{4(r-7s)(7r+s)(r^2-4rs-s^2)}{5(r^2+s^2)^2}, & \text{if } 8\|d. \end{cases} \tag{1.3}$$

Then $x^5 + ax + b$ is dihedral and $K \subseteq SF(x^5 + ax + b)$.

Example 1.3. We take $K = Q(\sqrt{-10})$. Here $d = -40$ so that $q = 5$. Choosing $r = 1$ and $s = -2$ we obtain $a = -5$ and $b = 12$ so that $Q(\sqrt{-10}) \subseteq SF(x^5 - 5x + 12)$, in agreement with the table in [**5**].

Choosing $r = 1$ and $s = 2$ we obtain $a = \frac{451}{25}$ and $b = \frac{5148}{125}$ so that

$$Q(\sqrt{-10}) \subseteq SF\left(x^5 + \frac{451}{25}x + \frac{5148}{125}\right) = SF(x^5 + 11275x + 128700).$$

Example 1.4. We take $K = Q(\sqrt{-5})$. Here $d = -20$ so that $q = 5$. Choosing $r = 1$ and $s = -2$ we obtain $a = 20$ and $b = 32$ so that $Q(\sqrt{-5}) \subseteq SF(x^5+20x+32)$.

Choosing $r = 1$ and $s = 2$ we obtain $a = -\frac{76}{25}$ and $b = \frac{352}{125}$ so that

$$Q(\sqrt{-5}) \subseteq SF\left(x^5 - \frac{76}{25}x + \frac{352}{125}\right) = SF(x^5 - 1900x - 8800),$$

in agreement with the table in [**5**].

2. Preliminary Results

We will need the following results in the course of the proof of Theorem 1.1.

Proposition 2.1. *If $x^5 + ax + b \in Q[x]$ is irreducible, then the Galois group of $x^5 + ax + b$ is D_5 if and only if there exist rational numbers $\varepsilon(= \pm 1)$, $c(\geq 0)$, $e(\neq 0)$, and $t(> 0)$ such that*

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \quad b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}, \quad c^2 + 1 = 5t^2. \tag{2.1}$$

Moreover ε, c, e, t are uniquely determined by a and b.

This result can be found in [**3**, pp. 987 and 990]. The only part of this proposition which is not explicitly stated in [**3**] is the assertion about uniqueness, which we now prove. Suppose that ε, c, e, t satisfy (2.1). Then

$$e^4 = \frac{a(c^2 + 1)}{5(3 - 4\varepsilon c)}, \quad e^5 = \frac{-b(c^2 + 1)}{4(11\varepsilon + 2c)},$$

and eliminating e we see that c is a rational root of

$$\frac{a^5(c^2 + 1)^5}{5^5(3 - 4\varepsilon c)^5} = \frac{b^4(c^2 + 1)^4}{2^8(11\varepsilon + 2c)^4},$$

or equivalently

$$a^5 2^8(11\varepsilon + 2c)^4(c^2 + 1) - 5^5 b^4(3 - 4\varepsilon c)^5 = 0.$$

As x^5+ax+b is dihedral, we have $a \neq 0$ and $b \neq 0$, and thus $3-4\varepsilon c \neq 0$ and $11\varepsilon + 2c \neq 0$. Setting

$$r = \frac{4a(4+3\varepsilon c)}{(3-4\varepsilon c)},$$

so that $r \neq -3a$, we have

$$\varepsilon c = \frac{3r-16a}{4(r+3a)}, \qquad c^2+1 = \frac{25(r^2+16a^2)}{16(r+3a)^2},$$

$$11\varepsilon + 2c = \frac{25(r+2a)\varepsilon}{2(r+3a)}, \qquad 3-4\varepsilon c = \frac{25a}{r+3a},$$

so that r is a rational root of

$$(r+2a)^4(r^2+16a^2) - 5^5b^4(r+3a) = 0.$$

This shows that r is a root of the resolvent sextic of x^5+ax+b. As the Galois group of x^5+ax+b is D_5, its resolvent sextic has a unique rational root [**2**, Theorem 1]. Thus r is uniquely determined by a and b. Clearly $c \neq 0$ in view of the third equation in (2.1). Then ε, c, e, t are uniquely determined by

$$\varepsilon c = \frac{3r-16a}{4(r+3a)} (c>0, \varepsilon = \pm 1), \quad e = -\frac{5b(3-4\varepsilon c)}{4a(11\varepsilon+2c)}, \quad \text{and} \quad t = +\sqrt{(c^2+1)/5}.$$

Proposition 2.2. *Suppose that $x^5+ax+b \in Q[x]$ is dihedral. Define ε, c, e, and t uniquely as in Proposition 2.1. Then the splitting field of x^5+ax+b contains a unique quadratic subfield, namely,*

$$Q\left(\sqrt{-5-(1+2\varepsilon c)/t}\right).$$

This result is proved in [**5**].

Proposition 2.3. *All positive integral solutions of $m^2+n^2 = 5z^2$, $(m,n)=1$, $m \equiv 1 \pmod 2$, $n \equiv 0 \pmod 2$, are given by*

$$m = |r^2-4rs-s^2|, \quad n = |2r^2+2rs-2s^2|, \quad z = r^2+s^2,$$

where r and s are integers with

$$r \equiv s+1 \pmod 2, \qquad (r,s)=1, \qquad 2r+s \not\equiv 0 \pmod 5. \tag{2.2}$$

This result is easily proved using the arithmetic of the domain of Gaussian integers.

Proposition 2.4. *Let $\varepsilon (=\pm 1)$, $c (\geq 0)$, $e (\neq 0)$ be rational numbers. Then the polynomial*

$$f_{\varepsilon,c,e}(x) = x^5 + \frac{5e^4(3-4\varepsilon c)}{c^2+1}x - \frac{4e^5(11\varepsilon+2c)}{c^2+1}$$

is reducible if and only if

$$c = 3/4, \quad \varepsilon = 1 \quad or \quad c = 11/2, \quad \varepsilon = -1.$$

Proof. If $c=3/4$, $\varepsilon = 1$ then $f_{\varepsilon,c,e}(x) = x^5 - 32e^5 = (x-2e)(x^4+2ex^3+4e^2x^2+8e^3x+16e^4)$. If $c = 11/2$, $\varepsilon = -1$ then $f_{\varepsilon,c,e}(x) = x^5+4e^4x = x(x^2-2ex+2e^2)(x^2+2ex+2e^2)$. Now suppose that $f_{\varepsilon,c,e}(x)$ is reducible. By [**3**, Theorem and remark following equation (19)] the roots of $f_{\varepsilon,c,e}(x)=0$ are

$$x_j = e(\omega^j u_1 + \omega^{2j}u_2 + \omega^{3j}u_3 + \omega^{4j}u_4) \quad (j=0,1,2,3,4),$$

where $\omega = \exp(2\pi i/5)$ and

$$u_1 = \left(\frac{v_1^2 v_3}{D^2}\right)^{1/5}, \quad u_2 = \left(\frac{v_3^2 v_4}{D^2}\right)^{1/5}, \quad u_3 = \left(\frac{v_2^2 v_1}{D^2}\right)^{1/5}, \quad u_4 = \left(\frac{v_4^2 v_2}{D^2}\right)^{1/5},$$

$$v_1 = \sqrt{D} + \sqrt{D - \varepsilon\sqrt{D}}, \qquad v_2 = -\sqrt{D} - \sqrt{D + \varepsilon\sqrt{D}},$$

$$v_3 = -\sqrt{D} + \sqrt{D + \varepsilon\sqrt{D}}, \qquad v_4 = \sqrt{D} - \sqrt{D - \varepsilon\sqrt{D}}, \quad D = c^2 + 1.$$

From these formulae we see that the degree of the splitting field of $f_{\varepsilon,c,e}(x)$ is of the form $2^r 5^s$ for some nonnegative integers r and s. Thus $f_{\varepsilon,c,e}(x)$ cannot have an irreducible cubic factor $\in Q[x]$. Hence $f_{\varepsilon,c,e}(x)$ possesses a linear factor over Q. Thus $f_{\varepsilon,c,1}(x)$ has a rational root x, and

$$x^5 + \frac{5(3-4\varepsilon c)x}{c^2+1} - \frac{4(11\varepsilon + 2c)}{c^2+1} = 0. \tag{2.3}$$

If $x = 0$ then $c = -11\varepsilon/2$, and so $c = 11/2$ and $\varepsilon = -1$ as required. If $x = 2\varepsilon$ then (2.3) gives after a short calculation $c = 3\varepsilon/4$, and so $c = 3/4$ and $\varepsilon = 1$ as required. Hence we may suppose that $x \neq 0, 2\varepsilon$. Writing (2.3) as a quadratic equation in c, we obtain

$$(x^5)c^2 + (-20\varepsilon x - 8)c + (x^5 + 15x - 44\varepsilon) = 0.$$

Solving this equation for c, we obtain

$$c = \frac{1}{x^5}\left(10\varepsilon x + 4 \pm (x^3 - \varepsilon x^2 + 2x + 2\varepsilon)\sqrt{-(x-2\varepsilon)(x^3 + 4\varepsilon x^2 + 7x + 2\varepsilon)}\,\right).$$

Thus there is a rational number y such that

$$y^2 = -(x-2\varepsilon)(x^3 + 4\varepsilon x^2 + 7x + 2\varepsilon). \tag{2.4}$$

Setting

$$X = \frac{-40\varepsilon}{x - 2\varepsilon}, \qquad Y = \frac{40y}{(x-2\varepsilon)^2}, \tag{2.5}$$

we deduce from (2.4) that (X, Y) is a rational point on the elliptic curve E given by

$$Y^2 = X^3 - 35X^2 + 400X - 1600. \tag{2.6}$$

The minimal equation for E is

$$y_1^2 + x_1 y_1 + y_1 = x_1^3 - x_1 - 2, \tag{2.7}$$

which is obtained from (2.6) by setting

$$X = 4x_1 + 12, \qquad Y = 4x_1 + 8y_1 + 4. \tag{2.8}$$

From the table in [1], we see that E has conductor 50, and that its group $E(Q)$ of rational points has order 3. Thus, apart from the point at infinity, the curve (2.7) has just 2 rational points on it, and these are $(x_1, y_1) = (2, 1)$ and $(2, -4)$. These give the rational points $(X, Y) = (20, \pm 20)$ on the curve (2.6), and the transformation (2.5) shows that there are no rational points on the curve (2.4) with $x \neq 0,\ 2\varepsilon$. $\square$

Proof of Theorem 1.1. Let $x^5+ax+b \in Q[x]$ be a dihedral polynomial. By Proposition 2.1 there exist unique rational numbers $\varepsilon(=\pm 1)$, $c(>0)$, $e(\neq 0)$, and $t(>0)$ such that (2.1) holds. As c is a positive rational number, there exist positive coprime integers m and n such that $c=m/n$. Then, from $c^2+1=5t^2$, we obtain $m^2+n^2=5z^2$, where $z=nt$ is a positive integer. Hence, by Proposition 2.3, there are integers r and s satisfying (2.2) such that

$$m=|r^2-4rs-s^2|,\quad n=|2r^2+2rs-2s^2|,\quad z=r^2+s^2,\quad \text{if}\quad m\equiv 1 \pmod 2,\ n\equiv 0 \pmod 2, \tag{2.9}$$

$$m=|2r^2+2rs-2s^2|,\quad n=|r^2-4rs-s^2|,\quad z=r^2+s^2,\quad \text{if}\quad m\equiv 0 \pmod 2,\ n\equiv 1 \pmod 2. \tag{2.10}$$

Now, by Proposition 2.2, $SF(x^5+ax+b)$ contains a unique quadratic subfield, namely,

$$K=Q\left(\sqrt{-5-(1+2\varepsilon c)/t}\,\right).$$

If (3.1) holds then $c=\frac{|r^2-4rs-s^2|}{2|r^2+rs-s^2|}$ and $t=\frac{r^2+s^2}{2|r^2+rs-s^2|}$, so that

$$(-5-(1+2\varepsilon c)/t)(r^2+s^2)=-5(r^2+s^2)-2\varepsilon|r^2-4rs-s^2|-2|r^2+rs-s^2|$$

$$=\begin{cases}-(3r-s)^2, & \text{if } \varepsilon|r^2-4rs-s^2|=r^2-4rs-s^2 \text{ and } |r^2+rs-s^2|=r^2+rs-s^2,\\ -5(r-s)^2, & \text{if } \varepsilon|r^2-4rs-s^2|=r^2-4rs-s^2 \text{ and } |r^2+rs-s^2|=-(r^2+rs-s^2),\\ -5(r+s)^2, & \text{if } \varepsilon|r^2-4rs-s^2|=-(r^2-4rs-s^2) \text{ and } |r^2+rs-s^2|=r^2+rs-s^2,\\ -(r+3s)^2, & \text{if } \varepsilon|r^2-4rs-s^2|=-(r^2-4rs-s^2) \text{ and } |r^2+rs-s^2|=-(r^2+rs-s^2),\end{cases}$$

and thus

$$K=\begin{cases}Q\left(\sqrt{-(r^2+s^2)}\,\right), & \text{if } \operatorname{sgn}\left(\varepsilon(r^2-4rs-s^2)(r^2+rs-s^2)\right)=+1,\\ Q\left(\sqrt{-5(r^2+s^2)}\,\right), & \text{if } \operatorname{sgn}\left(\varepsilon(r^2-4rs-s^2)(r^2+rs-s^2)\right)=-1.\end{cases}$$

If (3.2) holds then $c=\frac{2|r^2+rs-s^2|}{|r^2-4rs-s^2|}$ and $t=\frac{r^2+s^2}{|r^2-4rs-s^2|}$, so that

$$(-5-(1+2\varepsilon c)/t)(r^2+s^2)=-5(r^2+s^2)-|r^2-4rs-s^2|-4\varepsilon|r^2+rs-s^2|$$

$$=\begin{cases}-10r^2, & \text{if } \varepsilon|r^2+rs-s^2|=r^2+rs-s^2 \text{ and } |r^2-4rs-s^2|=r^2-4rs-s^2,\\ -2(r-2s)^2, & \text{if } \varepsilon|r^2+rs-s^2|=-(r^2+rs-s^2) \text{ and } |r^2-4rs-s^2|=r^2-4rs-s^2,\\ -2(2r+s)^2, & \text{if } \varepsilon|r^2+rs-s^2|=r^2+rs-s^2 \text{ and } |r^2-4rs-s^2|=-(r^2-4rs-s^2),\\ -10s^2, & \text{if } \varepsilon|r^2+rs-s^2|=-(r^2+rs-s^2) \text{ and } |r^2-4rs-s^2|=-(r^2-4rs-s^2),\end{cases}$$

and thus

$$K=\begin{cases}Q\left(\sqrt{-2(r^2+s^2)}\,\right), & \text{if } \operatorname{sgn}\left(\varepsilon(r^2-4rs-s^2)(r^2+rs-s^2)\right)=-1,\\ Q\left(\sqrt{-10(r^2+s^2)}\,\right), & \text{if } \operatorname{sgn}\left(\varepsilon(r^2-4rs-s^2)(r^2+rs-s^2)\right)=+1.\end{cases}$$

As $(r,s)=1$, the squarefree part of r^2+s^2 is a product of distinct primes $\equiv 1 \pmod 4$ or twice such a product and so

$$d=\operatorname{disc}(K)=-4q \quad\text{or}\quad -8q,$$

where q is a (possibly empty) product of distinct primes $\equiv 1 \pmod 4$.

Conversely suppose that K is a quadratic field with $d(K) = -4q$ or $-8q$, where q is a (possibly empty) product of distinct primes $\equiv 1 \pmod 4$. As q is a product of primes $\equiv 1 \pmod 4$ there exist integers r and s such that

$$q = r^2 + s^2, \quad r \equiv 1 \pmod 2, \quad s \equiv 0 \pmod 2.$$

Now define rational numbers $\varepsilon(= \pm 1)$, $c(> 0)$ and $t(> 0)$ by

$$\varepsilon = \begin{cases} \operatorname{sgn}\big((r^2 - 4rs - s^2)(r^2 + rs - s^2)\big), & \text{if } 2^2 \| d(K), \\ -\operatorname{sgn}\big((r^2 - 4rs - s^2)(r^2 + rs - s^2)\big), & \text{if } 2^3 \| d(K), \end{cases} \tag{2.11}$$

$$c = \begin{cases} \frac{|r^2-4rs-s^2|}{2|r^2+rs-s^2|}, & \text{if } 2^2 \| d(K), \\ \frac{2|r^2+rs-s^2|}{|r^2-4rs-s^2|}, & \text{if } 2^3 \| d(K), \end{cases}$$

$$t = \begin{cases} \frac{r^2+s^2}{2|r^2+rs-s^2|}, & \text{if } 2^2 \| d(K), \\ \frac{r^2+s^2}{|r^2-4rs-s^2|}, & \text{if } 2^3 \| d(K), \end{cases}$$

$$a = \begin{cases} \frac{4(r^2+11rs-s^2)(r^2+rs-s^2)}{(r^2+s^2)^2}, & \text{if } 2^2 \| d(K), \\ \frac{(11r^2-4rs-11s^2)(r^2-4rs-s^2)}{(r^2+s^2)^2}, & \text{if } 2^3 \| d(K), \end{cases}$$

$$b = \begin{cases} \frac{16(3r+4s)(4r-3s)(r^2+rs-s^2)}{5(r^2+s^2)^2}, & \text{if } 2^2 \| d(K), \\ \frac{4(r-7s)(7r+s)(r^2-4rs-s^2)}{5(r^2+s^2)^2}, & \text{if } 2^3 \| d(K). \end{cases} \tag{2.12}$$

Set $f(x) = x^5 + ax + b \in Q[x]$, so that $f(x) = f_{\varepsilon,c,-\varepsilon}(x)$. It is easy to check that $c^2 + 1 = 5t^2$ and $(c, \varepsilon) \neq (3/4, 1)$ or $(11/2, -1)$. Hence, by Proposition 2.4, $f(x)$ is irreducible. Then, by Proposition 2.1, we see that $f(x)$ is dihedral. By Proposition 2.2, $SF(x^5 + ax + b)$ contains $Q\big(\sqrt{-5 - (1 + 2\varepsilon c)/t}\,\big)$. It is easy to verify from (3.3) and (3.4) that $\varepsilon c \neq 2$. Then the relation

$$\big(-5 - (1 + 2\varepsilon c)/t\big)\big(-5 + (1 + 2\varepsilon c)/t\big) = \big((c - 2\varepsilon)/t\big)^2$$

shows that

$$\begin{aligned} Q\big(\sqrt{-5 - (1 + 2\varepsilon c)/t}\,\big) &= Q\big(\sqrt{-5 \pm (1 + 2\varepsilon c)/t}\,\big) \\ &= \begin{cases} Q\big(\sqrt{-(r^2 + s^2)}\,\big), & \text{if } 2^2 \| d(K), \\ Q\big(\sqrt{-2(r^2 + s^2)}\,\big), & \text{if } 2^3 \| d(K), \end{cases} \\ &= K. \end{aligned}$$

This completes the proofs of Theorems 1.1 and 1.2. $\square$

References

1. J.E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.
2. D.S. Dummit, *Solving solvable quintics*, Math. Comp. **57** (1991), 387–401.
3. C.U. Jensen and N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory **15** (1982), 347–375.
4. Blair K. Spearman and Kenneth S. Williams, *Characterization of solvable quintics $x^5 + ax + b$*, Amer. Math. Monthly **101** (1994), 986–992.
5. Blair K. Spearman, Laura Y. Spearman and Kenneth S. Williams, *The subfields of the splitting field of a solvable quintic trinomial $X^5 + aX + b$*, J. Math. Sci. **6** (1995), 15–18.

Blair K. Spearman
Department of Mathematics and Statistics
Okanagan University College
Kelowna, B.C. V1V 1V7
CANADA
bkspearm@okanagan.bc.ca

Laura Y. Spearman
City of Kelowna Information Services
Department
Kelowna, B.C. V1Y 1J4
CANADA

Kenneth S. Williams
Department of Mathematics and Statistics
Carleton University
Ottawa
Ontario K1S 5B6
CANADA
williams@math.carleton.ca