Far East J. Math. Sci. (FJMS) 1(4) (1999), 659-667

CYCLIC QUARTIC SUBFIELDS OF THE SPLITTING FIELD OF A QUINTIC TRINOMIAL $x^5 + ax + b$ WITH GALOIS GROUP F_{20}

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

(Received April 9, 1999)

Submitted by K. K. Azad

Abstract

Let K be a cyclic quartic field. A necessary and sufficient condition is given for K to belong to the splitting field of some quintic trinomial $x^5 + ax + b$ with Galois group F_{20}.

1. Introduction

We denote the splitting field of $f(x) \in Q[x]$ by $SF(f(x))$. Recently a characterization was given by Spearman, Spearman and Williams [5] for a quadratic field k to belong to $SF(x^5 + ax + b)$ for some quintic trinomial $x^5 + ax + b$ with Galois group D_5 (the dihedral group of order 10). In this paper, we consider the analogous problem for cyclic quartic fields and quintic trinomials $x^5 + ax + b$ with Galois group F_{20} (the Frobenius group of order 20).

1991 Mathematics Subject Classification: 11R04, 11R09, 11R16, 11R21.

Key words and phrases: cyclic quartic fields, splitting field, quintic trinomial.

Research of the first author was supported by a Natural Sciences and Engineering Research Council of Canada grant.

Research of the second author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

We recall that a cyclic quartic field K can be given uniquely in the following standard form [1]:

$$K = Q\left(\sqrt{A(D + B\sqrt{D})}\right), \tag{1.1}$$

where A, B, C, D are integers such that

$$A \text{ is squarefree and odd,} \tag{1.2}$$

$$D = B^2 + C^2 \text{ is squarefree, } B > 0,\ C > 0, \tag{1.3}$$

$$(A, D) = 1. \tag{1.4}$$

An algorithm to put a cyclic quartic field in standard form is given in [2]. We make use of this algorithm in proving the following theorem in Section 2.

Theorem. *Let K be a cyclic quartic field given in standard form* (1.1) *with A, B, C, D as specified in* (1.2)-(1.4) *except that if $B - 2C \equiv 0 \pmod 5$, we choose $C < 0$ instead of $C > 0$. Then there exists a quintic trinomial $x^5 + ax + b \in Q[x]$ with Galois group F_{20} such that $K \subseteq SF(x^5 + ax + b)$ if and only if*

$$A < 0,\ p\,(prime) \mid A \Rightarrow p \equiv 1 \pmod 4. \tag{1.5}$$

If (1.5) *holds, then there are integers X and Y such that*

$$|A| = X^2 + Y^2,\ X - 2Y \not\equiv 0 \pmod 5, \tag{1.6}$$

and

$$K \subseteq SF(x^5 + ax + b) \tag{1.7}$$

with

$$a = \frac{5(3 - 4\varepsilon c)}{c^2 + 1}, \quad b = \frac{-4(11\varepsilon + 2c)}{c^2 + 1}, \tag{1.8}$$

$$c = \left|\frac{m}{n}\right|, \quad \varepsilon = \operatorname{sgn}\left(\frac{m}{n}\right), \tag{1.9}$$

and

$$m + ni = (2 - i)(B + Ci)(X + Yi)^2 \tag{1.10}$$

2. Proof of Theorem

Suppose $x^5 + ax + b \in Q[x]$ has Galois group F_{20} and $K \subseteq SF(x^5 + ax + b)$. Then, by [3, Theorem], there exist $c\,(\geq 0) \in Q$, $e\,(\neq 0) \in Q$ and $\varepsilon = \pm 1$ such that

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

where

$$c^2 + 1 \neq 5t^2 \quad \text{for any } t \in Q. \tag{2.2}$$

By [4, Theorem], we have

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

As K is cyclic

$$K = Q\left(\sqrt{-5 \pm (1 + 2\varepsilon c)\sqrt{\frac{5}{c^2 + 1}}}\right) \tag{2.3}$$

for both choices of sign. Setting $\varepsilon c = m/n$, where m and n are coprime integers, we obtain

$$K = Q\left(\sqrt{-5 - (2m + n)\sqrt{\frac{5}{m^2 + n^2}}}\right)$$

so that as $\sqrt{5(m^2 + n^2)} \in K$, we have

$$K = Q\left(\sqrt{-25(m^2 + n^2) - (10m + 5n)\sqrt{5(m^2 + n^2)}}\right).$$

Writing

$$K = \begin{cases} Q\left(\sqrt{-5\left(5(m^2 + n^2) + (2m + n)\sqrt{5(m^2 + n^2)}\right)}\right), & \text{if } (2m + n, 2n - m) = 1, \\ Q\left(\sqrt{-5\left(\dfrac{m^2 + n^2}{5} + \dfrac{(2m + n)}{5}\sqrt{\dfrac{m^2 + n^2}{5}}\right)}\right), & \text{if } (2m + n, 2n - m) = 5, \end{cases}$$

we see that $A = -5$ in step 1 of the algorithm in [2]. Since the algorithm can only change A by primes congruent to 1 modulo 4 and does not change the sign of A, we see that K satisfies (1.5).

Now, suppose that K is a cyclic quartic field given in the standard form (1.1) with A, B, C, D satisfying (1.2)-(1.5) with the modification to the sign of C specified in the theorem. In view of (1.5), we can define integers X and Y by

$$|A| = X^2 + Y^2. \tag{2.4}$$

As A is squarefree, we have

$$(X, Y) = 1. \tag{2.5}$$

Further, if $X - 2Y \equiv 0 (\mathrm{mod}\ 5)$, we replace Y by $-Y$ so that

$$X - 2Y \not\equiv 0 (\mathrm{mod}\ 5). \tag{2.6}$$

Since

$$2 + i \mid u + iv \Leftrightarrow 5 \mid u - 2v$$

our choices for C and Y ensure that

$$2 + i \nmid B + Ci, \quad 2 + i \nmid X + Yi. \tag{2.7}$$

Define $(m, n) \in Q \times Q$ by

$$m + ni = (2 - i)(B + Ci)(X + Yi)^2. \tag{2.8}$$

Clearly,

$$2 + i \nmid m + ni \tag{2.9}$$

in view of (2.7). Taking norms in (2.8), we obtain

$$m^2 + n^2 = 5A^2D. \tag{2.10}$$

Next, we show that

$$(m, n) = 1. \tag{2.11}$$

First we suppose that $2 \mid (m, n)$. From (2.10) we see that $2^2 \mid 5A^2D$, which is impossible as A is odd and D is squarefree. Secondly, we suppose that $5 \mid (m, n)$. Then we see that $2 + i \mid m + ni$, contradicting (2.9). Next we suppose that $q \mid (m, n)$, where q is a prime with $q \equiv 3 (\mathrm{mod}\ 4)$. Then from (2.8) we see that $q \mid (B, C)$ or $q \mid (X, Y)$, contradicting $(B, C) = (X, Y) = 1$. Finally, we suppose that $p \mid (m, n)$, where p is a prime with $p \equiv 1 (\mathrm{mod}\ 4)$ and $p \neq 5$. Then $p = \pi\overline{\pi}$, where π and $\overline{\pi}$ are conjugate Gaussian primes not associated with $2 \pm i$. Thus, from (2.8), as $(B, C) = (X, Y) = 1$, we have, after interchanging the roles of π and $\overline{\pi}$ if necessary, $\pi \mid B + Ci$ and $\overline{\pi} \mid X + Yi$. Taking norms we deduce that $p \mid B^2 + C^2$ and $p \mid X^2 + Y^2$. Hence $p \mid (A, D)$, contradicting that $(A, D) = 1$. This completes the proof of (2.11).

Next, we show that

$$m \neq 0,\ n \neq 0. \tag{2.12}$$

If $m = 0$, (2.10) gives $n^2 = 5A^2D$. Since D is squarefree, we must have $D = 5$ and $n = \pm 5A$. Thus $(m, n) = (0, \pm 5A) = 5|A|$ contradicting (2.11). The argument is exactly the same if $n = 0$.

We now choose

$$\varepsilon = \mathrm{sgn}\left(\frac{m}{n}\right) (= \pm 1),\quad c = \left|\frac{m}{n}\right| (> 0), \tag{2.13}$$

$$a = \frac{5(3 - 4\varepsilon c)}{c^2 + 1},\quad b = \frac{-4(11\varepsilon + 2c)}{c^2 + 1}, \tag{2.14}$$

and set

$$f(x) = x^5 + ax + b \tag{2.15}$$

First we show that $f(x)$ is irreducible over Q. If not, by [5, Prop. 2.4], we have

$$\text{(i) } c = 3/4,\ \varepsilon = 1 \quad \text{or} \quad \text{(ii) } c = 11/2,\ \varepsilon = -1$$

In case (i) we have $m/n = 3/4$ and so, as $(m, n) = 1$, $(m, n) = (3, 4)$ or $(-3, -4)$. Since $2 + i \mid 3 + 4i$ we have $2 + i \mid m + ni$, which contradicts (2.9). In case (ii) we have $m/n = -11/2$ so that $(m, n) = (-11, 2)$ or $(11, -2)$. Since $2 + i \mid 11 - 2i$ we have $2 + i \mid m + ni$, which contradicts (2.9). Hence $f(x)$ is irreducible over Q.

Secondly, we show that the Galois group of $f(x)$ is F_{20}. Since

$$c^2 + 1 = \frac{m^2 + n^2}{n^2} = \frac{5A^2D}{n^2} \neq 5t^2 \quad \text{for any } t \in Q,$$

this follows from [3, p. 990].

Now, by [4, Theorem], the unique (cyclic) quartic subfield of $SF(f(x))$ is

$$\begin{aligned} L &= Q\left(\sqrt{-5 - (1 + 2\varepsilon c)\sqrt{\frac{5}{c^2 + 1}}}\right) \\ &= Q\left(\sqrt{-5 \pm (1 + 2\varepsilon c)\sqrt{\frac{5}{c^2 + 1}}}\right) \\ &= Q\left(\sqrt{-5 + (2m + n)\sqrt{\frac{5}{m^2 + n^2}}}\right) \\ &= Q\left(\sqrt{-25(m^2 + n^2) + (10m + 5n)\sqrt{5(m^2 + n^2)}}\right). \end{aligned}$$

We now apply the algorithm of [2] to express L in standard form. We use the notation of [2] in what follows. We choose

$$a = -25(m^2 + n^2), \; b = 10m + 5n, \; c = 5(m^2 + n^2),$$

so that

$$k = 10n - 5m.$$

As $(m, n) = 1$, we have

$$(2m + n, 2n - m) = 1 \text{ or } 5.$$

If $(2m + n, 2n - m) = 5$, then from

$$(2m + n) + (2n - m)i = (2 - i)(m + ni) = (2 - i)^2(B + Ci)(X + Yi)^2,$$

we see that $2 + i \mid (B + Ci)(X + Yi)^2$, contradicting (2.7). Hence $(2m + n, 2n - m) = 1$ and

$$(b, k) = (10m + 5n, 10n - 5m) = 5(2m + n, 2n - m) = 5.$$

Step 1. $A' = -5$, $B' = 2m + n$, $C' = 2n - m$, $D' = 5(m^2 + n^2)$.

Step 2. Squarefree part of $B' + C'i = (2m + n) + (2n - m)i = (2 - i)^2 \times (B + Ci)(X + Yi)^2$ is $B + Ci$ as $B^2 + C^2 = D$ is squarefree. Thus

$$A' = \left(-5\sqrt{5^2|A|^2}\right)^* = -|A| = A,$$

$$B' = |B| = B,$$

$$C' = |C|,$$

$$D' = B^2 + C^2 = D.$$

Step 3 and 4. Done.

Hence

$$L = Q\left(\sqrt{A(D + B\sqrt{D})}\right) = K,$$

which completes the proof of the theorem.

3. Examples

Example 1. $K = Q\left(\sqrt{-5 - \sqrt{5}}\right)$. Here

$$A = -1,\ B = 1,\ C = 2,\ D = 5.$$

From (1.6) we see that we can choose

$$X = 1,\ Y = 0.$$

Then, by (1.10), we have

$$m + ni = (2 - i)(1 + 2i) = 4 + 3i$$

so that $m = 4$, $n = 3$. Hence, by (1.9), $c = 4/3$ and $\varepsilon = 1$. Then, by (1.8), we have $a = -\frac{21}{5}$ and $b = -\frac{492}{25}$. The theorem gives

$$Q\left(\sqrt{-5-\sqrt{5}}\right) \subseteq SF\left(x^5 - \frac{21}{5}x - \frac{492}{25}\right).$$

Example 2. $K = Q\left(\sqrt{-5(2+\sqrt{2})}\right)$. Here

$$A = -5,\ B = 1,\ C = 1,\ D = 2.$$

From (1.6) we see that we can choose

$$X = 2,\ Y = -1.$$

Then, by (1.10), we have

$$m + ni = (2 - i)(1 + i)(2 - i)^2 = 13 - 9i$$

so that $m = 13$, $n = -9$. From (1.9) we deduce that $c = 13/9$ and $\varepsilon = -1$. Then, from (1.8), we obtain

$$a = \frac{711}{50},\quad b = \frac{1314}{125}$$

so by the theorem

$$Q\left(\sqrt{-5(2+\sqrt{2})}\right) \subseteq SF\left(x^5 + \frac{711}{50}x + \frac{1314}{125}\right).$$

Applying PARI we find that

$$SF\left(x^5 + \frac{711}{50}x + \frac{1314}{125}\right) = SF(x^5 + 10x^3 - 60x^2 + 95x - 44).$$

References

[1] K. Hardy, R. H. Hudson, D. Richman, K. S. Williams and N. M. Holtz, Calculation of the class numbers of imaginary cyclic quartic fields, Carleton-Ottawa Mathematical Lecture Note Series, Number 7, July 1986, 201 pp..

[2] James G. Huard, Blair K. Spearman and Kenneth S. Williams, Integral bases for quartic fields with quadratic subfields, Centre for Research in Algebra and Number Theory Mathematical Research Series (Carleton University, Ottawa, Canada), Number 4, June 1991, 44 pp..

[3] Blair K. Spearman and Kenneth S. Williams, Characterization of solvable quintics $X^5 + aX + b$, Amer. Math. Monthly 101 (1994), 986-992.

[4] Blair K. Spearman, Laura Y. Spearman and Kenneth S. Williams, The subfields of the splitting field of a solvable quintic trinomial, J. Math. Sci. 6 (1995), 15-18.

[5] Blair K. Spearman, Laura Y. Spearman and Kenneth S. Williams, Quadratic subfields of the splitting field of a dihedral quintic trinomial $x^5 + ax + b$, New Zealand J. Math. 26 (1997), 293-299.

Department of Mathematics and Statistics
Okanagan University College
Kelowna, BC, Canada V1V 1V7

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
e-mail: williams@math.carleton.ca