Far East J. Math. Sci. (FJMS) 2(5) (2000), 665-672

QUARTIC TRINOMIALS WITH GALOIS GROUPS A_4 AND V_4

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

(Received March 31, 2000)

Submitted by K. K. Azad

Abstract

Necessary and sufficient conditions for $Gal(X^4 + aX + b) \simeq A_4$ and $Gal(X^4 + aX + b) \simeq V_4$ are given in terms of simple arithmetic conditions on the integers a and b.

Let a and b be nonzero integers such that the quartic trinomial $X^4 + aX + b$ is irreducible in $\mathbb{Z}[X]$. Its discriminant is the integer $-3^3a^4 + 2^8b^3$, see for example [4], which is nonzero as $X^4 + aX + b$ is irreducible. It is known [3, Theorem 1] that

$$-3^3a^4 + 2^8b^3 = c^2 \tag{1}$$

for some integer c if and only if

$$Gal(X^4 + aX + b) \simeq A_4 \text{ or } V_4, \tag{2}$$

where A_4 denotes the alternating group of order 12 and V_4 denotes the Klein 4-group of order 4. (We note that the formula for the discriminant of a quartic polynomial given in [3] is incorrect.) Assuming that (1) holds,

---

2000 Mathematics Subject Classification: 11R09.

Key words and phrases: quartic trinomials, Galois group.

the two possibilities in (2) for the Galois group of $X^4 + aX + b$ can be distinguished by means of the factorization of the resolvent cubic

$$r(x) = X^3 - 4bX - a^2$$

of $X^4 + aX + b$ as follows:

$$Gal(X^4 + aX + b) \simeq \begin{cases} A_4 \Leftrightarrow r(X) \text{ is irreducible in } \mathbb{Z}[X], \\ V_4 \Leftrightarrow r(X) = (X - t_1)(X - t_2)(X - t_3) \\ \qquad \text{for } t_1, t_2, t_3 \in \mathbb{Z}, \end{cases} \qquad (3)$$

see [3, Theorem 1]. We remark that the discriminant of $r(X)$ is $-4(-4b)^3 - 27(-a^2)^2 = -3^3a^4 + 2^8b^3 = c^2$. The purpose of this note is to show the rather surprising result that the factorization conditions on $r(X)$ in (3) can be replaced by simple arithmetic conditions on the integers a and b. It is convenient to let r denote the largest integer such that

$$r^6 \mid gcd(a^4, 64b^3).$$

We note that $a^2/r^3 \in \mathbb{Z}$, $4b/r^2 \in \mathbb{Z}$ and $c/r^3 \in \mathbb{Z}$. With the above notation, we prove the following result.

Theorem.

$Gal(X^4 + aX + b) \simeq V_4$ if and only if

(a) *$gcd(a^2/r^3, 4b/r^2) = 1$ and either*

(i) $3 \nmid 4b/r^2$

or

(ii) $3 \parallel 4b/r^2$, $3 \nmid a^2/r^3$, $3^3 \mid c/r^3$.

$Gal(X^4 + aX + b) \simeq A_4$ if and only if

(b) *$gcd\,(a^2/r^3, 4b/r^2) \neq 1$*

or

(c) $gcd(a^2/r^3, 4b/r^2) = 1$ *and* $3 \parallel 4b/r^2, \quad 3 \nmid a^2/r^3, \quad 3^2 \parallel c/r^3$.

Before proceeding we state and prove a simple arithmetical lemma that we shall need.

Lemma. *Let x, y and z be nonzero integers such that*

$$-4x^3 - 27y^2 = z^2 \tag{4}$$

and

$$\text{not both of } 3^2 \mid x \text{ and } 3^3 \mid y \text{ hold.} \tag{5}$$

Then exactly one of the following possibilities occurs

$$3 \nmid x, \quad 3 \nmid z, \tag{6}$$

$$3 \parallel x, \quad 3 \nmid y, \quad 3^2 \mid z, \tag{7}$$

$$3^2 \parallel x, \quad 3^2 \parallel y, \quad 3^3 \parallel z. \tag{8}$$

Proof of Lemma. Define nonnegative integers r and s by $3^r \parallel x$ and $3^s \parallel y$. If $r = 1, \ s \geq 1$ or $r \geq 2, \ s = 0$, then $3^3 \parallel -4x^3 - 27y^2 = z^2$, which is impossible. If $r \geq 2, \ s = 1$, then $3^5 \parallel -4x^3 - 27y^2 = z^2$, which is impossible. If $r \geq 3, \ s = 2$, then $3^7 \parallel -4x^3 - 27y^2 = z^2$, which is impossible. The possibility $r \geq 2, \ s \geq 3$ cannot occur by (5). Hence $r = 0$ or $r = 1, \ s = 0$ or $r = 2, \ s = 2$. The first of these is (6), the second (7) and the third (8). □

The proof of our theorem makes use of an explicit formula for the conductor of an abelian cubic field. Let A and B be nonzero integers such that $X^3 + AX + B$ is irreducible in $\mathbb{Z}[X]$ and such that its discriminant $-4A^3 - 27B^2$ is a perfect square, say

$$-4A^3 - 27B^2 = C^2, \tag{9}$$

where $C \in \mathbb{Z}$. The irreducibility of $X^3 + AX + B$ ensures that C is nonzero. Let θ be a root of $X^3 + AX + B$. Then the cubic field $K = \mathbb{Q}(\theta)$

is a normal extension of $\mathbb{Q}$ with Galois group C_3 (the cyclic group of order 3). If R is an integer such that $R^2 \mid A$ and $R^3 \mid B$, then $K = \mathbb{Q}(\theta/R)$ and θ/R is a root of $X^3 + (A/R^2)X + (B/R^3)$ of discriminant $(C/R^3)^2$. Thus we may suppose that the following simplifying assumption

$$R^2 \mid A, \;\; R^3 \mid B \Rightarrow |R| = 1 \tag{10}$$

holds. In view of (9) and (10), the Lemma tells us that exactly one of the following possibilities occurs:

$$3 \nmid A, \;\; 3 \nmid C \text{ or } 3 \parallel A, \;\; 3 \nmid B, \;\; 3^2 \mid C \text{ or } 3^2 \parallel A, \;\; 3^2 \parallel B, \;\; 3^3 \parallel C. \tag{11}$$

We split the possibilities in (11) into two cases as follows:

$$\text{Case 1:} \quad 3 \nmid A, \;\; 3 \nmid C \text{ or } 3 \parallel A, \;\; 3 \nmid B, \;\; 3^3 \mid C, \tag{12}$$

$$\text{Case 2:} \quad 3^2 \parallel A, \;\; 3^2 \parallel B, \;\; 3^3 \parallel C \text{ or } 3 \parallel A, \;\; 3 \nmid B, \;\; 3^2 \parallel C, \tag{13}$$

and define

$$\alpha = 0, \text{ in Case 1,} \tag{14}$$

$$\alpha = 2, \text{ in Case 2.} \tag{15}$$

As K is an abelian field, by the Kronecker-Weber theorem, K is a subfield of some cyclotomic field, that is, $K \subseteq \mathbb{Q}(\zeta_m)$ for some primitive m-th root of unity ζ_m. The smallest such positive integer m is called the *conductor* of K and is denoted by $f(K)$. We will use the following formula for $f(K)$, which is due to Hasse [1]. A simple proof of Hasse's formula can be found in Huard, Spearman and Williams [2].

Proposition. *Under the above assumptions*

$$f(K) = 3^{\alpha} \prod_{\substack{p>3 \\ p \mid A, \; p \mid B}} p,$$

where p runs through primes and α is defined in (14) *and* (15).

We remark that in [2] the formula for $f(K)$ contains the additional restriction that $p \equiv 1 \pmod 3$. However, it is easily seen from (9) and the simplifying assumption (10) that there are no primes $p \equiv 2 \pmod 3$ dividing both A and B.

Proof of Theorem. From (1), we have

$$-4(-4b/r^2)^3 - 27(a^2/r^3)^2 = (c/r^3)^2.$$

Clearly, by the maximality of r, we cannot have both of $3^2 \mid 4b/r^2$ and $3^3 \mid a^2/r^3$ holding. Hence, by the Lemma, exactly one of the following possibilities must occur

$$3 \nmid 4b/r^2 \tag{16}$$

or

$$3 \parallel 4b/r^2, \quad 3 \nmid a^2/r^3, \quad 3^2 \mid c/r^3 \tag{17}$$

or

$$3^2 \parallel 4b/r^2, \quad 3^2 \parallel a^2/r^3, \quad 3^3 \parallel c/r^3. \tag{18}$$

Also by (2), we have

$$Gal(X^4 + aX + b) \simeq A_4 \text{ or } V_4. \tag{19}$$

We suppose first that $Gal(X^4 + aX + b) \simeq V_4$. By (3), $r(X)$ has three linear factors, say

$$X^3 - 4bX - a^2 = (X - u_1)(X - u_2)(X - u_3),$$

where $u_1, u_2, u_3 \in \mathbb{Z}$. Thus

$$r^3X^3 - 4brX - a^2 = (rX - u_1)(rX - u_2)(rX - u_3)$$

and so

$$X^3 - (4b/r^2)X - (a^2/r^3) = (X - (u_1/r))(X - (u_2/r))(X - (u_3/r)).$$

Since $4b/r^2 \in \mathbb{Z}$ and $a^2/r^3 \in \mathbb{Z}$, u_1/r, u_2/r, u_3/r are rational roots of a monic cubic polynomial with integer coefficients. Thus $t_1 = u_1/r$, $t_2 = u_2/r$, $t_3 = u_3/r \in \mathbb{Z}$ and

$$X^3 - (4b/r^2)X - (a^2/r^3) = (X - t_1)(X - t_2)(X - t_3).$$

Hence

$$t_1 + t_2 + t_3 = 0, \quad t_1t_2 + t_2t_3 + t_3t_1 = -4b/r^2, \quad t_1t_2t_3 = a^2/r^3. \tag{20}$$

Suppose there exists a prime p such that $p \mid gcd(a^2/r^3, 4b/r^2)$. Then, from the third equation in (20), we have $p \mid t_1t_2t_3$ so without loss of generality, we may suppose that $p \mid t_1$. Clearly $p \mid t_2t_3$ from the second equation in (20). Then, from the first equation in (20), we deduce that $p \mid t_2$ and $p \mid t_3$. Thus $p^3 \mid a^2/r^3$ and $p^2 \mid 4b/r^2$ so

$$p^6 \mid gcd(a^4/r^6, 64b^3/r^6)$$

contradicting the definition of r. Hence

$$gcd(a^2/r^3, 4b/r^2) = 1. \tag{21}$$

Thus (18) cannot occur. Next, we show that we cannot have

$$3 \parallel 4b/r^2, \quad 3 \nmid a^2/r^3, \quad 3^2 \parallel c/r^3. \tag{22}$$

Suppose (22) holds. Clearly from (20) we see that

$$3 \nmid t_1, t_2, t_3.$$

Since $t_1 + t_2 + t_3 = 0$ we must have $t_1 \equiv t_2 \equiv t_3 \pmod 3$. Now

$$(c/r^3)^2 = (t_1 - t_2)^2(t_1 - t_3)^2(t_2 - t_3)^2 \equiv 0 \pmod{3^6}$$

so that

$$c/r^3 \equiv 0 \pmod{3^3},$$

which is a contradiction. Hence we have shown that $gcd(a^2/r^3, 4b/r^2) = 1$ and either

$$3 \nmid 4b/r^2 \text{ or } 3 \parallel 4b/r^2,\ 3 \nmid a^2/r^3,\ 3^3 \mid c/r^3. \tag{23}$$

Now suppose that (21) and (23) hold. Clearly (21) ensures that the cubic polynomial $X^3 - (4b/r^2)X - (a^2/r^3)$ satisfies the simplifying assumption (10). Moreover,

$$disc(X^3 - (4b/r^2)X - (a^2/r^3)) = (c/r^3)^2$$

so that either $X^3 - (4b/r^2)X - (a^2/r^3)$ is irreducible or has three linear factors in $\mathbb{Z}[X]$. Suppose $X^3 - (4b/r^2)X - (a^2/r^3)$ is irreducible. Let θ be a root of this cubic polynomial. Then $K = \mathbb{Q}(\theta)$ is an abelian cubic field. Hence, by the Proposition, the conductor $f(K)$ of K is given by

$$f(K) = 3^{\alpha} \prod_{\substack{p>3 \\ p \mid 4b/r^2,\ p \mid a^2/r^3}} p,$$

where

$$\alpha = 0, \text{ if } 3 \nmid 4b/r^2 \text{ or } 3 \parallel 4b/r^2,\ 3 \nmid a^2/r^3,\ 3^3 \mid c/r^3, \tag{24}$$

and

$$\alpha = 2, \text{ if } 3^2 \parallel 4b/r^2,\ 3^2 \parallel a^2/r^3 \text{ or } 3 \parallel 4b/r^2,\ 3 \nmid a^2/r^3,\ 3^2 \parallel c/r^3. \tag{25}$$

By (21) and (23) we have $f(K) = 1$, contradicting $[K : \mathbb{Q}] = 3$. Hence $X^3 - (4b/r^2)X - (a^2/r^3)$ has three linear factors in $\mathbb{Z}[X]$. Thus $X^3 - 4bX - a^2$ has three linear factors in $\mathbb{Z}[X]$ and so, by (3), $Gal(X^4 + aX + b) \simeq V_4$. This completes the proof of the first part of the Theorem.

The second part of the Theorem follows from the first part and (16)-(19). □

We conclude with some examples. The authors would like to thank Shawn Godin who found the last example in the table for them.

a	b	c	r	Conditions satisfied	$Gal(X^4 + aX + b)$
8	12	576	4	(c)	A_4
24	36	1728	4	(b)	A_4
24	73	9520	2	(a)(i)	V_4
28	147	28224	2	(b)	A_4
36	63	4320	6	(a)(i)	V_4
56	196	40768	4	(b)	A_4
136	372	62784	4	(c)	A_4
144	468	120960	12	(a)(i)	V_4
168	441	21168	2	(b)	A_4
392	2793	2222640	14	(a)(ii)	V_4

References

[1] H. Hasse, Arithmetische Theorie der kubisch Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Z. 30 (1930), 565-582.

[2] James G. Huard, Blair K. Spearman and Kenneth S. Williams, A short proof of the formula for the conductor of an abelian cubic field, Norske Vid. Selsk. Skr. 2 (1994), 3-7.

[3] Luise-Charlotte Kappe and Bette Warren, An elementary test for the Galois group of a quartic polynomial, Amer. Math. Monthly 96 (1989), 133-137.

[4] D. W. Masser, The discriminants of special equations, Math. Gaz. 50 (1966), 158-160.

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

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6