REDUCIBILITY AND THE GALOIS GROUP OF A PARAMETRIC FAMILY OF QUINTIC POLYNOMIALS

Melisa J. Lavallee, Blair K. Spearman, and Kenneth S. Williams

Abstract. It is shown that $f_t(x) = x^5 + (t^2 - 3125)x - 4(t^2 - 3125)$ ($t \in \mathbb{Q}$) is reducible in $\mathbb{Q}[x]$ if and only if $t = 0$. When $t \neq 0$ it is shown that $\mathrm{Gal}(f_t) \simeq D_5$ or A_5, and necessary and sufficient conditions are given for each possibility.

1. Introduction. Smith [3] has shown that the Galois group of

$$f_t(x) = x^5 + (t^2 - 3125)(x - 4) \qquad (1.1)$$

over $\mathbb{Q}(t)$ is A_5. Let $t \in \mathbb{Q}$. By Hilbert's irreducibility theorem for infinitely many values of $t \in \mathbb{Q}$ the polynomial $f_t(x)$ has Galois group A_5 over $\mathbb{Q}$. The exceptions, which occur when either the polynomial is reducible over $\mathbb{Q}$ or is irreducible over $\mathbb{Q}$ but its Galois group is not A_5, form a "thin" set. In this paper we determine this set for the family (1.1). We set

$$g(u) = \frac{(u^3 - 18u^2 + 8u - 16)(u^3 + 2u^2 + 18u + 4)}{2u^2(u^2 + 4)}, \quad u \in \mathbb{Q} \setminus \{0\}, \qquad (1.2)$$

and prove the following result.

Theorem.

(a) Let $t \in \mathbb{Q}$. Then $f_t(x)$ is reducible in $\mathbb{Q}[x]$ if and only if $t = 0$. If $t = 0$ we have

$$f_0(x) = x^5 - 3125x + 12500 = (x - 5)^2(x^3 + 10x^2 + 75x + 500).$$

(b) If $t \in \mathbb{Q} \setminus \{0\}$ then

$$\mathrm{Gal}(f_t(x)) \simeq D_5 \text{ if } t = g(u) \text{ for some } u \in \mathbb{Q} \setminus \{0\}$$

and

$$\mathrm{Gal}(f_t(x)) \simeq A_5 \text{ if } t \neq g(u) \text{ for any } u \in \mathbb{Q} \setminus \{0\}.$$

Example 1. If $t = -\frac{125}{2}$ then $t = g(1)$ and by the theorem we have

$$\mathrm{Gal}(f_{-125/2}(x)) = \mathrm{Gal}\left(x^5 + \frac{3125}{4}x - 3125\right) \simeq D_5.$$

Example 2. If $t = 1$ then as

$$(x^3 - 18x^2 + 8x - 16)(x^3 + 2x^2 + 18x + 4) - 2x^2(x^2 + 4)$$

is irreducible in $\mathbb{Q}[x]$ there does not exist $u \in \mathbb{Q}$ such that $t = g(u)$ and by the theorem

$$\mathrm{Gal}(f_1(x)) = \mathrm{Gal}(x^5 - 3124x + 12496) \simeq A_5.$$

Example 3. As

$$\lim_{u \to 0^+} g(u) = -\infty, \quad \lim_{u \to +\infty} g(u) = +\infty,$$

and $g(u)$ is strictly increasing for $u > 0$, it is clear that $g(u)$ assumes infinitely many distinct (rational) values for $u \in \mathbb{Q}^+$. Hence, by the theorem, there are infinitely many $t \in \mathbb{Q}$ for which $\mathrm{Gal}(f_t(x)) \simeq D_5$.

Example 4. Let $t = 3n$, $n \in \mathbb{N}$. Suppose there exists $u \in \mathbb{Q} \setminus \{0\}$ with $3n = g(u)$. Then the sextic polynomial

$$(x^3 - 18x^2 + 8x - 16)(x^3 + 2x^2 + 18x + 4) - 6nx^2(x^2 + 4)$$

has a rational root. However,

$$\begin{aligned}&(x^3 - 18x^2 + 8x - 16)(x^3 + 2x^2 + 18x + 4) - 6nx^2(x^2 + 4)\\ &\equiv (x^3 + 2x + 2)(x^3 + 2x^2 + 1) \pmod 3\end{aligned}$$

has no roots $\pmod 3$. Hence, no such u exists and by the theorem there exist infinitely many $t \in \mathbb{Q}$ such that $\mathrm{Gal}(f_t(x)) \simeq A_5$.

We conclude this introduction by recalling a few facts about quintic trinomials, which will be used in the proof of the Theorem in Section 2.

Proposition 1. [2] Let A and B be rational numbers. The discriminant of $x^5 + Ax + B$ is $4^4A^5 + 5^5B^4$.

Proposition 2. [5] Let A and B be rational numbers such that $4^4A^5 + 5^5B^4 > 0$. Then $x^5 + Ax + B$ has exactly one real root.

Proposition 3. [4] Let A and B be rational numbers such that the quintic trinomial $x^5 + Ax + B$ is irreducible in $\mathbb{Q}[x]$. Then $x^5 + Ax + B$ is solvable by radicals if and only if there exist rational numbers $\epsilon(= \pm 1)$, $C(\geq 0)$ and $E(\neq 0)$ such that

$$A = \frac{5E^4(3-4\epsilon C)}{C^2+1}, \quad B = \frac{-4E^5(11\epsilon + 2C)}{C^2+1}.$$

Proposition 4. [4] Let $\epsilon(= \pm 1)$, $C(\geq 0)$ and $E(\neq 0)$ be rational numbers such that the quintic trinomial

$$x^5 + \frac{5E^4(3-4\epsilon C)}{C^2+1}x - \frac{4E^5(11\epsilon + 2C)}{C^2+1}$$

is irreducible in $\mathbb{Q}[x]$. Then the Galois group of $x^5 + Ax + B$ is the dihedral group D_5 of order 10 if and only if $5(C^2+1)$ is a perfect square in $\mathbb{Q}$.

2. Proof of Theorem. (a) If $t = 0$ we have

$$f_0(x) = x^5 - 3125x + 12500 = (x-5)^2(x^3 + 10x^2 + 75x + 500).$$

Now suppose $t \in \mathbb{Q}\backslash\{0\}$. We show that $f_t(x)$ is irreducible in $\mathbb{Q}[x]$. Suppose not. Then $f_t(x)$ has either a rational root or an irreducible quadratic factor.

Suppose first that $f_t(r) = 0$ with $r \in \mathbb{Q}$ so

$$r^5 + (t^2 - 3125)(r-4) = 0. \tag{2.1}$$

Clearly $r \neq 4, 5$. Set

$$x = \frac{-17r - 188}{r-4} \in \mathbb{Q} \tag{2.2}$$

and

$$y = \frac{8(r^2 + 7r + 16t - 60)}{(r-4)(r-5)} \in \mathbb{Q}. \tag{2.3}$$

Then

$$y^2 + xy + y - x^3 - 549x + 2202 = \frac{2^{14}(r^5 + (t^2 - 3125)(r-4))}{(r-4)^3(r-5)^2} = 0. \quad (2.4)$$

This elliptic curve is A4(H) of [1]. Its conductor is 50, its rank is 0 and the order of the torsion subgroup is 1. Thus, there are no pairs $(x, y) \in \mathbb{Q}^2$ satisfying (2.4), contradicting (2.2)–(2.4).

Now suppose $f_t(x)$ has the irreducible quadratic factor $x^2 + ax + b$ $(a, b \in \mathbb{Q}, a^2 - 4b \notin \mathbb{Q}^2)$. As

$$\begin{aligned} &x^5 + (t^2 - 3125)x - 4(t^2 - 3125) \\ &\quad = (x^2 + ax + b)(x^3 - ax^2 + (a^2 - b)x + (2ab - a^3)) \\ &\quad + (a^4 - 3a^2b + b^2 + t^2 - 3125)x + (a^3b - 2ab^2 - 4t^2 + 12500) \end{aligned}$$

we must have

$$a^4 - 3a^2b + b^2 + t^2 - 3125 = a^3b - 2ab^2 - 4t^2 + 12500 = 0. \quad (2.5)$$

Eliminating t^2 from (2.5), we obtain

$$(4 - 2a)b^2 + (a^3 - 12a^2)b + 4a^4 = 0. \quad (2.6)$$

If $a = -10$ then $b = 25$ or $200/3$ so $t^2 = 0$ or $78125/9$, a contradiction. If $a = 0$ then $b = 0$ and $t^2 = 3125$, a contradiction. If $a = 2$ then $b = 8/5$ and $t^2 = 78141/25$, a contradiction. Hence, $a \neq -10, 0, 2$. Solving the quadratic equation (2.6) for b we obtain

$$b = \frac{12a^2 - a^3 \pm a^2\sqrt{a^2 + 8a + 80}}{8 - 4a}. \quad (2.7)$$

As $b \in \mathbb{Q}$ there exists $z \in \mathbb{Q}$ such that

$$a^2 + 8a + 80 = z^2. \quad (2.8)$$

Hence,

$$(z + a + 4)(z - a - 4) = 64.$$

Thus, there exists $k \in \mathbb{Q} \setminus \{0\}$ such that

$$z + a + 4 = k, \quad z - a - 4 = \frac{64}{k}. \tag{2.9}$$

Solving (2.9) for a and z, we obtain

$$a = \frac{k^2 - 8k - 64}{2k}, \quad z = \frac{k^2 + 64}{2k}. \tag{2.10}$$

As $a \neq 2$ we have $k \neq -4, 16$. As $a \neq -10$ we have $k \neq 4, -16$. Hence, $k \neq 0, \pm 4, \pm 16$. Using (2.10) in (2.7) we deduce $b = b_1$ or b_2, where

$$b_1 = \frac{k^4 - 16k^3 - 64k^2 + 1024k + 4096}{8k^2 + 32k}, \tag{2.11}$$

$$b_2 = \frac{-2k^4 + 32k^3 + 128k^2 - 2048k - 8192}{k^3 - 16k^2}. \tag{2.12}$$

First, using the values of a and b_1 in (2.5), we find

$$t^2 = \frac{(k-4)(k^3 - 52k^2 + 768k + 4096)(k^3 + 8k^2 + 88k + 256)^2}{64k^4(k+4)^2}. \tag{2.13}$$

Set

$$x = \frac{2(k+46)}{k-4} \in \mathbb{Q}, \tag{2.14}$$

$$y = \frac{-100k^2(k+4)t}{(k-4)^2(k^3 + 8k^2 + 88k + 256)} - \frac{(3k+88)}{2(k-4)} \in \mathbb{Q}. \tag{2.15}$$

Then

$$\frac{2^2}{5^4}(y^2 + yx + y - x^3 + 76x - 298) =$$

$$\frac{64k^4(k+4)^2t^2 - (k-4)(k^3 - 52k^2 + 768k + 4096)(k^3 + 8k^2 + 88k + 256)^2}{(k-4)^4(k^3 + 8k^2 + 88k + 256)^2}.$$

Thus, by (2.13), we have

$$y^2 + yx + y - x^3 + 76x - 298 = 0. \tag{2.16}$$

The elliptic curve (2.16) is curve A3(G) [1]. The conductor is 50, the rank is 0 and the order of the torison subgroup is 3. There are exactly two finite rational points on this curve, namely, $(2, 11)$ and $(2, -14)$. It is clear from (2.14) that these do not correspond to a rational value of k.

Next, by using the values of a and b_2 in (2.5), we obtain

$$t^2 = \frac{-(k+16)(k^3 - 12k^2 - 52k - 64)(k^3 - 22k^2 + 128k - 1024)^2}{16k^4(k-16)^2}. \tag{2.17}$$

As $k \neq 0$ we can set $k_1 = -64/k \in \mathbb{Q} \setminus \{0\}$. As $k \neq \pm 4, \pm 16$ we have $k_1 \neq \pm 4, \pm 16$. Replacing k by $-64/k_1$ in (2.17), we obtain (2.13) with k replaced by k_1, which we have shown has no rational solutions (t, k_1) with $k_1 \neq 0, \pm 4, \pm 16$.

This completes the proof of part (a) of the theorem.

(b) We now turn to the proof of part (b). Let $t \in \mathbb{Q} \setminus \{0\}$. By Proposition 1 the discriminant of $f_t(x)$ is $2^8 t^2 (t^2 - 3125)^4$. As the discriminant $\in \mathbb{Q}^2$, $\mathrm{Gal}(f_t(x))$ is isomorphic to one of $\mathbb{Z}_5$, D_5 or A_5. It is easy to see by Rolle's Theorem that $f_t(x)$ has at most three real roots (indeed by Proposition 2 it has exactly one real root) so $\mathrm{Gal}(f_t(x)) \not\simeq \mathbb{Z}_5$. Thus, $\mathrm{Gal}(f_t(x)) \simeq D_5$ or A_5.

Suppose first that there exists $u \in \mathbb{Q} \setminus \{0\}$ such that $t = g(u)$, where g is defined in (1.2). Set

$$c = \left| \frac{11u^2 + 8u - 44}{2u^2 - 44u - 8} \right| \in \mathbb{Q}, \tag{2.18}$$

$$e = \left(\mathrm{sgn} \left(\frac{11u^2 + 8u - 44}{2u^2 - 44u - 8} \right) \right) \frac{(u^2 - 2u - 4)}{2u} \in \mathbb{Q}, \tag{2.19}$$

$$\epsilon = -\mathrm{sgn} \left(\frac{11u^2 + 8u - 44}{2u^2 - 44u - 8} \right) = \pm 1. \tag{2.20}$$

We note that $c \geq 0$ and $e \neq 0$. Then

$$t^2 - 3125 = \frac{5e^4(3 - 4\epsilon c)}{c^2 + 1}$$

and

$$-4(t^2-3125)=\frac{-4e^5(11\epsilon+2c)}{c^2+1}$$

so

$$f_t(x)=x^5+\frac{5e^4(3-4\epsilon c)}{c^2+1}x-\frac{4e^5(11\epsilon+2c)}{c^2+1}.$$

Further

$$5(c^2+1)=\left(\frac{25(u^2+4)}{2(u^2-22u-4)}\right)^2\in\mathbb{Q}^2$$

so by Proposition 4, $\mathrm{Gal}(f_t)\simeq D_5$.

Conversely, suppose that $\mathrm{Gal}(f_t(x))\simeq D_5$. Hence, $f_t(x)=0$ is solvable by radicals. Then, by Propostion 3, there exist rationals $c(\geq 0)$, $\epsilon(=\pm 1)$ and $e(\neq 0)$ such that

$$t^2-3125=\frac{5e^4(3-4\epsilon c)}{c^2+1},\quad -4(t^2-3125)=\frac{-4e^5(11\epsilon+2c)}{c^2+1}. \tag{2.21}$$

Eliminating t^2-3125, we obtain

$$c=\frac{15-11\epsilon e}{2(e+10\epsilon)}. \tag{2.22}$$

Then, from (2.22) and the first equation in (2.21), we deduce

$$t^2=\frac{(2e^3+10\epsilon e^2-25e+125\epsilon)^2}{(e^2-2\epsilon e+5)}. \tag{2.23}$$

From (2.23) we see that there exists $z\in\mathbb{Q}\setminus\{0\}$ such that

$$e^2-2\epsilon e+5=z^2.$$

Hence,

$$(z-e+\epsilon)(z+e-\epsilon)=4.$$

Thus, there exists $u \in \mathbb{Q} \setminus \{0\}$ such that

$$z + e - \epsilon = -\epsilon u,$$

$$z - e + \epsilon = -\frac{4\epsilon}{u}.$$

Solving these two equations for e we find

$$e = -\epsilon \left(\frac{u^2 - 2u - 4}{2u} \right). \tag{2.24}$$

From (2.23) and (2.24) we obtain

$$t^2 = \frac{(u^3 - 18u^2 + 8u - 16)^2 (u^3 + 2u^2 + 18u + 4)^2}{4u^4 (u^2 + 4)^2}$$

so that

$$t = \pm g(u).$$

If the plus sign holds then $t = g(u)$ as required. If the minus sign holds then $t = -g(u) = g(-4/u)$ as required.

This completes the proof of the theorem.

Acknowledgement. The second and third authors were supported by grants from the Natural Sciences and Engineering Research Council of Canada.

References

1. J. E. Cremona, *Algorithms for Modular Elliptic Curves,* Second Edition, Cambridge University Press, 1997.

2. N. Jacobson, *Basic Algebra I,* W. H. Freeman and Company, San Francisco, 1974.

3. G. W. Smith, "Some Polynomials Over $\mathbb{Q}(t)$ and Their Galois Groups," *Math. Comp.,* 69 (2000), 775–796.

4. B. K. Spearman and K. S. Williams, "Characterization of Solvable Quintics," *Amer. Math. Monthly,* 101 (1994), 986–992.

5. J. V. Uspensky, *Theory of Equations*, McGraw-Hill Book Company, Inc., New York, Toronto, London, 1948.

Mathematics Subject Classification (2000): 11R21

Melisa J. Lavallee
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B.C.
Canada V1V 1V7

Blair K. Spearman
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, B.C.
Canada V1V 1V7
email: blair.spearman@ubc.ca

Kenneth S. Williams
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
email: kwilliam@connect.carleton.ca