Far East J. Math. Sci. (FJMS) 1(1) (1999), 137-143

DEMOIVRE'S QUINTIC AND A THEOREM OF GALOIS

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

(Received September 19, 1998)

Submitted by K. K. Azad

Abstract

Explicit formulae for the five roots of DeMoivre's quintic polynomial are given in terms of any two of the roots.

If $f(x)$ is an irreducible polynomial of prime degree over the rational field Q, a classical theorem of Galois asserts that $f(x)$ is solvable by radicals if and only if all the roots of $f(x)$ can be expressed as rational functions of any two of them, see for example [2, p. 254]. It is known that DeMoivre's quintic polynomial

$$f(x) = x^5 - 5ax^3 + 5a^2x - b, \qquad a, b \in Q, \tag{1}$$

is solvable by radicals, see for example Borger [1]. In this paper we give explicit formulae for the roots of $f(x)$ in terms of any two of them. We do not need to assume that $f(x)$ is irreducible only that it has nonzero discriminant, that is,

$$d = 5^5\left(4a^5 - b^2\right)^2 \neq 0. \tag{2}$$

We remark that if $d = 0$ then $4a^5 = b^2$ so that $a = u^2$ and $b = 2u^5$ for some $u \in Q$ and the roots of $f(x)$ are

1991 Mathematics Subject Classification: Primary 11R09, 11R16.

Key words and phrases: roots of DeMoivre's quintic.

$$2u,\ \left(\omega+\omega^4\right)u,\ \left(\omega+\omega^4\right)u,\ \left(\omega^2+\omega^3\right)u,\ \left(\omega^2+\omega^3\right)u,$$

where

$$\omega = e^{2\pi i/5}. \tag{3}$$

We denote the roots of $f(x)$ by x_0, x_1, x_2, x_3, x_4 so that the splitting field of $f(x)$ is $F = Q(x_0, x_1, x_2, x_3, x_4)$. As

$$\sqrt{d} = \pm \prod_{0 \le i < j \le 4} \left(x_i - x_j\right) \in F,$$

we see from (2) that

$$\sqrt{5} \in F. \tag{4}$$

We denote the Galois group of $f(x)$ by G_f, the cyclic group of order m by Z_m, and the symmetric group of order $m!$ by S_m. The Frobenius group F_{20} (of order 20) is the group under composition of transformations of the form

$$x \to mx + n, \quad m(\neq 0), \quad n \in GF(5),$$

where $GF(5)$ is the finite field with 5 elements. If we write A for the transformation $x \to x+1$, B for the transformation $x \to 2x+1$, and I for the identity transformation $x \to x$, we find that

$$F_{20} = \langle A, B \rangle, \quad A^5 = B^4 = I, \quad AB = BA^3.$$

The elements of F_{20} are $A^i B^j$ $(i = 0, 1, 2, 3, 4;\ j = 0, 1, 2, 3)$ and their orders are given as follows:

order	elements
1	I
2	$B^2, AB^2, A^2B^2, A^3B^2, A^4B^2$
4	$B, AB, A^2B, A^3B, A^4B, B^3, AB^3, A^2B^3, A^3B^3, A^4B^3$
5	A, A^2, A^3, A^4

Thus F_{20} has five subgroups of order 2 (generated by B^2, AB^2, A^2B^2, A^3B^2 and A^4B^2), five subgroups of order 4 (generated by B, AB, A^2B, A^3B, A^4B), one subgroup of order 5 (generated by A), and one subgroup of order 10 (generated by A and B^2).

With $f(x)$ as in (1) and (2), we prove

Theorem. (a) *$f(x)$ is solvable by radicals.*

(b) *$f(x)$ is either irreducible in $Q[x]$ or $f(x)$ is the product of a linear polynomial and an irreducible quartic polynomial in $Q[x]$.*

(c) *F contains the cyclic quartic field*

$$Q\left(\sqrt{\left(4a^5 - b^2\right)\left(5 + 2\sqrt{5}\right)}\right).$$

(d) *If $f(x)$ is irreducible, then $G_f = F_{20}$.*

(e) *F contains a unique quadratic field, namely $Q\left(\sqrt{5}\right)$.*

(f) *If r_1 and r_2 are any two roots of $f(x)$ then the other three roots are*

$$\frac{(r_1 + r_2)\left(3a - \left(r_1^2 + r_2^2\right)\right)}{r_1r_2 + a}, \quad \frac{r_1^3 - 3ar_1 - ar_2}{r_1r_2 + a}, \quad \frac{r_2^3 - 3ar_2 - ar_1}{r_1r_2 + a}.$$

Proof. (a) Setting $x = y + (a/y)$ we obtain the roots of $f(x)$ as $x_j = \omega^j H + \omega^{-j} K$ $(j = 0, 1, 2, 3, 4)$, where ω is defined in (3),

$$H = \left(\frac{1}{2}\left(b + \sqrt{b^2 - 4a^5}\right)\right)^{1/5}, \quad K = \left(\frac{1}{2}\left(b - \sqrt{b^2 - 4a^5}\right)\right)^{1/5}, \quad HK = a.$$

Thus $f(x)$ is solvable by radicals and G_f is a solvable group.

(c) Let r be a root of $f(x)$. Now

$$f(x)/(x - r) = x^4 + rx^3 + \left(r^2 - 5a\right)x^2 + \left(r^3 - 5ar\right)x + \left(r^4 - 5ar^2 + 5a^2\right),$$

which has the root

$$\frac{1}{4}\left(-r + r\sqrt{5} + \sqrt{\left(4a - r^2\right)\left(10 + 2\sqrt{5}\right)}\right).$$

Appealing to (4) we deduce that

$$\sqrt{\left(4a - r^2\right)\left(10 + 2\sqrt{5}\right)} \in F.$$

Taking $r = x_0, x_1, x_2, x_3, x_4$ (the roots of $f(x)$), we obtain

$$\prod_{j=0}^{4} \sqrt{\left(4a - x_j^2\right)\left(10 + 2\sqrt{5}\right)} \in F,$$

that is

$$\left(10 + 2\sqrt{5}\right)^2 \sqrt{\prod_{j=0}^{4}\left(4a - x_j^2\right)\left(10 + 2\sqrt{5}\right)} \in F.$$

As $\left(10 + 2\sqrt{5}\right)^2 \in Q\left(\sqrt{5}\right) \subseteq F$ we deduce that

$$\sqrt{\prod_{j=0}^{4}\left(4a - x_j^2\right)\left(10 + 2\sqrt{5}\right)} \in F.$$

Now

$$\prod_{j=0}^{4}\left(4a - x_j^2\right) = g(4a),$$

where

$$g(x) = \prod_{j=0}^{4}\left(x - x_j^2\right).$$

A standard calculation gives

$$g(x) = x^5 - 10ax^4 + 35a^2x^3 - 50a^3x^2 + 25a^4x - b^2$$

from which it follows that

$$g(4a) = 4a^5 - b^2.$$

Hence

$$Q\left(\sqrt{\left(4a^5 - b^2\right)\left(10 + 2\sqrt{5}\right)}\right) \subseteq F.$$

Since

$$10 + 2\sqrt{5} = \left(5 + 2\sqrt{5}\right)\left(1 - \sqrt{5}\right)^2$$

we obtain

$$Q\left(\sqrt{\left(4a^5 - b^2\right)\left(5 + 2\sqrt{5}\right)}\right) \subseteq F.$$

It is easily checked that $Q\left(\sqrt{\left(4a^5 - b^2\right)\left(5 + 2\sqrt{5}\right)}\right)$ is a cyclic quartic field, see for example [3, Theorem 3(ii)]. Thus, by Galois theory,

$$4 \text{ divides } \left| G_f \right| \tag{5}$$

and

$$\text{a quotient group of } G_f \text{ is isomorphic to } Z_4. \tag{6}$$

(b) If $f(x)$ is not irreducible in $Q[x]$ then $f(x)$ must have a factorization into distinct irreducible polynomials of $Q[x]$ whose degrees are

(i)	1, 4
(ii)	1, 1, 3
(iii)	1, 1, 1, 2
(iv)	1, 1, 1, 1, 1
(v)	1, 2, 2
or (vi)	2, 3.

In cases (ii), (iii), (vi) $\left| G_f \right| = 1, 2, 3$ or 6 contradicting (5). In case (v) $G_f = Z_2$ or $Z_2 \times Z_2$ contradicting (6). In case (vi) $G_f = Z_2 \times Z_3$ or $Z_2 \times S_3$ or S_3 again contradicting (6). Hence case (i) must hold.

(d) If $f(x)$ is irreducible, then by (a) G_f is a solvable transitive subgroup of S_5 and thus can be identified with a subgroup of F_{20} [2, pp. 253-254]. Hence $\left| G_f \right| \leq \left| F_{20} \right| = 20$. But, by (5), 4 divides $\left| G_f \right|$ and, as $f(x)$ is of degree 5, 5 divides $\left| G_f \right|$ so that $\left| G_f \right| = 20$ and $G_f = F_{20}$.

(e) If $f(x)$ is irreducible, by (d), $G_f = F_{20}$. We have already noted that F_{20} has a unique subgroup of order 10, that is, a unique subgroup of index 2. Hence, by Galois theory, F has a unique quadratic subfield. By (4), $Q(\sqrt{5}) \subseteq F$ so $Q(\sqrt{5})$ must be the unique quadratic field in F.

(f) Let r_1 and r_2 be any two roots of $f(x)$, say, $r_1 = x_j$ and $r_2 = x_k$, where $j, k = 0, 1, 2, 3, 4$; $j \neq k$. Set

$$u = \omega^j H, \quad v = \omega^{-j} K, \quad z = \omega^{k-j},$$

so that u, v are complex numbers and z is a fifth root of unity $\neq 1$ such that

$$r_1 = u + v, \quad r_2 = zu + z^{-1}v, \quad uv = a. \tag{7}$$

The other three roots of $f(x)$ are

$$r_3 = z^2 u + z^{-2} v, \quad r_4 = z^3 u + z^{-3} v, \quad r_5 = z^4 u + z^{-4} v.$$

As $1 + z + z^2 + z^3 + z^4 = 0$, we have

$$\begin{aligned} r_3 &= \left(-1 - z - z^3 - z^4\right)u + \left(-1 - z - z^2 - z^4\right)v \\ &= -(u + v) - \left(1 + z^2 + z^3\right)\left(zu + z^{-1}v\right), \end{aligned}$$

that is

$$r_3 = -r_1 + \left(z + z^4\right)r_2. \tag{8}$$

A similar calculation shows that

$$r_5 = -r_2 + \left(z + z^4\right)r_1. \tag{9}$$

Then, from $r_1 + r_2 + r_3 + r_4 + r_5 = 0$, we obtain

$$r_4 = -\left(z + z^4\right)(r_1 + r_2). \tag{10}$$

It remains to determine $z + z^4$ in terms of r_1 and r_2. From (7) we obtain

$$u = \frac{r_2 - z^4 r_1}{z - z^4}, \quad v = \frac{z r_1 - r_2}{z - z^4}. \tag{11}$$

As $uv = a$, we deduce as $\left(z - z^4\right)^2 = -3 - z - z^4$ that

$$(r_1 r_2 + a)\left(z + z^4\right) = r_1^2 + r_2^2 - 3a. \tag{12}$$

If $r_1 r_2 + a = 0$, then (12) gives $r_1^2 + r_2^2 - 3a = 0$ so that

$$r_1 + r_2 = \varepsilon\sqrt{a}, \qquad r_1 r_2 = -a, \tag{13}$$

where $\varepsilon = \pm 1$. From the first equation in (13) we see that $Q(\sqrt{a}) \subseteq F$. But the only quadratic subfield of F is $Q(\sqrt{5})$ so that $a = t^2$ or $5t^2$ for some positive rational number t. From (13) we deduce that

$$r_1 = \sqrt{a}\left(\varepsilon + \delta\sqrt{5}\right)/2, \qquad r_2 = \sqrt{a}\left(\varepsilon - \delta\sqrt{5}\right)/2,$$

for some $\delta = \pm 1$. This shows that $r_1 \in Q(\sqrt{5})$ and $r_2 \in Q(\sqrt{5})$. Thus $f(x)$ is divisible by a quadratic polynomial in $Q[x]$, contradicting (b). Hence we have shown that $r_1 r_2 + a \neq 0$ so that

$$z + z^4 = \frac{r_1^2 + r_2^2 - 3a}{r_1 r_2 + a}. \tag{14}$$

Using (14) in (8), (9) and (10), we obtain the asserted formulae for r_3, r_4 and r_5.

References

[1] R. L. Borger, On DeMoivre's quintic, Amer. Math. Monthly 15 (1908), 171-174.

[2] N. Jacobson, Basic Algebra I, W. H. Freedman and Company, San Francisco, 1974.

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

Department of Mathematics and Statistics
Okanagan University College
Kelowna, B. C. V1V 1V7
Canada

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6
Canada