# 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

$$
\begin{equation*}
f(x)=x^{5}-5 a x^{3}+5 a^{2} x-b, \quad a, b \in Q \tag{1}
\end{equation*}
$$

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,

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

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

[^0]Key words and phrases: roots of DeMoivre's quintic.

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

where

$$
\begin{equation*}
\omega=e^{2 \pi i / 5} \tag{3}
\end{equation*}
$$

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 $F=Q\left(x_{0}, x_{1}, x_{2}, x_{3}, x_{4}\right)$. As

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

we see from (2) that

$$
\begin{equation*}
\sqrt{5} \in F \tag{4}
\end{equation*}
$$

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

$$
x \rightarrow m x+n, \quad m(\neq 0), \quad n \in G F(5)
$$

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

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

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:

$$
\begin{array}{cl}
\begin{array}{cl}
\text { order } & \text { elements } \\
1 & I \\
2 & B^{2}, A B^{2}, A^{2} B^{2}, A^{3} B^{2}, A^{4} B^{2} \\
4 & B, A B, A^{2} B, A^{3} B, A^{4} B, B^{3}, A B^{3}, A^{2} B^{3}, A^{3} B^{3}, A^{4} B^{3} \\
5 & A, A^{2}, A^{3}, A^{4}
\end{array} .
\end{array}
$$

Thus $F_{20}$ has five subgroups of order 2 (generated by $B^{2}, A B^{2}, A^{2} B^{2}$, $A^{3} B^{2}$ and $A^{4} B^{2}$ ), five subgroups of order 4 (generated by $B, A B, A^{2} B$, $A^{3} B, A^{4} B$ ), 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

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

(d) If $f(x)$ is irreducible, then $G_{f}=F_{20}$.
(e) $F$ contains a unique quadratic field, namely $Q(\sqrt{5})$.
(f) If $r_{1}$ and $r_{2}$ are any two roots of $f(x)$ then the other three roots are

$$
\frac{\left(r_{1}+r_{2}\right)\left(3 a-\left(r_{1}^{2}+r_{2}^{2}\right)\right)}{r_{1} r_{2}+a}, \frac{r_{1}^{3}-3 a r_{1}-a r_{2}}{r_{1} r_{2}+a}, \frac{r_{2}^{3}-3 a r_{2}-a r_{1}}{r_{1} r_{2}+a}
$$

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 $\omega$ is defined in (3),

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

Thus $f(x)$ is solvable by radicals and $G_{f}$ is a solvable group.
(c) Let $r$ be a root of $f(x)$. Now

$$
f(x) /(x-r)=x^{4}+r x^{3}+\left(r^{2}-5 a\right) x^{2}+\left(r^{3}-5 a r\right) x+\left(r^{4}-5 a r^{2}+5 a^{2}\right)
$$

which has the root

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

Appealing to (4) we deduce that

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

Taking $r=x_{0}, x_{1}, x_{2}, x_{3}, x_{4}$ (the roots of $f(x)$ ), we obtain

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

that is

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

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

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

Now

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

where

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

A standard calculation gives

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

from which it follows that

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

Hence

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

Since

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

we obtain

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

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

$$
\begin{equation*}
4 \text { divides }\left|G_{f}\right| \tag{5}
\end{equation*}
$$

and

$$
\begin{equation*}
\text { a quotient group of } G_{f} \text { is isomorphic to } Z_{4} \text {. } \tag{6}
\end{equation*}
$$

(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 $Z_{2} \times Z_{2}$ rontradicting (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, $\boldsymbol{F}$ 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

$$
\begin{equation*}
r_{1}=u+v, \quad r_{2}=z u+z^{-1} v, \quad u v=a . \tag{7}
\end{equation*}
$$

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

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

that is

$$
\begin{equation*}
r_{3}=-r_{1}+\left(z+z^{4}\right) r_{2} \tag{8}
\end{equation*}
$$

A similar calculation shows that

$$
\begin{equation*}
r_{5}=-r_{2}+\left(z+z^{4}\right) r_{1} . \tag{9}
\end{equation*}
$$

Then, from $r_{1}+r_{2}+r_{3}+r_{4}+r_{5}=0$, we obtain

$$
\begin{equation*}
r_{4}=-\left(z+z^{4}\right)\left(r_{1}+r_{2}\right) \tag{10}
\end{equation*}
$$

It remains to determine $z+z^{4}$ in terms of $r_{1}$ and $r_{2}$. From (7) we obtain

$$
\begin{equation*}
u=\frac{r_{2}-z^{4} r_{1}}{z-z^{4}}, \quad v=\frac{z r_{1}-r_{2}}{z-z^{4}} . \tag{11}
\end{equation*}
$$

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

$$
\begin{equation*}
\left(r_{1} r_{2}+a\right)\left(z+z^{4}\right)=r_{1}^{2}+r_{2}^{2}-3 a . \tag{12}
\end{equation*}
$$

If $r_{1} r_{2}+a=0$, then (12) gives $r_{1}^{2}+r_{2}^{2}-3 a=0$ so that

$$
\begin{equation*}
r_{1}+r_{2}=\varepsilon \sqrt{a}, \quad r_{1} r_{2}=-a \tag{13}
\end{equation*}
$$

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 $5 t^{2}$ for some positive rational number $t$. From (13) we deduce that

$$
r_{1}=\sqrt{a}(\varepsilon+\delta \sqrt{5}) / 2, \quad r_{2}=\sqrt{a}(\varepsilon-\delta \sqrt{5}) / 2
$$

for some $\delta= \pm 1$. This shqus 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

$$
\begin{equation*}
z+z^{4}=\frac{r_{1}^{2}+r_{2}^{2}-3 a}{r_{1} r_{2}+a} . \tag{14}
\end{equation*}
$$

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


[^0]:    1991 Mathematics Subject Classification: Primary 11R09, 11R16.

