Indian J. pure appl. Math., **30**(9) : 839-845, September 1999
© Printed in India.

DIHEDRAL QUINTIC POLYNOMIALS AND A THEOREM OF GALOIS

BLAIR K. SPEARMAN*

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

AND

KENNETH S. WILLIAMS†

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

(*Received* 12 *October* 1998; *Accepted* 2 *February* 1999)

Let r_1 and r_2 be any two roots of a monic irreducible quintic polynomial in $Q[X]$ with Galois group D_5. It is shown how to determine the other three roots as rational functions of r_1 and r_2 in accordance with a theorem of Galois.

Key Words : Dihehral; Quintic Polynomials; Theorem of Galois; Rational Functions; Algebraic Number Theory

1. INTRODUCTION

If $f(X) \in Q[X]$ is a solvable irreducible polynomial of prime degree, a theorem of Galois asserts that all the roots of $f(X)$ can be given as rational functions of any two of them. When the degree of $f(X)$ is 2 or 3, this assertion is trivial. However, it is an unsolved problem to determine these rational functions when $f(X)$ is of degree 5 [Bruen *et al.*[1], p. 355]. In this paper, we show how to find these rational functions when $f(X)$ is an irreducible quintic polynomial whose Galois group is D_5, the dihedral group of order 10. When $f(X)$ is a trinomial of the form $X^5 + aX + b$ the rational functions are given explicitly.

* Research supported by a Natural Sciences and Engineering Research Council of Canada grant.
† Research supported by Natural Sciences and Enginnering Research Council of Canada grant A-7233.

2. The Main Result

We prove

Theorem — *Let $f(X) \in Q[X]$ be a monic irreducible quintic polynomial with Galois group D_5. Let r be a root of $f(X)$. Then there exist four polynomials $g_1(X), g_2(X), h_1(X), h_2(X) \in Q[X]$ of degree at most 4 such that*

$$f(X) = (X - r)\,(X^2 + g_1(r)X + h_1(r))\,(X^2 + g_2(r)X + h_2(r))$$

is the factorization of $f(X)$ into irreducible polynomials in $Q(r)[X]$. Let r_1 and r_2 be any two of the roots of $f(X)$. Then the other three roots of $f(X)$ are

$$-\left(\frac{h_1(r_1) - h_2(r_2)}{g_1(r_1) - g_2(r_2)}\right), -\left(\frac{h_1(r_2) - h_2(r_1)}{g_1(r_2) - g_2(r_1)}\right),$$

$$\left(\frac{h_1(r_1) - h_2(r_2)}{g_1(r_1) - g_2(r_2)}\right) + \left(\frac{h_1(r_2) - h_2(r_1)}{g_1(r_2) - g_2(r_1)}\right) - r_1 - r_2 - u, \qquad \text{... (2.1)}$$

where u is the coefficient of X^4 in $f(X)$. The polynomials $g_1(X), g_2(X), h_1(X), h_2(X)$ are unique up to interchange of the pairs $(g_1(X), h_1(X))$ and $(g_2(X), h_2(X))$.

Proof : Let L be the splitting field of $f(X)$. As the Galois group G of $f(X)$ is D_5, we have $[L : Q] = 10$. Let r be any root of $f(X)$. Set $K = Q(r)$, so that K is a subfield of L such that $[K : Q] = 5$ and $[L : K] = 2$. As $f(X)$ is of prime degree and its Galois group $G = D_5$ is solvable, by a theorem of Galois[3], all the roots of $f(X)$ can be given as rational functions of any two of them, in particular as rational functions of r and r', where r' is any other root of $f(X)$. Thus $L = Q(r, r') = K(r')$. We now consider the factorization of $f(X)$ over K. If the factorization of $f(X)$ over K has a linear factor $X - s\ (\neq X - r)$ then $s (\neq r)$ is a root of $f(X)$ in K and so $L = K(s) = K$, contradicting $[L : K] = 2$. If the factorization of $f(X)$ over K has an irreducible quartic factor then $[L : K] = [K(r') : K] = 4$, contradicting $[L : K] = 2$. Hence

$$f(X) = (X - r)m_1(X)m_2(X),$$

where $m_1(X)$ and $m_2(X)$ are monic irreducible quadratic polymonials in $K[X]$. Thus

$$m_i(X) = X^2 + g_i(r)X + h_i(r),\ i = 1,\ 2,$$

where $g_i(X), h_i(X) \in Q[X]$. Since $[Q(r) : Q] = 5$ we can choose $g_i(X)$ and $h_i(X)$ to be of degree at most 4. Since $K[X]$ is a unique factorization domain $m_1(X)$ and $m_2(X)$ are uniquely determined up to order and so the uniqueness of the pairs $(g_1(X), h_1(X))$ and $(g_2(X), h_2(X))$ follows up to order.

Now let r_1 and r_2 be any two of the roots of $f(X)$. We have

$$\frac{f(X)}{X - r_1} = (X^2 + g_1(r_1)X + h_1(r_1))\,(X^2 + g_2(r_1)X + h_2(r_1))$$

and

$$\frac{f(X)}{X-r_2}=(X^2+g_1(r_2)X+h_1(r_2))\,(X^2+g_2(r_2)X+h_2(r_2)).$$

As r_2 is a root of $\frac{f(X)}{X-r_1}$, it is either a root of

(i) $X^2+g_1(r_1)X+h_1(r_1)$ or of (ii) $X^2+g_2(r_1)X+h_2(r_1)$.

Case (i) In this case r_2 is a root of $X^2+g_1(r_1)X+h_1(r_1)$. Let r_3 be the other root. As r_3 is a root of $\frac{f(X)}{X-r_2}$ it is a root of $X^2+g_1(r_2)X+h_1(r_2)$ or a root of $X^2+g_2(r_2)X+h_2(r_2)$. We show that the latter occurs. If not we have

$$r_3^2+g_1(r_1)r_3+h_1(r_1)=0,$$

$$r_3^2+g_1(r_2)r_3+h_1(r_2)=0.$$

Subtracting these equations, we obtain

$$(g_1(r_1)-g_1(r_2))r_3+(h_1(r_1)-h_1(r_2))=0.$$

If $\quad g_1(r_1)-g_1(r_2)=0$ then $h_1(r_1)-h_1(r_2)=0$

and

$$g_1(r_1)=g_1(r_2)\in Q(r_1)\cap Q(r_2)=Q$$

and

$$h_1(r_1)=h_1(r_2)\in Q(r_1)\cap Q(r_2)=Q$$

so that r_3 is a root of a quadratic polynomial in $Q[X]$ contradicting that $[Q(r_3):Q]=5$. Hence, $g_1(r_1)-g_1(r_2)\neq 0$ and so

$$r_3=-\frac{(h_1(r_1)-h_1(r_2))}{(g_1(r_1)-g_1(r_2))}. \qquad \text{... (2.2)}$$

The Galois group of L/Q is D_5. As a permutation group the elements of D_5 of order 2 are (in cycle notation)

$$(12)(35),\ (13)(45),\ (14)(23),\ (15)(24),\ (25)(34). \qquad \text{... (2.3)}$$

Thus there is a unique automorphism of L/Q which interchanges any pair of roots of $f(X)$. In particular there exists an automorphism ϕ such that $\phi(r_1)=r_2$ and $\phi(r_2)=r_1$. Applying ϕ to (2.2) we see that $\phi(r_3)=r_3$. Further from the cycle structure (2.3) we see that $\phi(r_4)=r_5$ and $\phi(r_5)=r_4$, where r_4 and r_5 are the remaining roots of $f(X)$. Applying ϕ to

$$X^2 + g_2(r_1)X + h_2(r_1) = (X - r_4)\,(X - r_5)$$

we deduce that

$$X^2 + g_2(r_2)X + h_2(r_2) = (X - r_5)\,(X - r_4)$$

so that

$$g_2(r_1) = g_2(r_2) \in Q(r_1) \cap Q(r_2) = Q$$

and

$$h_2(r_1) = h_2(r_2) \in Q(r_1) \cap Q(r_2) = Q.$$

Hence r_4 is a root of a quadratic polynomial in $Q[X]$ contradicting that $[Q(r_4) : Q] = 5$. Hence r_3 is a root of $X^2 + g_2(r_2)X + h_2(r_2)$. Thus

$$r_3^2 + g_1(r_1)r_3 + h_1(r_1) = 0,$$

$$r_3^2 + g_2(r_2)r_3 + h_2(r_2) = 0.$$

Subtracting these equations we obtain

$$(g_1(r_1) - g_2(r_2))r_3 + (h_1(r_1) - h_2(r_2)) = 0.$$

Arguing as above we see that $(g_1(r_1) - g_2(r_2) \neq 0$ so that

$$r_3 = -\left(\frac{h_1(r_1) - h_2(r_2)}{g_1(r_1) - g_2(r_2)}\right). \qquad \text{... (2.4)}$$

The roots of $X^2 + g_1(r_2)X + h_1(r_2)$ are r_1 and r_4 or r_1 and r_5. Interchanging r_4 and r_5, if necessary, we may suppose that the roots are r_1 and r_4. Hence $\phi(r_3) = r_4$. Applying ϕ to (2.4) we obtain

$$r_4 = -\left(\frac{h_1(r_2) - h_2(r_1)}{g_1(r_2) - g_2(r_1)}\right).$$

Then from the relation

$$r_1 + r_2 + r_3 + r_4 + r_5 = -u,$$

we obtain r_5.

Case (ii) — In this case r_2 is a root of $X^2 + g_2(r_1)X + h_2(r_1)$. Let r_3 be the other root. Arguing as in Case (i), we obtain that r_3 is a root of $X^2 + g_1(r_2)X + h_1(r_2)$. As in Case (i) we deduce that

$$r_3 = -\left(\frac{h_1(r_2) - h_2(r_1)}{g_1(r_2) - g_2(r_1)}\right). \qquad \ldots (2.5)$$

Applying ϕ to (2.5) we obtain

$$r_4 = -\left(\frac{h_1(r_1) - h_2(r_2)}{g_1(r_1) - g_2(r_2)}\right).$$

Thus the three roots of $f(X)$ different from r_1 and r_2 are

$$\left[-\left(\frac{h_1(r_1) - h_2(r_2)}{g_1(r_1) - g_2(r_2)}\right), -\left(\frac{h_1(r_2) - h_2(r_1)}{g_1(r_2) - g_2(r_1)}\right), \left(\frac{h_1(r_1) - h_2(r_2)}{g_1(r_1) - g_2(r_2)}\right)\right.$$

$$\left. + \left(\frac{h_1(r_2) - h_2(r_1)}{g_1(r_2) - g_2(r_1)}\right) - u - r_1 - r_2\right]$$

in agreement with (2.1).

3. Examples

In order to apply the theorem to a particular polynomial $f(X)$, it is necessary to factor $f(X)$ over an algebraic number field. An algorithm for doing this is described in Cohen's book[2], [pp. 143-145] and is available in software packages such as MAPLE and PARI. We illustrate the computations with some examples.

Example 1 — The quintic $f(X) = X^5 - X^3 - 2X^2 - 2X - 1$ has Galois group D_5. MAPLE determined that

$$f(X) = (X - r)\,(X^2 + (2r^4 - r^3 - 2r^2 - 2r - 2)X + (-r^4 + r^3 + 2r + 1))$$

$$\times\ (X^2 + (-2r^4 + r^3 + 2r^2 + 3r + 2)X + (-r^4 + r^3 + r^2 + r))$$

for any root r of $f(X)$. Hence

$$g_1(X) = 2X^4 - X^3 - 2X^2 - 2X - 2,$$

$$h_1(X) = -X^4 + X^3 + 2X + 1,$$

$$g_2(X) = -2X^4 + X^3 + 2X^2 + 3X + 2$$

and $$h_2(X) = -X^4 + X^3 + X^2 + X.$$

Thus if r_1 and r_2 are any two roots of $f(X)$ then the remaining three roots of $f(X)$ are

$$r_3 = -\left(\frac{(-r_1^4 + r_1^3 + 2r_1 + 1) - (-r_2^4 + r_2^3 + r_2^2 + r_2)}{(2r_1^4 - r_1^3 - 2r_1^2 - 2r_1 - 2) - (-2r_2^4 + r_2^3 + 2r_2^2 + 3r_2 + 2)}\right),$$

$$r_4 = -\left(\frac{(-r_2^4 + r_2^3 + 2r_2 + 1) - (-r_1^4 + r_1^3 + r_1^2 + r_{1)}}{(2r_2^4 - r_2^3 - 2r_2^2 - 2r_2 - 2) - (-2r_1^4 + r_1^3 + 2r_1^2 + 3r_1 + 2)}\right)$$

and

$$r_5 = -r_1 - r_2 - r_3 - r_4.$$

Example 2 — Let $X^5 + aX + b \in Q[X]$ $(a \neq 0, b \neq 0)$ be an irreducible quintic trinomial with Galois group D_5. Then, by [Spearman and Williams[4], pp. 987, 990] there exist rational numbers $c(\geq 0)$, $e(\neq 0)$, $\varepsilon(= \pm 1)$, $t(> 0)$, such that

$$\begin{cases} a = 5e^4\,(3 - 4\varepsilon c)/(c^2 + 1), \\ b = -4e^5(11\varepsilon + 2c)/(c^2 + 1), \\ 5(c^2 + 1) = t^2. \end{cases} \qquad \text{... (3.1)}$$

Moreover, any choice of c, e, ε, t satisfying (3.1) gives an irreducible quintic trinomial with Galois group D_5 except $c = 11/2$, $e \neq 0$, $\varepsilon = -1$, $t = 5/2$ [5]. MAPLE found that

$$g_1(X) = a_0 + a_1X + a_2C^2 + a_3X^3 + a_4X^4,$$

and
$$h_1(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + b_4X^4$$

where

$$a_0 = 20e\varepsilon(4\varepsilon c - 3)t/E,$$

$$a_1 = \frac{1}{2} + (2\varepsilon c + 1)\,(\varepsilon c - 7)t/E,$$

$$a_2 = -\varepsilon(2c^2 + 2\varepsilon c + 13)t/eE,$$

$$a_3 = (3\varepsilon c + 4)\,(2\varepsilon c + 1)t/2e^2E,$$

$$a_4 = -\varepsilon t^3/e^3E,$$

$$b_0 = -5e^2\,(2(4\varepsilon c - 3)^2 + (2\varepsilon c + 11)\,(2\varepsilon c + 1)\,(3\varepsilon c + 4)/t)/E,$$

$$b_1 = -e\varepsilon((265 + 85\varepsilon c + 110c^2) + (55 + 10\varepsilon c)t)/2E,$$

$$b_2 = ((4\varepsilon c - 3)(2c^2 + 2\varepsilon c + 13) + (20\varepsilon c - 15)t)/2E,$$

$$b_3 = -\varepsilon(5(2\varepsilon c + 11)(c^2 + 1) + (2\varepsilon c + 1)(\varepsilon c - 7)t)/2eE$$

and

$$b_4 = (5(4\varepsilon c - 3)(c^2 + 1) + (2c^2 + 2\varepsilon c + 13)t)/2e^2E,$$

where

$$E = 4\varepsilon c^3 - 84c^2 - 37\varepsilon c - 122.$$

The polynomials $g_2(X)$ and $h_2(X)$ are formed from $g_1(X)$ and $h_1(X)$ by changing t to $-t$. Taking $c = 2$, $e = -1$, $\varepsilon = 1, t = 5$, we obtain $f(X) = X^5 - 5X + 12$. The above formulae give

$$\left.\begin{aligned} g_1(X) &= \frac{1}{4}(-X^4 - X^3 - X^2 + 3X + 4), \\ h_1(X) &= \frac{1}{4}(-X^4 - X^3 - X^2 - 5X + 8), \\ g_2(X) &= \frac{1}{4}(X^4 + X^3 + X^2 + X - 4), \\ h_2(X) &= \frac{1}{4}(-2X^3 - 2X - 4). \end{aligned}\right\} \qquad \ldots (3.2)$$

Thus if r_1 and r_2 are any two roots of $X^2 - 5X + 12$ the other three roots are given by (2.1) with g_1, h_1, g_2, h_2 as in (3.2). The roots of $X^5 - 5X + 12$ in radical form are given in [4].

REFERENCES

1. A. A. Bruen, C. U. Jensen and N. Yui, *J. Nt. Theor.* **24** (1986), 305-39.
2. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg New York (1996).
3. F. Sigrist, *Math. Intelligencer* **11** (1989), 53-54.
4. B. K. Spearman and K. S. Williams, *Amer. math. Mon.* **101** (1994), 986-92.
5. B. K. Spearman, L. Y. Spearman and K. S. Williams, *New Zealand J. Math.* **26** (1997), 293-99.