MATHEMATICS OF COMPUTATION
VOLUME 57, NUMBER 195
JULY 1991, PAGES 387-401

SOLVING SOLVABLE QUINTICS

D. S. DUMMIT

ABSTRACT. Let $f(x) = x^5 + px^3 + qx^2 + rx + s$ be an irreducible polynomial of degree 5 with rational coefficients. An explicit resolvent sextic is constructed which has a rational root if and only if $f(x)$ is solvable by radicals (i.e., when its Galois group is contained in the Frobenius group F_{20} of order 20 in the symmetric group S_5). When $f(x)$ is solvable by radicals, formulas for the roots are given in terms of p, q, r, s which produce the roots in a cyclic order.

1. INTRODUCTION

It is well known that an irreducible quintic with coefficients in the rational numbers $\mathbb{Q}$ is solvable by radicals if and only if its Galois group is contained in the Frobenius group F_{20} of order 20, i.e., if and only if the Galois group is isomorphic to F_{20}, to the dihedral group D_{10} of order 10, or to the cyclic group $\mathbb{Z}/5\mathbb{Z}$. (More generally, for any prime p, it is easy to see that a solvable subgroup of the symmetric group S_p whose order is divisible by p is contained in the normalizer of a Sylow p-subgroup of S_p, cf. [1].) The purpose here is to give a criterion for the solvability of such a general quintic in terms of the existence of a rational root of an explicit associated resolvent sextic polynomial, and when this is the case, to give formulas for the roots analogous to Cardano's formulas for the general cubic and quartic polynomials (cf. [1, §14.7], for example) and to determine the precise Galois group. In particular, the roots are produced in an order which is a cyclic permutation of the roots (see the remark before the examples below), which can be useful in other computations (e.g., cf. [3]). We work over the rationals $\mathbb{Q}$, but the results are valid over any field K of characteristic different from 2 and 5. The reader may wish to compare Weber [4] (particularly §§189 and 196).

2. FIXED FIELD OF THE FROBENIUS SUBGROUP

Let x_1, x_2, x_3, x_4, x_5 be the roots of the general quintic polynomial

$$x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5,$$

Received January 19, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12F10.
Research partially sponsored by an NSERC Grant and an NSA Grant.

where the s_i are the elementary symmetric functions in the roots. Let $F_{20} < S_5$ be the Frobenius group of order 20 with generators $(1\,2\,3\,4\,5)$ and $(2\,3\,5\,4)$. Then the stabilizer in S_5 of the element

$$\theta = \theta_1 = x_1^2x_2x_5 + x_1^2x_3x_4 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_5 + x_3^2x_2x_4 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_4 + x_5^2x_2x_3$$

is precisely F_{20}. It follows that θ_1 satisfies a polynomial equation of degree 6 over $\mathbb{Q}(s_1, s_2, s_3, s_4, s_5)$ with conjugates

$$\begin{aligned}
\theta_2 &= (1\,2\,3)\theta_1 \\
&= x_1^2x_2x_5 + x_1^2x_3x_4 + x_2^2x_1x_4 + x_2^2x_3x_5 + x_3^2x_1x_2 \\
&\quad + x_3^2x_4x_5 + x_4^2x_1x_5 + x_4^2x_2x_3 + x_5^2x_1x_3 + x_5^2x_2x_4, \\
\theta_3 &= (1\,3\,2)\theta_1 \\
&= x_1^2x_2x_3 + x_1^2x_4x_5 + x_2^2x_1x_4 + x_2^2x_3x_5 + x_3^2x_1x_5 \\
&\quad + x_3^2x_2x_4 + x_4^2x_1x_3 + x_4^2x_2x_5 + x_5^2x_1x_2 + x_5^2x_3x_4, \\
\theta_4 &= (1\,2)\theta_1 \\
&= x_1^2x_2x_3 + x_1^2x_4x_5 + x_2^2x_1x_5 + x_2^2x_3x_4 + x_3^2x_1x_4 \\
&\quad + x_3^2x_2x_5 + x_4^2x_1x_2 + x_4^2x_3x_5 + x_5^2x_1x_3 + x_5^2x_2x_4, \\
\theta_5 &= (2\,3)\theta_1 \\
&= x_1^2x_2x_4 + x_1^2x_3x_5 + x_2^2x_1x_5 + x_2^2x_3x_4 + x_3^2x_1x_2 \\
&\quad + x_3^2x_4x_5 + x_4^2x_1x_3 + x_4^2x_2x_5 + x_5^2x_1x_4 + x_5^2x_2x_3, \\
\theta_6 &= (1\,3)\theta_1 \\
&= x_1^2x_2x_4 + x_1^2x_3x_5 + x_2^2x_1x_3 + x_2^2x_4x_5 + x_3^2x_1x_4 \\
&\quad + x_3^2x_2x_5 + x_4^2x_1x_5 + x_4^2x_2x_3 + x_5^2x_1x_2 + x_5^2x_3x_4.
\end{aligned}$$

By computing the elementary symmetric functions of the θ_i, which are symmetric polynomials in x_1, x_2, x_3, x_4, x_5, it is a relatively straightforward matter to express these elements in terms of s_1, s_2, s_3, s_4, s_5 to determine the resolvent sextic $f_{20}(x)$ with θ as a root. By making a translation, we may assume $s_1 = 0$, i.e., that our quintic is

$$f(x) = x^5 + px^3 + qx^2 + rx + s, \tag{1}$$

in which case $f_{20}(x)$ is

$$
\begin{aligned}
f_{20}(x) = {} & x^6 + 8rx^5 + (2pq^2 - 6p^2r + 40r^2 - 50qs)x^4 \\
& + (-2q^4 + 21pq^2r - 40p^2r^2 + 160r^3 - 15p^2qs - 400qrs + 125ps^2)x^3 \\
& + (p^2q^4 - 6p^3q^2r - 8q^4r + 9p^4r^2 + 76pq^2r^2 - 136p^2r^3 + 400r^4 \\
& \qquad - 50pq^3s + 90p^2qrs - 1400qr^2s + 625q^2s^2 + 500prs^2)x^2 \\
& + (-2pq^6 + 19p^2q^4r - 51p^3q^2r^2 + 3q^4r^2 + 32p^4r^3 + 76pq^2r^3 \\
& \quad - 256p^2r^4 + 512r^5 - 31p^3q^3s - 58q^5s + 117p^4qrs + 105pq^3rs \\
& \quad + 260p^2qr^2s - 2400qr^3s - 108p^5s^2 - 325p^2q^2s^2 + 525p^3rs^2 \\
& \qquad + 2750q^2rs^2 - 500pr^2s^2 + 625pqs^3 - 3125s^4)x \qquad (2) \\
& + (q^8 - 13pq^6r + p^5q^2r^2 + 65p^2q^4r^2 - 4p^6r^3 - 128p^3q^2r^3 + 17q^4r^3 \\
& \quad + 48p^4r^4 - 16pq^2r^4 - 192p^2r^5 + 256r^6 - 4p^5q^3s - 12p^2q^5s \\
& \quad + 18p^6qrs + 12p^3q^3rs - 124q^5rs + 196p^4qr^2s + 590pq^3r^2s \\
& \quad - 160p^2qr^3s - 1600qr^4s - 27p^7s^2 - 150p^4q^2s^2 - 125pq^4s^2 \\
& \quad - 99p^5rs^2 - 725p^2q^2rs^2 + 1200p^3r^2s^2 + 3250q^2r^2s^2 \\
& \qquad - 2000pr^3s^2 - 1250pqrs^3 + 3125p^2s^4 - 9375rs^4).
\end{aligned}
$$

For the particular case when $f(x) = x^5 + ax + b$, this polynomial is simply

$$
\begin{aligned}
f_{20}(x) = {} & x^6 + 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^2 \\
& + (512a^5 - 3125b^4)x + (256a^6 - 9375ab^4).
\end{aligned} \qquad (2')
$$

Theorem 1. *The irreducible quintic* $f(x) = x^5 + px^3 + qx^2 + rx + s \in \mathbb{Q}[x]$ *is solvable by radicals if and only if the polynomial* $f_{20}(x)$ *in* (2) *has a rational root. If this is the case, the sextic* $f_{20}(x)$ *factors into the product of a linear polynomial and an irreducible quintic.*

Proof. The polynomial $f(x)$ is solvable if and only if the Galois group of $f(x)$, considered as a permutation group on the roots, is contained in the normalizer of some Sylow 5-subgroup in S_5. The normalizers of the six Sylow 5-subgroups in S_5 are precisely the conjugates of F_{20} above, hence are the stabilizers of the elements $\theta_1, \ldots, \theta_6$. It follows that $f(x)$ is solvable by radicals if and only if one of the θ_i is rational. By renumbering the roots as $x_1, \ldots, x_5$, we may assume $\theta = \theta_1$ is rational, so that the Galois group of $f(x)$ is contained in the specific group F_{20} above. Since $f(x)$ is irreducible, the order of its Galois group is divisible by 5. It follows that the 5-cycle (1 2 3 4 5) survives any specialization (this element generates the unique subgroup of order 5 in this F_{20}). Because this element is transitive on $\theta_2, \ldots, \theta_6$ (in fact cycling them as $\theta_2, \theta_6, \theta_3, \theta_4, \theta_5$), the remaining roots θ_i are roots of an irreducible quintic over $\mathbb{Q}(\theta) = \mathbb{Q}$. □

Theorem 1 provides an easy criterion for the solvability of a general quintic polynomial (see the examples below). We now consider the question of solving for the roots of $f(x)$ when $f(x)$ is solvable, i.e., solving for the roots $x_1, \dots, x_5$ in terms of radicals over the field $\mathbb{Q}(s_1, \dots, s_5, \theta)$. We suppose the rational root of $f_{20}(x)$ is the root θ above, so the Galois group of $f(x)$ is contained in the version of F_{20} above. This determines an ordering of the roots x_i up to a permutation in F_{20}.

Let ζ be a fixed primitive 5th root of unity, and define the function fields $k = \mathbb{Q}(s_1, \dots, s_5)$, $K = k(\theta)$, and $F = \mathbb{Q}(x_1, \dots, x_5)$, so that $F(\zeta)/K$ is a Galois extension with $F_{20} \times (\mathbb{Z}/5\mathbb{Z})^\times$ as Galois group. Define the automorphisms σ, τ, and ω of F to be $\sigma = (1\,2\,3\,4\,5)$ (trivial on constants), $\tau = (2\,3\,5\,4)$ (trivial on constants), $\omega: \zeta \mapsto \zeta^3$ (trivial on $x_1, \dots, x_5$).

Let $\Delta = \prod_{i<j}(x_i - x_j)$ denote the fixed square root of the discriminant $D = \Delta^2$ of $f(x)$. Note that for a solvable quintic, the discriminant D is always positive: if the Galois group is dihedral or cyclic, then the Galois group is contained in A_5, so that D is actually a square; if the Galois group is the Frobenius group, then $\sqrt{D}$ generates a quadratic extension which is a subfield of a cyclic quartic extension, so again $D > 0$ (in fact, D is then the sum of two squares).

Define the usual Lagrange resolvents of the root x_1:

$$\begin{aligned}
(x_1, 1) &= x_1 + x_2 + x_3 + x_4 + x_5 = 0, \\
r_1 &= (x_1, \zeta) = x_1 + x_2\zeta + x_3\zeta^2 + x_4\zeta^3 + x_5\zeta^4, \\
r_2 &= (x_1, \zeta^2) = x_1 + x_2\zeta^2 + x_3\zeta^4 + x_4\zeta + x_5\zeta^3, \\
r_3 &= (x_1, \zeta^3) = x_1 + x_2\zeta^3 + x_3\zeta + x_4\zeta^4 + x_5\zeta^2, \\
r_4 &= (x_1, \zeta^4) = x_1 + x_2\zeta^4 + x_3\zeta^3 + x_4\zeta^2 + x_5\zeta,
\end{aligned}$$

so that

$$\begin{aligned}
x_1 &= (r_1 + r_2 + r_3 + r_4)/5, \\
x_2 &= (\zeta^4 r_1 + \zeta^3 r_2 + \zeta^2 r_3 + \zeta r_4)/5, \\
x_3 &= (\zeta^3 r_1 + \zeta r_2 + \zeta^4 r_3 + \zeta^2 r_4)/5, \\
x_4 &= (\zeta^2 r_1 + \zeta^4 r_2 + \zeta r_3 + \zeta^3 r_4)/5, \\
x_5 &= (\zeta r_1 + \zeta^2 r_2 + \zeta^3 r_3 + \zeta^4 r_4)/5.
\end{aligned} \tag{3}$$

Write

$$(x_1, z) = x_1 + x_2 z + x_3 z^2 + x_4 z^3 + x_5 z^4$$

with an indeterminate z (so $z = \zeta$ gives the Lagrange resolvent r_1). Expanding $(x_1, z)^5$ gives

$$R_1 = r_1^5 = (x_1, \zeta)^5 = l_0 + l_1\zeta + l_2\zeta^2 + l_3\zeta^3 + l_4\zeta^4, \tag{4.1}$$

where l_0 by definition is the sum of the terms in $(x_1, z)^5$ involving powers z^i of z with i divisible by 5, l_1 is the sum of the terms with $i \equiv 1 \bmod 5$, and so forth. Explicitly,

$$
\begin{aligned}
l_0 &= 30x_2x_4^2x_5^2 + 20x_1x_4x_5^3 + 20x_1^3x_2x_5 + 20x_2x_3x_5^3 + x_2^5 + x_5^5 \\
&\quad + x_1^5 + x_3^5 + x_4^5 + 20x_1^3x_3x_4 + 30x_1^2x_2^2x_4 + 30x_1^2x_2x_3^2 + 20x_1x_2^3x_3 \\
&\quad + 30x_1^2x_3x_5^2 + 30x_1^2x_4^2x_5 + 30x_2^2x_3^2x_5 + 30x_2^2x_3x_4^2 \\
&\quad + 20x_2^3x_4x_5 + 20x_2x_3^3x_4 + 20x_1x_2x_4^3 + 30x_1x_2^2x_5^2 + 30x_1x_3^2x_4^2 \\
&\quad + 20x_1x_3^3x_5 + 120x_1x_2x_3x_4x_5 + 30x_3^2x_4x_5^2 + 20x_3x_4^3x_5, \qquad (5.0) \\
l_1 &= 20x_1x_3x_4^3 + 30x_1^2x_4x_5^2 + 5x_1^4x_2 + 10x_1^3x_4^2 + 10x_1^2x_3^3 \\
&\quad + 5x_2^4x_3 + 10x_2^2x_4^3 + 5x_3^4x_4 + 10x_2^3x_5^2 + 10x_3^2x_5^3 + 5x_4^4x_5 \\
&\quad + 5x_1x_5^4 + 20x_1^3x_3x_5 + 30x_1^2x_2^2x_5 + 30x_1x_2^2x_3^2 + 20x_1x_2^3x_4 \\
&\quad + 30x_2x_3^2x_4^2 + 20x_2x_3^3x_5 + 20x_2x_4x_5^3 + 30x_3x_4^2x_5^2 + 60x_1^2x_2x_3x_4 \\
&\quad + 60x_2^2x_3x_4x_5 + 60x_1x_2x_4^2x_5 + 60x_1x_2x_3x_5^2 + 60x_1x_3^2x_4x_5, \qquad (5.1) \\
l_2 &= 20x_1^3x_4x_5 + 10x_1^3x_2^2 + 5x_1^4x_3 + 10x_2^3x_3^2 + 5x_2^4x_4 + 10x_1^2x_5^3 \\
&\quad + 10x_3^3x_4^2 + 5x_1x_4^4 + 5x_3^4x_5 + 5x_2x_5^4 + 10x_4^3x_5^2 + 30x_1^2x_2x_4^2 \\
&\quad + 30x_1^2x_3^2x_4 + 20x_1x_2x_3^3 + 20x_1x_2^3x_5 + 30x_2^2x_3x_5^2 \\
&\quad + 20x_2x_3x_4^3 + 30x_2^2x_4^2x_5 + 30x_1x_3^2x_5^2 + 60x_1^2x_2x_3x_5 + 60x_1x_2^2x_3x_4 \\
&\quad + 60x_1x_2x_4x_5^2 + 60x_2x_3^2x_4x_5 + 60x_1x_3x_4^2x_5 + 20x_3x_4x_5^3, \qquad (5.2) \\
l_3 &= 20x_2^3x_3x_4 + 20x_3^3x_4x_5 + 5x_1^4x_4 + 10x_1^2x_2^3 + 10x_1^3x_5^2 + 10x_2^2x_3^3 \\
&\quad + 5x_2^4x_5 + 5x_1x_3^4 + 5x_2x_4^4 + 10x_3^2x_4^3 + 5x_3x_5^4 + 10x_4^2x_5^3 \\
&\quad + 20x_1^3x_2x_3 + 30x_1^2x_3x_4^2 + 30x_1^2x_3^2x_5 + 30x_1x_2^2x_4^2 + 30x_2x_3^2x_5^2 \\
&\quad + 30x_2^2x_4x_5^2 + 20x_1x_2x_5^3 + 20x_1x_4^3x_5 + 60x_1^2x_2x_4x_5 \\
&\quad + 60x_1x_2x_3^2x_4 + 60x_1x_2^2x_3x_5 + 60x_2x_3x_4^2x_5 + 60x_1x_3x_4x_5^2, \qquad (5.3) \\
l_4 &= 30x_1^2x_2x_5^2 + 5x_1^4x_5 + 10x_1^3x_3^2 + 5x_1x_2^4 + 5x_2x_3^4 + 10x_1^2x_4^3 \\
&\quad + 10x_2^3x_4^2 + 10x_2^2x_5^3 + 5x_3x_4^4 + 10x_3^3x_5^2 + 5x_4x_5^4 + 20x_1^3x_2x_4 \\
&\quad + 30x_1^2x_2^2x_3 + 30x_2^2x_3^2x_4 + 20x_2^3x_3x_5 + 20x_1x_3^3x_4 + 20x_2x_4^3x_5 \\
&\quad + 30x_3^2x_4^2x_5 + 20x_1x_3x_5^3 + 30x_1x_4^2x_5^2 + 60x_1^2x_3x_4x_5 \\
&\quad + 60x_1x_2^2x_4x_5 + 60x_1x_2x_3x_4^2 + 60x_1x_2x_3^2x_5 + 60x_2x_3x_4x_5^2. \qquad (5.4)
\end{aligned}
$$

(Note also that setting $z = 1$ shows that

$$l_0 + l_1 + l_2 + l_3 + l_4 = (x_1 + x_2 + x_3 + x_4 + x_5)^5.$$

In particular, if $s_1 = 0$, we have $l_0 = -l_1 - l_2 - l_3 - l_4$.)

Similarly we have

$$R_2 = r_2^5 = l_0 + l_3\zeta + l_1\zeta^2 + l_4\zeta^3 + l_2\zeta^4, \tag{4.2}$$

$$R_3 = r_3^5 = l_0 + l_2\zeta + l_4\zeta^2 + l_1\zeta^3 + l_3\zeta^4, \tag{4.3}$$

$$R_4 = r_4^5 = l_0 + l_4\zeta + l_3\zeta^2 + l_2\zeta^3 + l_1\zeta^4. \tag{4.4}$$

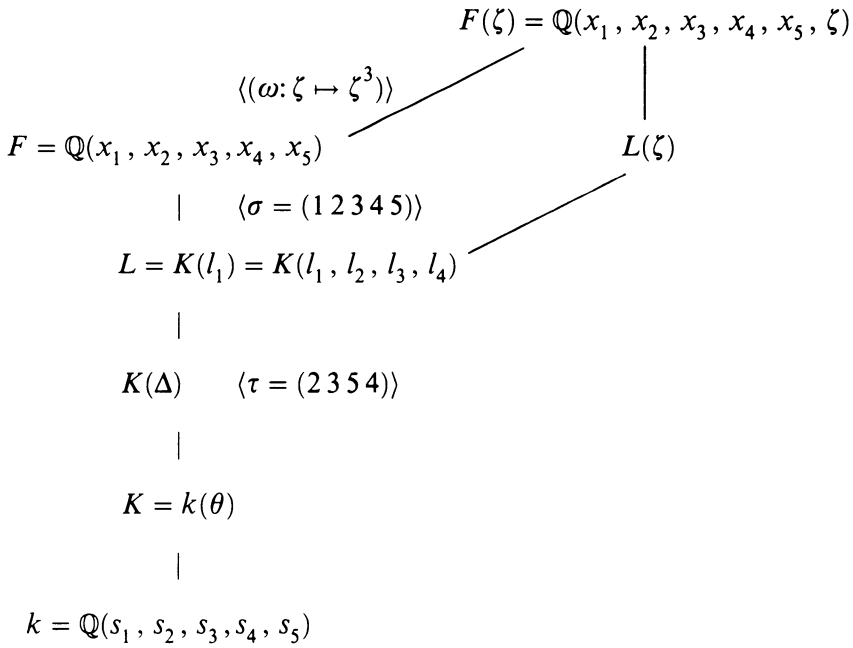
The Galois action over K on these elements is the following: The elements l_0, l_1, l_2, l_3, l_4 are contained in the field F and are fixed by σ;

$$\tau l_0 = l_0, \quad \tau l_1 = l_2, \quad \tau l_2 = l_4, \quad \tau l_3 = l_1, \quad \tau l_4 = l_3,$$

and the action on the Lagrange resolvents is given by

$$\begin{aligned} \sigma r_1 &= \zeta^4 r_1, & \tau r_1 &= \omega r_1 = r_3, \\ \sigma r_2 &= \zeta^3 r_2, & \tau r_2 &= \omega r_2 = r_1, \\ \sigma r_3 &= \zeta^2 r_3, & \tau r_3 &= \omega r_3 = r_4, \\ \sigma r_4 &= \zeta^1 r_4, & \tau r_4 &= \omega r_4 = r_2. \end{aligned} \tag{6}$$

It follows that $l_0 \in K$ and that l_1, l_2, l_3, l_4 are the roots of a quartic polynomial over K, and the field $L = K(l_1) = K(l_1, l_2, l_3, l_4)$ is a cyclic extension of K of degree 4 (with Galois group generated by the restriction of $\tau = (2\,3\,5\,4)$. The unique quadratic subfield of L over K is the field $K(\Delta)$. The field diagram is the following:



Since the Galois group of L/K is cyclic of degree 4, it follows that l_1, l_2, l_3, l_4 are the roots of a quartic over K which factors over $K(\Delta)$ into the product of

two conjugate quadratics:

$$(7) \qquad [x^2 + (T_1 + T_2\Delta)x + (T_3 + T_4\Delta)][x^2 + (T_1 - T_2\Delta)x + (T_3 - T_4\Delta)]$$

with $T_1, T_2, T_3, T_4 \in K$. The roots of one of these two quadratic factors are $\{l_1, l_4\ (= \tau^2 l_1)\}$, and the roots of the other are the conjugates $\{l_2\ (= \tau l_1), l_3\ (= \tau^3 l_1)\}$ for the specific l_i defined in equations (5.1)–(5.4). We may fix the order of the factors and determine the coefficients T_i explicitly by assuming that the roots of the first factor in (7) are $\{l_1, l_4\}$. Then

$$l_1 + l_4 = -T_1 - T_2\Delta, \qquad l_2 + l_3 = -T_1 + T_2\Delta,$$

$$l_1 l_4 = T_3 + T_4\Delta, \qquad l_2 l_3 = T_3 - T_4\Delta,$$

which defines the T_i as explicit rational functions in $x_1, \ldots, x_5$. Writing these elements as linear combinations of $1, \theta, \theta^2, \ldots, \theta^5$ with symmetric functions as coefficients would be relatively more straightforward if $\mathbb{Z}[s_1, \ldots, s_5][\theta]$ were integrally closed in K, but unfortunately this is not the case. We proceed as follows. In a relation of the form

$$P = \alpha_0 + \alpha_1\theta + \alpha_2\theta^2 + \alpha_3\theta^3 + \alpha_4\theta^4 + \alpha_5\theta^5,$$

where the α_i are rational symmetric functions, if we apply the automorphisms $(1\,2\,3)$ and $(1\,2)$ (which generate a complement to F_{20} in S_5 and so give the automorphisms of $K = k(\theta)$), we obtain the system of equations

$$\begin{aligned}
P &= \alpha_0 + \alpha_1\theta_1 + \alpha_2\theta_1^2 + \alpha_3\theta_1^3 + \alpha_4\theta_1^4 + \alpha_5\theta_1^5,\\
(1\,2\,3)P &= \alpha_0 + \alpha_1\theta_2 + \alpha_2\theta_2^2 + \alpha_3\theta_2^3 + \alpha_4\theta_2^4 + \alpha_5\theta_2^5,\\
(1\,3\,2)P &= \alpha_0 + \alpha_1\theta_3 + \alpha_2\theta_3^2 + \alpha_3\theta_3^3 + \alpha_4\theta_3^4 + \alpha_5\theta_3^5,\\
(1\,2)P &= \alpha_0 + \alpha_1\theta_4 + \alpha_2\theta_4^2 + \alpha_3\theta_4^3 + \alpha_4\theta_4^4 + \alpha_5\theta_4^5,\\
(2\,3)P &= \alpha_0 + \alpha_1\theta_5 + \alpha_2\theta_5^2 + \alpha_3\theta_5^3 + \alpha_4\theta_5^4 + \alpha_5\theta_5^5,\\
(1\,3)P &= \alpha_0 + \alpha_1\theta_6 + \alpha_2\theta_6^2 + \alpha_3\theta_6^3 + \alpha_4\theta_6^4 + \alpha_5\theta_6^5,
\end{aligned}$$

from which we may solve for the α_i using Cramer's rule. The denominator appearing in Cramer's rule is the Vandermonde determinant $-\prod_{i<j}(\theta_i - \theta_j)$, and it is not difficult to see that this is $\Delta^3 F$, where F is a symmetric polynomial. In particular, if P is a polynomial, this gives a bound for the denominator necessary for the rational symmetric functions α_i (since then the numerator in Cramer's rule is a polynomial).

3. Computational matters

As a practical matter, the computation of the relevant symmetric functions is done by first computing the weights and degrees of the polynomial in the numerator of Cramer's rule for each α_i, then determining which symmetric

monomials in $s_1, \ldots, s_5$ are involved (for example, there are 258 monomials of weight 50 involved in the computation of the numerator of α_0 for T_4). The problem then is to determine explicitly the coefficients involved in writing a given polynomial (expressed as a determinant) as a linear combination of these monomials. Because of the high weights involved, it is impractical to simply expand the appropriate polynomials in $x_1, \ldots, x_5$ and apply the usual lexicographic algorithm. It is also impractical to substitute simple values for $x_1, \ldots, x_5$ into these polynomial identities and then solve the resulting linear system of equations, since a sufficiently independent choice of variables to produce a determined system of equations produces relatively large (viz. 258×258) matrices with large entries (viz. $\sim 10^{300}$).

The computations here were performed first by solving the equation $x^5 - s_1x^4 + s_2x^3 - s_3x^2 + s_4x - s_5$ for the roots $x_1, \ldots, x_5$ to sufficiently high precision (typically ~ 100 digits) for a given set of values of $s_1 = 0, s_2, \ldots, s_5$ (for example, with $s_2 = s_5 = 0$ and sufficiently independent integer values for s_3, s_4), then computing the determinant involved in Cramer's rule and rounding to achieve a system of equations with relatively small ($\sim 10^{20}$) integer coefficients. By judicious choice, the number of equations is manageable (involving only the monomials without s_1, s_2, and s_5, for example). When all such "easy" coefficients were determined, a p-adic approach was used: equation (1) was solved for $x_1, \ldots, x_5$ to sufficiently high precision with $s_1 = 0$, s_2 (say) equal to a prime p, and s_3, s_4, s_5 sufficiently independent integer values. The determinant was calculated and the value of the known monomials subtracted, giving a value V which should be an integer (which was rounded after checking). If n is the smallest power of s_2 appearing in the remaining monomials to be determined, then V/p^n should be an integer (providing another useful check on the computations), namely the sum of the values corresponding to the remaining monomials when the exponent of s_2 has been reduced by n. In particular, $V/p^n \bmod p$ corresponds to those remaining terms whose original exponent of s_2 was precisely n. Solving such systems, we can determine the coefficients $\bmod p$ for the terms involving first s_2^0, then for the terms involving s_2^1, etc., which reduces both the number of equations involved and also the size of the coefficients (namely, $< p$) of the system considerably. Performing this p-adic computation for several primes p then determines the coefficients. In practice, these terms were determined modulo the first eight primes greater than 1000, and the coefficients determined modulo the product of the first and the last seven of these values to be sure the values were in agreement. Once the coefficients were determined, they were checked.

4. Ordering the resolvents

If we write

$$l_0 = (a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4 + a_5\theta^5)/F \tag{8.0}$$

and

$$T_1 = (b_{10} + b_{11}\theta + b_{12}\theta^2 + b_{13}\theta^3 b_{14}\theta^4 + b_{15}\theta^5)/(2F), \tag{8.1}$$

$$T_2 = (b_{20} + b_{21}\theta + b_{22}\theta^2 + b_{23}\theta^3 + b_{24}\theta^4 + b_{25}\theta^5)/(2DF), \tag{8.2}$$

$$T_3 = (b_{30} + b_{31}\theta + b_{32}\theta^2 + b_{33}\theta^3 + b_{34}\theta^4 + b_{35}\theta^5)/(2F), \tag{8.3}$$

$$T_4 = (b_{40} + b_{41}\theta + b_{42}\theta^2 + b_{43}\theta^3 + b_{44}\theta^4 + b_{45}\theta^5)/(2DF), \tag{8.4}$$

the values are given explicitly for the general polynomial $f(x) = x^5 + px^3 + qx^2 + rx + s$ in the Appendix (on microfiche) in terms of p, q, r, s. For the particular case when $f(x) = x^5 + ax + b$, these values are

$$T_1 = (512a^5 - 15625b^4 + 768a^4\theta + 416a^3\theta^2 + 112a^2\theta^3 + 24a\theta^4 + 4\theta^5)/(50b^3), \tag{8.1'}$$

$$T_2 = (3840a^5 - 78125b^4 + 4480a^4\theta + 2480a^3\theta^2 + 760a^2\theta^3 + 140a\theta^4 + 30\theta^5)/(512a^5 b + 6250b^5), \tag{8.2'}$$

$$T_3 = (-18880a^5 + 781250b^4 - 34240a^4\theta - 21260a^3\theta^2 - 5980a^2\theta^3 - 1255a\theta^4 - 240\theta^5)/(2b^2), \tag{8.3'}$$

$$T_4 = (68800a^5 + 25000a^4\theta + 11500a^3\theta^2 + 3250a^2\theta^3 + 375a\theta^4 + 100\theta^5)/(512a^5 + 6250b^4). \tag{8.4'}$$

If we compute these expressions in terms of our given rational θ, and choose a specific Δ as our square root of D, then the roots of the quadratics in (7) give us $\{l_1, l_4\}$ and $\{l_2, l_3\}$, up to a permutation of the two pairs. This is not sufficient to solve for the resolvents R_1, R_2, R_3, R_4, however, since for example if our choice of the roots in fact corresponds to $\{l_1, l_3, l_2, l_4\}$, then we do not simply obtain a permutation of the R_i (this permutation is not obtained by an element of F_{20}). This difficulty is overcome by introducing an ordering condition. For this, observe that $(l_1 - l_4)(l_2 - l_3) = \mathscr{O}\Delta$ for some element $\mathscr{O} \in K$. Computing this element as before, we write

$$\mathscr{O} = (o_0 + o_1\theta + o_2\theta^2 + o_3\theta^3 + o_4\theta^4 + o_5\theta^5)/(DF), \tag{9}$$

where again the values of $o_1, \ldots, o_5$ for general $f(x)$ are given in the Appendix. For the special case of $f(x) = x^5 + ax + b$ we have

$$\mathscr{O} = (-1036800a^5 + 48828125b^4 - 2280000a^4\theta - 1291500a^3\theta^2 - 399500a^2\theta^3 - 76625a\theta^4 - 16100\theta^5)/(256a^5 + 3125b^4). \tag{9'}$$

For any specific quintic $f(x)$, choose a square root Δ' of the discriminant D, then define the roots of the first quadratic in (7) to be l_1' and l_4', and the

roots of the second quadratic to be l_2' and l_3', ordered so that $(l_1'-l_4')(l_2'-l_3') = \mathscr{O}\Delta'$. If our choice of square root Δ' is the same as that corresponding to Δ determined by the ordering of the roots above, then our choice of l_1', l_2', l_3', l_4' is either l_1, l_2, l_3, l_4 or l_4, l_3, l_2, l_1. If our choice of square root Δ' corresponds to $-\Delta$, then our choice of l_1', l_2', l_3', l_4' is either l_2, l_4, l_1, l_3 or l_3, l_1, l_4, l_2. The corresponding resolvents computed in (4.1)–(4.4) are then simply permuted (namely, (R_1, R_2, R_3, R_4), (R_4, R_3, R_2, R_1), (R_3, R_1, R_4, R_2), (R_2, R_4, R_1, R_3), respectively), which will simply permute the order of the roots x_i in (3), as we shall see.

It remains to consider the choice of the fifth roots of the R_i to obtain the resolvents r_i. We now show that, given $R_1 = r_1^5$, each of the five possible choices for r_1 uniquely defines the choices for r_2, r_3, r_4, hence uniquely defines the five roots of the quintic.

Consider the expressions r_1r_4 and r_2r_3, which by the explicit Galois actions above are fixed by σ, $\tau\omega^{-1}$, and τ^2, hence are elements of the corresponding fixed field $K(\Delta\sqrt{5})$.

As mentioned above, the discriminant D for any solvable quintic is a positive rational number. It follows that under any specialization, the elements r_1r_4 and r_2r_3 are elements of the field $\mathbb{Q}(\sqrt{5D})$. Since the r_i are uniquely defined up to multiplication by a fifth root of unity, this uniquely determines r_4 given r_1, and r_3 given r_2. It remains to see how r_2 is determined by r_1.

Consider now the elements $r_1r_2^2, r_3r_1^2, r_4r_3^2, r_2r_4^2$, which are invariant under σ and cyclically permuted by both τ and ω. It follows that these are the roots of a cyclic quartic over K, and that in particular

$$\begin{aligned} r_1r_2^2 + r_4r_3^2 &= u + v\Delta\sqrt{5}, \\ r_3r_1^2 + r_2r_4^2 &= u - v\Delta\sqrt{5} \end{aligned} \tag{10}$$

for some $u, v \in K$, where $\sqrt{5}$ is defined by the choice of ζ: $\zeta + \zeta^{-1} = (-1+\sqrt{5})/2$.

Lemma. *Given r_1, there is a unique choice of r_2, r_3, r_4 such that $r_1r_4, r_2r_3 \in K(\Delta\sqrt{5})$ and such that the two equations in* (10) *are satisfied.*

Proof. We have already seen that r_1 uniquely determines r_4 and that r_2 uniquely determines r_3 by the conditions $r_1r_4, r_2r_3 \in K(\Delta\sqrt{5})$. It remains to show that r_1 uniquely defines r_2 subject to the equations in (10).

If r_2 were replaced by εr_2 for some nontrivial fifth root of unity ε, then r_3 would be replaced by $\bar{\varepsilon}r_3$ (where $\varepsilon\bar{\varepsilon} = 1$), since their product must lie in $K(\Delta\sqrt{5})$. If this new choice for r_2 and r_3 (together with the fixed r_1 and r_4) also satisfied the equations in (10), we would have

$$\begin{aligned} r_1r_2^2 + r_4r_3^2 &= u + v\Delta\sqrt{5}, \\ r_3r_1^2 + r_2r_4^2 &= u - v\Delta\sqrt{5} \end{aligned} \quad \text{and} \quad \begin{aligned} r_1(\varepsilon r_2)^2 + r_4(\bar{\varepsilon}r_3)^2 &= u + v\Delta\sqrt{5}, \\ (\bar{\varepsilon}r_3)r_1^2 + (\varepsilon r_2)r_4^2 &= u - v\Delta\sqrt{5}. \end{aligned}$$

Equating the expressions for $u + v\Delta\sqrt{5}$ gives

$$\frac{r_1 r_2^2}{r_4 r_3^2} = -\frac{1-\bar{\varepsilon}^2}{1-\varepsilon^2} = \frac{1}{\varepsilon^2},$$

and equating the expressions for $u - v\Delta\sqrt{5}$ gives

$$\frac{r_1^2 r_3}{r_4^2 r_2} = -\frac{1-\varepsilon}{1-\bar{\varepsilon}} = \varepsilon.$$

These two equations give $(r_1/r_4)^5 = 1$, which implies that r_1/r_4 is a fifth root of unity. This is a contradiction, since this element generates a quintic extension of $L(\zeta)$ which survives any specialization (the order of the Galois group of the irreducible $f(x)$ is divisible by 5), and completes the proof. □

The elements u and v are computed as before:

$$\begin{aligned} u &= -25q/2, \\ v &= (c_0 + c_1\theta + c_2\theta^2 + c_3\theta^3 + c_4\theta^4 + c_5\theta^5)/(2DF), \end{aligned} \tag{11}$$

where the coefficients c_i for the general $f(x)$ are given in the Appendix. For the special case of $f(x) = x^5 + ax + b$ these are:

$$\begin{aligned} u &= 0, \\ v &= (-2048a^7 + 25000a^2b^4 - 3072a^6\theta - 6250ab^4\theta \\ &\quad - 1664a^5\theta^2 - 3125b^4\theta^2 - 448a^4\theta^3 \\ &\qquad - 96a^3\theta^4 - 16a^2\theta^5)/(32000a^5b^3 + 390625b^7). \end{aligned} \tag{11′}$$

Theorem 2. *Suppose the irreducible polynomial* $f(x) = x^5 + px^3 + qx^2 + rx + s \in \mathbb{Q}[x]$ *is solvable by radicals, and let* θ *be the unique rational root of the associated resolvent sextic* $f_{20}(x)$ *as in Theorem* 1. *Fix any square root* Δ *of the discriminant* D *of* $f(x)$ *and fix any primitive fifth root of unity* ζ. *Define* l_0 *as in equation* (8.0), *and define* l_1, l_4 *and* l_2, l_3 *to be the roots of the quadratic factors in* (7), *subject to the condition* $(l_1 - l_4)(l_2 - l_3) = \mathscr{O}\Delta$ *in* (9). *Then the Galois group of* $f(x)$ *is*:

(a) *the Frobenius group of order* 20 *if and only if the discriminant* D *of* $f(x)$ *is not a square, which occurs if and only if the quadratic factors in* (7) *are irreducible over* $\mathbb{Q}(\sqrt{D})$,

(b) *the dihedral group of order* 10 *if and only if* D *is a square and the rational quadratics in* (7) *are irreducible over* $\mathbb{Q}$,

(c) *the cyclic group of order* 5 *if and only if* D *is a square and the rational quadratics in* (7) *are reducible over* $\mathbb{Q}$.

Let r_1 *be any fifth root of* R_1 *in* (4.1), *and let* r_2, r_3, r_4 *be the corresponding fifth roots of* R_2, R_3, R_4 *as in the lemma above. Then the formulas* (3) *give the roots of* $f(x)$ *in terms of radicals and* x_1, x_2, x_3, x_4, x_5 *are permuted cyclically by some* 5*-cycle in the Galois group.*

Proof. The conditions in (a) to (c) are simply restatements of the structure of the field $L = K(l_1) = K(l_1, l_2, l_3, l_4)$ under specialization.

We have already seen that the choice of Δ and the roots l_i of the quadratics determines the R_i up to an ordering: (R_1, R_2, R_3, R_4) or (R_4, R_3, R_2, R_1) if the choice of Δ is the same as that in the computations above, and (R_3, R_1, R_4, R_2) or (R_2, R_4, R_1, R_3) if the choice of Δ is the negative of that used in the computations above. It is easy to check that the corresponding resolvents r_i are then simply (r_1, r_2, r_3, r_4), (r_4, r_3, r_2, r_1), (r_3, r_1, r_4, r_2), and (r_2, r_4, r_1, r_3), respectively (this is the action of the automorphism $\tau = (2\,3\,5\,4)$ above). The formulas (3) then give the roots x_i in the orders $(x_1, x_2, x_3, x_4, x_5)$, $(x_1, x_5, x_4, x_3, x_2)$, $(x_1, x_3, x_5, x_2, x_4)$, and $(x_1, x_4, x_2, x_5, x_3)$, respectively. In terms of the 5-cycle $\sigma = (1\,2\,3\,4\,5)$ above, these correspond to cyclic permutations by σ, σ^{-1}, σ^2, and σ^3, respectively.

Finally, any choice of primitive fifth root of unity ζ produces precisely the same permutations of the roots x_i, so the roots of $f(x)$ are produced in a cyclic ordering independent of all choices. □

Remark. Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of degree n whose Galois group is, for example, known to be the cyclic group of order n. If the roots of $f(x)$ are given (numerically in $\mathbb{C}$, say), how can one order the roots so that they are cyclically permuted by some element in the Galois group? For $n = 5$, a solution is provided by Theorem 2, and the situation for $n = 4$ is solved implicitly above (this is the reason for considering the factorization in equation (7) and the ordering condition $(l_1 - l_4)(l_2 - l_3) = \mathscr{O}\Delta$). Such orderings are necessary in the computation of regulators as in [3], and the question for general n seems an interesting one.

5. Examples

(1) Let $f(x) = x^5 + 15x + 12$, whose discriminant is $D = 2^{10}3^4 5^5$. The corresponding resolvent sextic $f_{20}(x)$ is the polynomial

$$x^6 + 120x^5 + 9000x^4 + 540000x^3 + 20250000x^2 + 324000000x,$$

which clearly has $\theta = 0$ as a root. It follows that the Galois group of $f(x)$ is the Frobenius group F_{20} and that $f(x)$ is solvable by radicals. With $\Delta = 7200\sqrt{5}$, where $\zeta + \zeta^{-1} = (-1 + \sqrt{5})/2$, the roots l_1, l_2, l_3, l_4 of the quadratics in (7) (subject to the ordering condition in (9)) are

$$\begin{aligned}
l_1 &= -375 - 750\sqrt{5} + 75i\sqrt{625 + 29\sqrt{5}}, \\
l_4 &= -375 - 750\sqrt{5} - 75i\sqrt{625 + 29\sqrt{5}}, \\
l_2 &= -375 + 750\sqrt{5} - 75i\sqrt{625 - 29\sqrt{5}}, \\
l_3 &= -375 + 750\sqrt{5} + 75i\sqrt{625 - 29\sqrt{5}}.
\end{aligned}$$

Then

$$R_1 = -1875 - 75\sqrt{1635 + 385\sqrt{5}} + 75\sqrt{1635 - 385\sqrt{5}},$$
$$R_4 = -1875 + 75\sqrt{1635 + 385\sqrt{5}} - 75\sqrt{1635 - 385\sqrt{5}},$$
$$R_2 = 5625 - 75\sqrt{1490 + 240\sqrt{5}} - 75\sqrt{1490 - 240\sqrt{5}},$$
$$R_3 = 5625 + 75\sqrt{1490 + 240\sqrt{5}} + 75\sqrt{1490 - 240\sqrt{5}}.$$

Viewing these as real numbers, and letting r_1 be the real fifth root of R_1, we conclude that the corresponding r_2, r_3, and r_4 are the real fifth roots of R_2, R_3, and R_4, respectively, and then (3) gives the roots of $f(x)$. For example, the sum of the real fifth roots of R_1, R_2, R_3, R_4 above gives five times the (unique) real root of $x^5 + 15x + 12$.

(2) Let $f(x) = x^5 - 5x + 12$, whose discriminant is $D = 2^{12}5^6$. The corresponding resolvent sextic $f_{20}(x)$ is the polynomial

$$x^6 - 40x^5 + 1000x^4 + 20000x^3 + 250000x^2 - 66400000x + 976000000,$$

which has $\theta = 40$ as a root, so that $f(x)$ has solvable Galois group. Since in this case the quadratic factors in (7) are $x^2 + 1250x + 6015625$ and $x^2 - 3750x + 4921875$, which are irreducible over $\mathbb{Q}$, it follows that the Galois group of $f(x)$ is the dihedral group of order 10. If $\Delta = 8000$, the roots l_1, l_2, l_3, l_4 of the quadratics in (7) (subject to the ordering condition in (9)) are

$$l_1 = -625 + 750\sqrt{-10},$$
$$l_4 = -625 - 750\sqrt{-10},$$
$$l_2 = 1875 + 375\sqrt{-10},$$
$$l_3 = 1875 - 375\sqrt{-10}.$$

Then

$$R_1 = -3125 - 1250\sqrt{5} - \frac{750}{2}\sqrt{100 + 20\sqrt{5}} - \frac{375}{2}\sqrt{100 - 20\sqrt{5}},$$
$$R_4 = -3125 - 1250\sqrt{5} + \frac{750}{2}\sqrt{100 + 20\sqrt{5}} + \frac{375}{2}\sqrt{100 - 20\sqrt{5}},$$
$$R_2 = -3125 + 1250\sqrt{5} + \frac{375}{2}\sqrt{100 + 20\sqrt{5}} - \frac{750}{2}\sqrt{100 - 20\sqrt{5}},$$
$$R_3 = -3125 + 1250\sqrt{5} - \frac{375}{2}\sqrt{100 + 20\sqrt{5}} + \frac{750}{2}\sqrt{100 - 20\sqrt{5}}.$$

Again viewing these as real numbers, and letting r_1 be the real fifth root of R_1, we conclude that the corresponding r_2, r_3, and r_4 are the real fifth roots of R_2, R_3, and R_4, respectively, and then (3) gives the roots of $f(x)$. For example, the sum of the real fifth roots of R_1, R_2, R_3, R_4 above again gives five times the (unique) real root in this example.

(3) Let $f(x) = x^5 - 110x^3 - 55x^2 + 2310x + 979$, whose discriminant is $D = 5^{20}11^4$. The corresponding resolvent sextic $f_{20}(x)$ is the polynomial

$$x^6 + 18480x^5 + 47764750x^4 - 580262760000x^3 - 1796651418959375x^2 + 2980357148316659375x - 36026068564469671875,$$

which has $\theta = -9955$ as a root, so that $f(x)$ has solvable Galois group. Since in this case the quadratic factors in (7) are $(x - 797500)(x + 61875)$ and $(x - 281875)(x + 405625)$, it follows that the Galois group of $f(x)$ is the cyclic group of order 5. If $\Delta = 5^{10}11^2$, the roots l_1, l_2, l_3, l_4 of the quadratics in (7) (subject to the ordering condition in (9)) are

$$\begin{aligned} l_1 &= 797500, \\ l_4 &= -61875, \\ l_2 &= 281875, \\ l_3 &= -405625. \end{aligned}$$

Then

$$\begin{aligned} R_1 &= 5^5 11(41\zeta + 26\zeta^2 + 6\zeta^3 + 16\zeta^4), \\ R_2 &= 5^5 11(6\zeta + 41\zeta^2 + 16\zeta^3 + 26\zeta^4), \\ R_3 &= 5^5 11(26\zeta + 16\zeta^2 + 41\zeta^3 + 6\zeta^4), \\ R_4 &= 5^5 11(16\zeta + 6\zeta^2 + 26\zeta^3 + 41\zeta^4). \end{aligned}$$

Here,

$$u + v\Delta = \frac{1375 + 6875\sqrt{5}}{2}, \qquad u - v\Delta = \frac{1375 - 6875\sqrt{5}}{2},$$

so with r_1 any fifth root of R_1, r_4 is the fifth root of R_4 such that $r_1 r_4$ is real, and r_2, r_3 are the fifth roots of R_2, R_3 whose product is real and which satisfy $r_3 r_1^2 + r_2 r_4^2 = (1375 - 6875\sqrt{5})/2$. This is the *Casus Irreducibilis* for quintic polynomials, where the five real roots of the quintic are expressed by radicals of necessarily nonreal complex numbers (in general, if only real radicals are required for a solvable polynomial, all of whose roots are real, then the Galois group is a 2-group, cf. [2]).

Acknowledgment

I would like to acknowledge the assistance of Hershy H. Kisilevsky and Richard M. Foote for helpful conversations.

BIBLIOGRAPHY

1. D. S. Dummit and R. M. Foote, *Abstract algebra*, Prentice-Hall, New York, 1991.
2. I. M. Isaacs, *Solution of polynomials by real radicals*, Amer. Math. Monthly **92** (1985), 571–575.
3. R. Schoof and L. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556.
4. H. Weber, *Lehrbuch der Algebra*. I, Chelsea, New York, 1961.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VERMONT, BURLINGTON, VERMONT 05405
E-mail address: dummit@griffin.uvm.edu