Solving Quintics and Septics by Radicals

Mohammed A. Faggal [*], Daniel Lazard [**]

[*] National Grid, Dammam, Saudi Arabia
[**] UPMC Univ Paris 06, LIP6, F-75005, Paris, France
INRIA Paris-Rocquencourt, SALSA project team, F-78153 Le Chesnay, France
CNRS, LIP6, F-75005, Paris, France

Abstract- Formulas are given for solving by radicals every solvable quintic or septics. The formula for the quintics are much shorter than the preceding ones, while the formula for the septics seems the first published one. Instead of using resolvent as the preceding papers on this subject, this paper uses the factorization of the polynomials whose roots are the sum of two different roots of the input (for the quintics) or the sum of three different roots of the input (for the septics).

I. Introduction

Solving equations by radical is a long standing open problem. The problem was almost closed by Abel who proved that, *in general*, the solutions of the equations of degree five or higher may not be expressed in term of radicals. However Abel did left open two sub problems.

The first one is, given an equation, to test if it is solvable by radicals. This problem has, theoretically, been solved by Galois who introduced Galois theory for this purpose. However, for a given equation, the computation which is needed is not practicable without a computer. Even with a computer, the computation needs very efficient algorithms, and it is rather recent that one is able to compute the Galois group and thus to test solvability of equations of degrees up to 15 (Geissler and

The second problem is, when one has a solvable equation, to effectively compute the solutions in term of radicals. All the papers that we know on this subject concern the quintic equations (Paxton Young, 1888; Dummit, 1991; Lazard, 2004; Lavallee et al., 2005) or sextic equations (Hagedorn, 2000). One of the reasons for this is the size of the formulas. The formula for the quintic given in Lazard (2004) is three pages length. Using the same method to solve a septic equation would need to consider a resolvent equation of degree 120 instead of degree 6 for solving quintics. Such a computation is thus unrealistic.

In this paper we present some progress on this second problem. Firstly we describe a new formula for solving quintics which is much shorter than the preceding ones. Secondly, we present a complete formula for solving solvable septics. In the worst case the roots extractions which are needed for getting the first root are one seventh root, the root of a cyclic cubic (which involves a cubic root and $\sqrt{-3}$) and the square root of the product of the discriminant by -7. For the other roots, one has to add a seventh root of unit, which involves $\sqrt{-7}$, $\sqrt{-3}$ and a cubic root. As far as we know this is the first complete formula for solving solvable septics.

The key idea which allows these progresses is the following. In the preceding formulas for quintics, the roots are expressed in term of a single invariant, which is a root of a polynomial of degree six, the quintic being solvable if and only if this polynomial has a rational root. Instead we use the characterization given by Bruen et al. (1986) of the solvable polynomials of prime degree in the following way.

Let f be a quintic whose discriminant is a square, and f_{10} be the polynomial of degree 10 whose roots are the sums of two different roots of f. The quintic f is solvable if and only if f_{10} factors into two quintics. Thus the for every solvable quintic, the polynomial f_{10} factors in two quintics over the field extension by the square root of the discriminant. The coefficient of these quintics is not only invariants of the group of order 10, but they generate the algebra of the invariants of this group. It follows that the roots of the input quintic may be expressed in term of these invariants. This is detailed in Section 4.

Similarly, for a septic, let f_{35} be the polynomial of degree 35 whose roots are the sums of three different roots of the septic. The septic is solvable if and only if f_{35} factors either in more than two factors or in a factor of degree 21 and a factor of degree 14. Factorizing further on the extension by the square root of the discriminant, we get, in any case, two polynomials of degree 7 which are invariant by the group of order 21. These two factors do not provide directly enough invariants to express the solutions. We have thus to deduce from them other septics which are invariant by the same group of order 21 for expressing the roots of the input septic.
The details are given in Section 5.

II. Generalities and Notation

In this section, we describe the generalities which may applied to any solvable equation of prime degree, even the trivial cases 2 and 3.

We consider a univariate irreducible polynomial $f = x^n + a_1x^{n-1} + \ldots + a_n$ of prime degree n, with coefficients in a field whose characteristic does not divide $n(n-1)$.

To simplify the formulas, we usually suppose that f is in *depressed* form, that is that $a_1 = 0$. This does not restricts the generality, as the depressed form may be obtained by the Tschirnhaus transformation $x \to x - a_1/n$ and the roots of the initial polynomial may be obtained by subtracting a_1/n from the roots of the depressed form.

We choose once for all an arbitrary root x0 off, a cycle σ of order n in the Galois group of f and a primitive nth root of unit ω.

These choices allow to number the other roots of f by $x_i = \sigma^i(x_0)$. The index i of x_i is supposed to belong to the finite field F_n, i.e. $x_{i+n} = x_i$.

As usual when solving by radical in prime degree [1] the roots are computed from their Fourier transform $u_j = \sum_{i=0}^{n-1} \omega^{ij} x_i$. In particular $u_0 = x_0 + \cdots + x_{n-1}$ is the sum of the roots and, if the polynomial is in depressed form, we have u0 = 0.

We have $\sigma(u_j) = \omega^{-j} u_j$. It follows that any monomial in the u_i whose the sum of the indexes are a multiple of n is invariant by σ.

As n is supposed to be prime, the polynomial f is solvable if and only if its Galois group is contained in the affine group of F_n, of order $n(n-1)$. Each element of this groups of order $n(n-1)$ is defined by a pair (a, b) of elements of Fn, with $b \neq 0$, and acts on x_i by $x_i \rightarrow x_{a+bi}$. If g is a generator of the multiplicative group F^*_n, this group is thus generated by σ, which corresponds to $(a, b) = (1, 1)$ and the automorphism γ, which corresponds to $(a, b) = (0, g)$. Thus $\gamma(x_i) = x_{gi}$ and $\gamma(u_i) = u_{ig-1}$. In this paper, we choose $g = 3$, $g^{-1} = 2$ when $n = 5$ and $g = 5$, $g^{-1} = 3$ when $n = 7$.

These notations allow to be more accurate than in the introduction for describing our method. The factorization of the minimal polynomial of the sum of two or three roots over the field extension by the square root of the discriminant provides

[1] This is true even in degree 2 an 3, even if it is not explicit on classical formulas.

a number of invariants of the group of order $n(n-1)/2$ generated by σ and γ^2. The game consists in defining some polynomials in the u_i which are invariant by this group, in expressing them in term of these known invariants, which gives some equations in the u_i. One of these equations is a polynomial of degree $(n-1)/2$ in u_1^n which allows to compute u_1. The other equations depend only on u_1 and some u_i and are linear in u_i and thus allows to express u_i in term of u_1.

A key ingredient for this is an algorithm for expressing some invariant in term of a given set of invariants, which will be described in next section.

2.1 Reducing invariants

The invariants, we are considering here are homogeneous polynomials in the indeterminates $x_0, \ldots, x_{n-1}$, which are invariant under the action of a subgroup of the symmetric group of all permutations of the x_i. [2] In practice we will consider only invariants for the group of order $n(n-1)/2$.

The problem that we consider is to express an invariant (which is useful for solving) in term of a given set of invariants (which are easy to compute). The method that we use is essentially described in Lazard (2004). It is based on the following classical result.

Proposition 1. *The algebra of the invariants of a subgroup* G *of the group of permutations of* n *elements is a free module of finite type over the ring of the polynomials in the elementary symmetric functions.*

To describe how this result may be used, we need some notation.

We denote by E_d the elementary symmetric function of degree d of the x_i, and we associate to it a new indeterminate e_d and the polynomial $E_d - e_d$ (depending on the variables $x_0, \ldots, x_{n-1}$ and e_d). Let G be the Grobner basis of the ideal $<E_1 - e_1, \ldots, E_n - e_n>$, for a monomial ordering which eliminates the x_i (i.e. for comparing two monomials, one uses the powers of the e_d only when the powers of the x_i are the same). The following result is proved in Lazard (2004).

Lemma 2. *An invariant belongs to a basis of the free module of Proposition 1 if and only if the leading monomial of its normal form by* G *is independent of the* e_d.

[2] We use the same notations for the roots of a specific polynomial f and for the roots of the generic polynomial $\Pi^{n-1}_{i=0}(x - x_i)$. The choice between the two meanings of x_i will be clear form the context. This ambiguity is useful as it allows, even in the case of a specific polynomial, to consider an invariant either as an element of the field of the coefficients or as a polynomial function of the roots.

This allows the following procedure to compute invariants.

For the first invariant F_1, we compute its normal $NF(F_1)$ form by G. If it belongs to a basis of the free module of invariants (i.e. its leading term depends only on the x_i), we introduce a new indeterminate f_1 and the polynomial $P_1 := NF(F_1) - f_1$.

From now on, the normal form procedure is modified and consists in reducing first by G, then by $P_1, \ldots$, a polynomial being reducible by some P_i only if its leading term is the product of the leading term of P_i by a monomial which is independent of the x_i.

With this special normal form procedure, if the normal form of an invariant has leading term which depends only on the x_i, it is linearly independent of the invariant corresponding to the preceding P_i, and one may add a new indeterminate f_i and a new polynomial P_i. On the other hand, if the normal form depends only on the e_i and the f_i then this gives the expression of the new invariant in term of the preceding ones.

This procedure allows to output easily the formulas presented in the next sections.

III. Minimal Polynomial of Sums of Roots

As the solutions are expressed by factorizing the minimal polynomial of the sum of two or three roots of the input polynomial, we need to compute this minimal polynomial. This may be done at run time by a sub procedure of the solving procedure, but it is better to compute it, once for all, as a polynomial whose coefficients are polynomials in the coefficients of a generic polynomial. This has the advantage to avoid to take care of the nature of the coefficients when writing the solving procedure, and also to be closer to what is usually called a formula.

We know of several ways to do this computation. We present the two which are the most convenient for solving in degree 5 and 7.

3.1 Sum of two roots by resultant

Let $f(x)$ be a polynomial. If s is the sum of two roots of f, then there is α such α and $s - \alpha$ are roots of f. Thus s is a root of the polynomial R defined in MAPLE syntax by *resultant(f, subs(x=s-x,f),x)*. Unfortunately, R is not the minimal polynomial

of *s*. It the product of the square of the desired polynomial and the polynomial whose roots are the double of a root of *f*.

One may get the desired polynomial by factoring *R*, but it is much more convenient to get it directly without factoring. For this purpose, we consider the two polynomials
$f_+ = f(x)+f(y)$ and $f_- = (f(x) - f(y))/(x - y)$. Both are symmetric in *x* and *y*. Thus, if we substitute *x* by $(s+d)/2$ and *y* by $(s-d)/2$, we get two polynomials in s and d^2, and we get the desired polynomial by the resultant eliminating d^2. This resultant is the minimal polynomial of *s*. In fact the desired minimal polynomial has degree $n\ (n - 1)/2$. The degrees in d^2 of f_+ and f_- are respectively $\lfloor n/2 \rfloor$ and $\lfloor (n-1)/2 \rfloor$. The degrees in *s* of the coefficient of d^{2i} in f_+ and f_- are respectively at most $n - 2i$ and $n - 2i - 1$. It follows that the resultant has degree in s at most $n\ (n - 1)/2$ which is the degree of the desired minimal polynomial.

This computation is easily and efficiently implemented in MAPLE by the following instructions.

```
fx :=f; fy :=subs (x = y, f);
fp :=subs (t =sqrt (t), primpart (subs (x = (s + t)/2, y = (s − t)/2,
fx +fy)));
fm:=subs (t =sqrt (t)),
   primpart (normal (subs (x = (s + t)/2, y = (s − t)/2, (fx −fy)/(x
− y))));
collect (primpart (resultant (fp, fm, t)), s);
```

3.2 Sum of three roots by Newton's identities

For getting the minimal polynomial of the sum of three roots, the preceding method based on a resultant computation may not be used because there are several variables to eliminate. Grobner bases may be used, but induce problems of efficiency when the coefficients of the input polynomial are algebraic numbers or are generic (independent variables). This case of generic coefficients is especially important because it provides a formula which may be used directly, whichever is the nature of the coefficients.

To get this minimal polynomial, we use Newton inequality in the following way.

We start from the polynomial $f = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$. There are
$N = n\ (n - 1)\ (n - 2)/6$ sums of three different roots. Thus we are looking for a polynomial of degree *N*. We compute first the sums S_i of the *i*th powers of the roots for $i = 1, \ldots, N$ by the Newton inequalities:

$$
\begin{aligned}
-S_1 &= a_1 \\
-S_i &= a_1 S_{i-1} + a_2 S_{i-2} + \cdots + a_{i-1} S_1 + i\, a_i && \text{for } i \le n \\
-S_i &= a_1 S_{i-1} + a_2 S_{i-2} + \cdots + a_{n-1} S_{i-n+1} + a_n S_{i-n} && \text{for } i > n
\end{aligned}
$$

Then we compute, for $i + j \le N$ the sums $S_2(i, j)$ of the products $x^i y^j$ where *x* and *y* are two different roots of *f*. We have

$$
\begin{aligned}
S_{i,j} &= S_i S_j - S_{i+j} && \text{if } i > j \\
S_{i,i} &= (S_i^2 - S_{2i})/2.
\end{aligned}
$$

From this we deduce the sums $S_3(i, j, k)$ of the products $x^i y^j z^k$ of three powers of roots:

$$
\begin{aligned}
S_{i,j,k} &= S_i S_{j,k} - S_{i+j,k} - S_{i+k,j} && \text{if } i > j > k \\
S_{i,i,k} &= S_k S_{i,i} - S_{i+k,i} && \text{if } i > k \\
S_{i,k,k} &= S_i S_{k,k} - S_{i+k,k} && \text{if } i > k \\
S_{i,i,i} &= (S_i S_{i,i} - S_{2i,i})/3.
\end{aligned}
$$

These sums are useful to compute the sums of Newton of the roots of the desired polynomial of degree *N*. In fact these sums of Newton are the sums of the $(x+y+z)^m$ where *x*, *y*, *z* runs over all triplets of roots of *f*. When expanding these sums of products, the S_i, $S_{i,j}$, $S_{i,j,k}$ appear with multinomial coefficients. However it should be remarked that a term $x^i y^j$ appears in the expansion of $n-2$ terms $(x+y+z)^m$ and x^i in the expansion of $(n - 1)\ (n - 2)/2$ terms.

Thus we have

$$S(m) = \sum (x+y+z)^m = \frac{(n-1)(n-2)}{2} S_m + (n-2) \sum_{i \ge j, i+j=m} \binom{m}{i} S_{i,j} + \sum_{i \ge j \ge k, i+j+k=m} \binom{m}{i,j,k} S_{i,j,k}$$

Finally the coefficients of the desired polynomial are obtained by using the Newton identities again:

$$A_0 = 1; \qquad -k A_k = \sum_{i=1}^{k} S(i) A_{k-i} \quad \text{for } k = 1 \ldots n(n-1)(n-2)/6$$

Although rather involved this procedure is quite efficient: Applied to the generic depressed polynomial of degree 7, all the A_i have together *2, 635* terms which are computed in around two seconds on a laptop.

IV. QUINTICS

4.1 Generic quintic

Let $F = x^5 + A_1 x^4 + A_2 x^3 + A_3 x^2 + A_4 x + A_5 = \Pi^4_{i=0}(x - x_i)$ be a generic quintics, where the roots x_i are indeterminates. The action on the sums of two roots of the circular permutation σ defined in Section 2 has two orbits, containing respectively $x_0 + x_1$ and $x_0 + x_2$. These orbits are invariant under the action of γ^2 and exchanged by γ. It follows that the polynomials F1 = $\Pi^4_{i=0}$ s − $(x_i + x_{i+1})$ and F2 = Q4i=0 s − (xi + xi+2) (recall that the indexes are defined modulo 5) are invariant by the group of order 10 generated by σ and γ^2.

Let us denote respectively by B_i and C_i the coefficients of s^{5-i} in F_1 and F_2. Let also $D_i = B_i - C_i$. All these polynomials in the x_i are thus invariant for the group of order 10.

The procedure described in Section 2.1 allows to prove easily the following.

Proposition 3. *We have* $B_1 = C_1 = 2A_1$, $B_2 + C_2 = 3A_2 + 2A_1^2$, $B_3 + C_3 = A_3 + 3A_1 A_2$.

There is a base of the free module of the invariants of the group of 10 elements containing $1, D_2, D_3, D_4, D_5, D_2^2, D_2 D_3, D_2^3, D_3^2, D_2 D_5, D_2^4, D_2 D_3 D_5$.

There is another base containing the same invariants, with D_2^2 and $D_2 D_3$ replaced by $B_4 + C_4$ and $B_5 + C_5$.

Let us recall that the Molien series of a group is the formal series whose coefficient of degree i is the dimension of the vector space of the invariants of degree

i. The Molien series of the symmetric group of order *n* is the series expansion of $1/\Pi^n_{i=1}(1 - t^i)$. Proposition 1 implies that the Molien series of a group of permutations is the expansion of $M/\Pi^n_{i=1}(1 - t^i)$ where *M* is a polynomial whose coefficient of degree *i* is the number of invariants of degree i in the bases defined in Proposition 1. There are standard procedures to compute the Molien series. One is implemented is software MAGMA, which gives that for the group of order 10 the polynomial *M* is $t^{10} + t^8 + t^7 + 2t^6 + 2t^5 + 2t^4 + t^3 + t^2 + 1$. Similarly, the polynomial M for the maximal solvable group of order 20 is $t^8 + t^7 + t^6 + t^5 + t^4 + 1$.
It follows.

Proposition 4. *Each set of invariants described in Proposition 3 is a basis over the ring of elementary symmetric functions of the module of the invariants of the group of 10 elements.*

A basis of the invariants of the maximal solvable group of degree 5 and order 20 is $(1, D_2^2, D_2D_3, D_3^2, D_2D_5, D_2^4)$.

4.2 Solving quintics

When the generic polynomial *F* of the preceding section is specialized to a polynomial $f = a_0 x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5$, all the invariants specialize as well. In this section, we denote by *K* the field of the coefficients of *f*. If *f* is irreducible over *K* and solvable, its Galois group may be of order 20. Let us consider the extension $K(\sqrt{D})$ of *K* generated by the square root of the discriminant *D* of *f*. Over this field the Galois group is either the cyclic group of order 5 of the group of order 10. It follows that the specializations f_1 and f_2 of F_1 and F_2 have their coefficients in this field and are irreducible on it (the Galois group is transitive on their roots). Moreover, if the discriminant of *f* is not a square, its Galois group is transitive on the sums of two roots and f_1 and f_2 are conjugate, i.e. they are exchanged by changing the sign of the square root of the discriminant. Thus we have the following

Proposition 5. *Over $K(\sqrt{D})$, the minimal polynomial f_{10} of the sum of two roots of f factors exactly in two factors of degree 5.*

Moreover if the discriminant of f is not a square (i.e. $K(\sqrt{D}) \neq K$), then f1 and f2 are conjugate. It follows that, in any case, the coefficients of $f_1 + f_2$ and $(f_1 - f_2)\sqrt{D}$ belong to K.

To simplify the formulas, from now on we suppose, w.l.o.g., that f is in depressed form, that is $a_1 = 0$.

Supposing, w.l.o.g., that f_1 and f_2 are monic, let us denote by e_i and d_i the coefficients of degree $5 - i$ of $f_1 + f_2$ and $(f_1 - f_2)\sqrt{D}$ respectively. Proposition 4 shows that any invariant of the group of order 10 may be expressed polynomially in term of the ai, di and ei, and we have described a procedure to compute such an expression.

The following polynomials in the ui (Fourier transform of the roots) are such invariants. We give them with their expression in term of the coefficients of f_1 and f_2 computed by above procedure.

$$u_1 u_4 = -\frac{1}{2} d_2 - \frac{5}{2} a_2 \tag{1}$$

$$u_1^5 + u_4^5 = \frac{125}{2} d_5 + 125 e_5 - \frac{25}{4} d_3 a_2 - \frac{75}{4} d_2 a_3 - \frac{125}{2} a_2 a_3 - \frac{375}{2} a_5 \tag{2}$$

$$u_4^2 u_2 + u_1^2 u_3 = -\frac{5}{2} d_3 - \frac{25}{2} a_3 \tag{3}$$

$$u_1^3 u_2 + u_4^3 u_3 = \frac{25}{2} d_4 + \frac{15}{2} e_4 - \frac{15}{2} d_2 a_2 - 40 a_4 - \frac{5}{2} a_2^2 \tag{4}$$

Equations 1 and 2 show that u_1^5 and u_2^5 are the roots of a quadratic equation with may be solved to get u_1^5. Extracting a fifth root gives u_1. If it is not null, the value of u_1u_4 gives u_4 rationally in term of u_1. Then u_2 and u_3 are deduced by solving the linear system given by Equations 3 and 4. Finally the roots are deduced by inverse Fourier transform. This procedure is made explicit below.

However some care is needed if the quadratic equation for u_1^5 has a null root or a double root.

If the two roots of this quadratic equation are null, one may exchange f_1 and f_2, which amounts to change the sign of all d_i in the above relations. If the new quadratic equation would have also two null roots, then all the u_i would be null and the five roots of *f* would be equal, which is impossible as *f* is irreducible.

If one root of the quadratic equation is null then one chooses $u_4 = 0$ and u_1 is the fifth root of the right hand side of Equation 2.

The determinant of the linear system in u_2 and u_3 is $u_1^5 - u_4^5$. We show now that it may be null only if $u_1 = u_4 = 0$. In fact, if $u_1^5 = u_4^5 \neq 0$, we have $u_4 = \omega^i u_1$ for some *i*, where ω is the primitive root of unit which has been chosen. Thus, if we denote by h_1 and h_3 the right hand sides of Equations 1 and 3 respectively, we have $u_1^2 = h_1/\omega^i$ and $u_2 \omega^2 + u_3 = h_3$. As $u_2 u_3 = d_2/2 - 5 a_5$ (conjugate equation of Equation 1), we see that all the u_i and thus all the roots belong to an extension of *K* of degree prime to 5, which implies that *f* is not irreducible. Thus we have proved that the following MAPLE procedure computes the roots of *f*. However, for better readability we write separately the polynomial of degree 10 which is factored during the procedure. For the same reason, the usual mathematical notation for product and root extractions has been preferred to the alphanumerical notation which is usual in programming languages.

$$\begin{aligned} f_{10} = {} & s^{10} + 3a_2 s^8 + a_3 s^7 + \left(-3a_4 + 3a_2^2\right) s^6 + \left(2a_2 a_3 - 11 a_5\right) s^5 \\ & + \left(-2a_4 a_2 + a_2^3 - a_3^2\right) s^4 + \left(-4a_4 a_3 + a_2^2 a_3 - 4a_5 a_2\right) s^3 \\ & + \left(7a_5 a_3 + a_4 a_2^2 - 4a_4^2 - a_2 a_3^2\right) s^2 + \left(4a_4 a_5 - a_2^2 a_5 - a_3^3\right) s \\ & - a_5^2 + a_2 a_3 a_5 - a_4 a_3^2 \end{aligned} \tag{5}$$

With this definition, the MAPLE procedure is:

$$
\begin{aligned}
&quintic := proc\,(pol);\\
&x := op\,(indets\,(pol);\\
&t := coeff\,(pol, x, 4)/coeff\,(pol, x, 5)/5;\\
&f := primpart\,(subs\,(x{=}x{-}t{,}pol));\\
&D := discrim\,(f, x);\\
&for\quad i\quad from\quad 2\quad to\quad 5\quad do\quad a_i := coeff\,(f, x, 5-i)\quad od;\\
&f_{10} := factor\,(\ \langle\ \text{Equation 5}\ \rangle\ , D^{1/2});\\
&if\ not\ type\,(f_{10}, `*`)\ then\ RETURN\,(\text{"the quintic is not solvable"})\ fi;\\
&(f_1, f_2) := op\,(f_{10});\\
&e_4 := coeff\,(f_1+f_2, s, 1);\quad e_5 := coeff\,(f_1+f_2, s, 0);\\
&d_2 := \sqrt{5}\cdot coeff\,(f_1-f_2, s, 3);\quad d_3 := \sqrt{5}\cdot coeff\,(f_1-f_2, s, 2);\\
&d_4 := \sqrt{5}\cdot coeff\,(f_1-f_2, s, 1);\quad d_5 := \sqrt{5}\cdot coeff\,(f_1-f_2, s, 0);\\
&if\quad d_2/2-5\,a_2/2=0\\
&\quad and\quad 125\,d_5/2+125\,e_5-25\,d_3\,a_2/4-75\,d_2\,a_3/4-125\,a_2\,a_3/2-375\,a_5/2=0\\
&\quad then\quad d_2 := -d_2;\quad d_3 := -d_3;\quad d_4 := -d_4;\quad d_5 := -d_5;\quad fi;\\
&h_1 := -d_2/2-5\,a_2;\quad h_3 := -5\,d_3/2-25\,a_3/2;\\
&h_2 := 125\,d_5/2+125\,e_5-25\,d_3\,a_2/4-75\,d_2\,a_3/4-125\,a_2\,a_3/2-375\,a_5/2;\\
&h_4 := 25\,d_4/2+15\,e_4/2-15\,d_2\,a_2/2-40\,a_4-5\,a_2^2/2;\\
&if\quad h_1=0\quad then\quad u_1 := h_2^{1/5};\quad u_4 := 0;\quad d := h_2\\
&\quad else\quad d := \sqrt{h_2^2-4\,h_1^5};\quad u_1 := ((-h_2+d)/2)^{1/5};\quad u_4 := h_1/u_1;\quad fi;\\
&\omega := (\sqrt{-2\sqrt{5}-10}+\sqrt{5}-1)/4;\\
&u_2 := (h_4\,u_1^2-h_3\,u_4^3)/d;\quad u_3 := (h_3\,u_1^3-h_4\,u_4^2)/d;\\
&result :=\\
&\quad -t+(u_1+u_2+u_3+u_4)/5,\\
&\quad -t+(\omega\,u_1+\omega^2\,u_2+\omega^3\,u_3+\omega^4\,u_4)/5,\quad -t+(\omega^2\,u_1+\omega^4\,u_2+\omega\,u_3+\omega^3\,u_4)/5,\\
&\quad -t+(\omega^3\,u_1+\omega\,u_2+\omega^4\,u_3+\omega^2\,u_4)/5,\quad -t+(\omega^4\,u_1+\omega^3\,u_2+\omega^2\,u_3+\omega\,u_4)/5\\
&end;
\end{aligned}
$$

Remark 6. The length of this complete program has to be compared with the three pages length formula of Lazard (2004). On the other hand, more square roots appear apparently in our new formula than in the one of Lazard (2004). In fact $\sqrt{D}$ and $\sqrt{5}$ appear both in factor of the d_i. Thus if they are replaced by $\sqrt{5D}$, the final expression of the roots contains exactly the same square roots as in Lazard (2004).

V. Septics

For solving septics, we consider the minimal polynomial of the sums of three different roots, which is of degree 35. It is shown in Bruen et al. (1986) (Theorem II.3.2) that the factorization of this polynomial allows to determine the Galois group.

Proposition 7. *The minimal polynomial of the sum of three roots is irreducible if the Galois group is either the alternate or the symmetric group. It has two irre- ducible factors of degrees 7 and 28 in the case of the non solvable group of order 168, two irreducible factors of degrees 14 and 21 in the case of the solvable group of order 42, three irreducible factors, one of degrees 21 and two of degree 7 in case of the solvable group of order 21, four irreducible factors, one of degree 14 and three of degree 7 in case of the dihedral group of order 14 and five irreducible factors of degree 7 in the case of the cyclic group of order seven.*

To explain how this result may be used in solving, we have to look inside its proof, which will be done in next subsection.

5.1 Generic septic

Let $x_0, \ldots, x_6$ be the seven roots of a generic septic.

The circular permutation σ defined in Section 2 acts on the sum of three roots. There are five orbits under this action, generated respectively by $x_0+x_1+x_3$, $x_0+x_2+x_3$, $x_0+x_1+x_6$, $x_0+x_2+x_5$ *and* $x_0+x_3+x_4$. Let us denote $\mathcal{O}_1, \ldots, \mathcal{O}_5$ these orbits, numbered in that order. The permutation $: x_i \to x_{5i}$ exchanges $\mathcal{O}_1$

and $\mathcal{O}_2$ and permutes circularly the three other orbits. As each solvable group is generated by σ and a power of , the part of Proposition 7 devoted to solvable groups deduce easily.

Let $F_i = \prod_{x+y+z \in \mathcal{O}_i}(s-(x+y+z))$, for $i = 1, 2$. As $\mathcal{O}_1$ and $\mathcal{O}_2$ are fixed by γ^2, the coefficients of the powers of s in F1 and F2 are invariants of the solvable group of order 21. Like for quintic, we want to use these invariants to express the solution. Unfortunately we do not have yet enough invariants, and we have to introduce other septics which are invariant for the same group.

The first such septic is the polynomial F_3 whose roots are the elements of the orbit of $x_1+x_2+x_4-(x_3+x_5+x_6)$ (difference of an element of $\mathcal{O}_1$ and an element of $\mathcal{O}_2$ which have no root in common). This polynomial do not give sufficiently many new invariants. In fact, it will be useful only in some special cases.

Recall that we denote by $u_0, \ldots, u_6$ the Fourier transform of the x_i and that the image of ui by σ is u_i/ω^i. With our choice of γ, we have $\gamma(u_i) = u_{3i}$ and $\gamma^2(u_i) = u_{2i}$ (indexes defined modulo 7). It follows easily that $\gamma^2(\sigma(u_i)) = \sigma^4(\gamma^2(u_i))$ which means that the orbit of $u_1+u_2+u_4$ (resp. $u_3+u_5+u_6$) is left invariant by the action of γ^2. Thus the septics G_1 and G_2 which have these orbits as roots are invariant by the group of order 21.

At this point the solving strategy becomes clear:

Firstly, given a solvable septic f defined on a field K, compute the septics f_1, f_2, f_3, g_1 and g_2 which are the specialization of F_1, F_2, F_3, G_1 and G_2. As these septics are not invariant under the maximal solvable group, these computations will be done over $K(\sqrt{D})$ the extension of the field of the coefficients of f by the square root of the discriminant D of f. On this field, the Galois group of f is included in the group of 21 elements and the coefficients of f_1, f_2, f_3 are thus rational. As the definition of g_1 and g_2 involve the seventh roots of unit, g_1 and g_2 are rational on $K(\sqrt{D}, \omega)$. In fact we will see that the coefficients of f_1+f_2, $(f_1+f_2)\sqrt{D}$, $f_3\sqrt{D}$ belong to K while those of g_1 and g_2 belong to $K(\sqrt{-7D})$.

Secondly, design some polynomials in the u_i which are invariants under the action of this group, express them as functions of the coefficients of $f_1, \ldots$ and use these expressions to compute the u_i.

5.2 Computing invariant septics f_1 and f_2

From now on, we consider a solvable septic f whose coefficients belong to a field K of characteristic different from 2, 3, 7. W.l.o.g. we suppose that that it is in depressed form, that is its coefficient of degree 6 is null. This implies that $u_0 = 0$.

To compute f_1 and f_2, we use Proposition 7. Thus we factorize the minimal polynomial of the sum of three roots, whose computation has been described in Section 3.2.

If the Galois group has the order 21, there are two factors of degree 7 which are f_1 and f_2. It does not matter which is named f_1, because they are exchanged if we replace σ by σ^{-1} when numbering the roots.

If the polynomial of degree 35 has a factor of degree 14 (group of order 14 or 42), we factorize it over the field $K(\sqrt{D})$ where D is the discriminant of f. This gives two factors of degree 7 which are f_1 and f_2.

It remains the case of the cyclic group where there are 5 factors of degree 7. One has to decide which are the specialization of f_1 and f_2. For this we use the following property of above defined orbits $\mathcal{O}_i$.

Lemma 8. *Given any element* s *of $\mathcal{O}_1$ or $\mathcal{O}_2$, there exists in each other orbit exactly one element which has not root in common with s.*

Given an element s of $\mathcal{O}_3$, $\mathcal{O}_4$ or $\mathcal{O}_5$ and another orbit $\mathcal{O}_j$, there exist an element $t \in \mathcal{O}_j$ with no root in common with s if and only if j = 1 or 2. In this case there is exactly one such element.

Proof. By cases enumeration.

Proposition 9. *Let* f *an irreducible septic in depressed form, and h_1 and h_2 be two different factors of degree 7 of the minimal polynomial of degree 35 of the sum of three roots of f. Then a root s_1 of h_1 and a root s_2 of h_2 have a root of f as common summand if and only if $f(-s_1-s_2) \neq 0$.*

If the system $h_1(s_1) = h_2(s_2) = f(-s_1-s_2) = 0$ has a solution, then it has exactly 7 solutions

Proof. If s_1 and s_2 have no root of f as a common summand, then s_1 and s_2 involve 6 different roots of f. As the sum of the seven roots of f is null, we have thus $f(-s_1-s_2) = 0$.

If (s_1, s_2) is solution *of* $h_1(s_1) = h_2(s_2) = f(-s_1-s_2) = 0$, we obtain immediately six other solutions by permuting circularly the roots of f. If $-s_1-s_2$ is a root x of f, this defines a linear relation $c_0x_0 + \cdots + c_6x_6 = 0$ between the roots of f, with non negative integer coefficients. As the Galois group of f contains a circular permutation of the roots, the roots of f are in the kernel of the circulant matrix defined by the vector $(c_0, \ldots, c_6)$. As the eigenvalues of this matrix are $c_0+\omega^i c_1+\cdots+\omega^{6i}$ for $i = 0, \ldots, 6$ (where ω is a primitive seventh root of unit) the determinant of this matrix is null if and only if either $c_0 + \cdots + c_6 = 0$ (eigenvalue for $i = 0$) or if all the ci are equal (unique equation satisfied by a primitive root of unit). As the c_i are non negative, the first case is excluded, all the ci are equal to 1 and s_1 and s_2 have no root of f as a common summand.

Corollary 10. *Let f be a septic in depressed form whose Galois group is cyclic, and let h_i, i = 1, . . . ,* 5 *be the factors of degree 7 of the minimal polynomial f_{35} of the sum of three roots. Let R(t) be the resultant with respect to* s *of $f(-s-t)$ and $h_1(s)$.*

• If the remainder of the Euclidean division of R(t) by $h_i(t)$ is null for i = 2, 3, 4 then the roots of h_1 belong to one of the orbits $\mathcal{O}_1$ or $\mathcal{O}_2$

• If the remainder of the division of R(t) by $h_i(t)$ is null for exactly two i in {2, 3, 4} *then the roots of the two corresponding h_i belong to the orbits $\mathcal{O}_1$ and $\mathcal{O}_2$.*

• If the remainder of the division of R(t) by $h_i(t)$ is null for exactly one i in {2, 3, 4} *then the roots of h_5 and of this h_i belong to the orbits $\mathcal{O}_1$ and $\mathcal{O}_2$.*

Proof. This follows immediately from the preceding results, because the remainder is null if and only the system $f(-s-t) = h_1(s) = h_i(t) = 0$ has a solution (and thus seven).

Except in the first case, this corollary allows to choose the factors of f_{35} corresponding to $\mathcal{O}_1$ and $\mathcal{O}_2$. In the first case, the lacking orbit may be found by applying the corollary to h_2 instead of h_1

5.3 Other invariant septics

Having the invariants polynomials f_1 and f_2 whose roots are the orbits of $x_0+x_1+x_3$ and $x_0+x_2+x_3$, we may deduce several other septics which are also invariants by the group of 21 elements.

The first one is f_3 whose set of roots is the orbit of $x_1+x_2+x_5-(x_3+x_5+x_6)$. A root of f_3 is the difference of a root of f_1

(orbit $\mathcal{O}_1$) and a root of f_2 (orbit $\mathcal{O}_2$), with no common summand. It follows from Proposition 9 that, if t is such a root of f_3, then there exists s_1 and s_2 such $f_1(s_1) = f_2(s_2) = f(-s_1-s_2) = t-s_1+s_2 = 0$. Moreover s_1 and s_2 are unique if t is given and every t which belongs to a solution of this system is a root of f_3.

This shows that f_3 may be obtained by eliminating s_1 and s_2. There are several ways to do this elimination, the simplest one being the following.

Proposition 11. *The polynomial f_3 is the GCD of R_1 and R_2, where R_1 (resp. R_2) is the resultant of $f(x)$ and $f_1((t-x)/2)$ (resp. $f_2((-t-x)/2)$) with respect to x.*

Proof. It follows from Proposition 9 that t is a root of this GCD if and only if there is a root x of f, a root s_1 of f_1 and a root s_2 of f_2 such that $s_1 = (t-x)/2$ and $s_2 = (-t-x)/2$, that is $s_1 + s_2 = -x$ and $s_1 - s_2 = t$.

Remark 12. The computation implied by Proposition 11 may be viewed as an algorithm. It may also viewed as a formula, because a resultant or a GCD of fixed degree (here 7) are both polynomial in term of the coefficients of their arguments (for GCD, this follows from the subresultant theory).

To compute the invariant septics g_2 and g_3 which have, as roots, the orbits under the cyclic group of $u_1 + u_2 + u_4$ and $u_3 + u_5 + u_6$ respectively, we need a lemma.

Lemma 13. *If $u_0, \ldots, u_6$ is the Fourier transform of the roots $x_0, \ldots, x_6$ of an irreducible septic f, then there is a square root of -7 such that $u_1 + u_2 + u_4 - (u_3 + u_5 + u_6) = (x_1 + x_2 + x_4 - (x_3 + x_5 + x_6))\sqrt{-7}$.*

Proof. Expand and simplify the definition of the u_i.

This lemma is used in the following way. Let t_1, t_2, s_1, s_2 be the images under the action of σ^i, for some i, of, respectively, $u_1 + u_2 + u_4$, $u_3 + u_5 + u_6$, $x_1 + x_2 + x_4$ and $x_3 + x_5 + x_6$. By Lemma 13, there is a root x of f such the following relations are satisfied: $s_1 + s_2 + x = 0$, $t_1 + t_2 = 7x$, $t_1 - t_2 = (s_1 - s_2)\sqrt{-7}$, $f(x) = 0$, $f_1(s_1) = 0$ and $f_2(s_2) = 0$. Using the three linear equations to eliminate, say, s_1, s_2 and x, we get three equations of degree 7 in t_1 and t_2. Thus like for computing f_3, we get the minimal polynomials of g_1 and g_2 as a GCD of resultants, Proposition 9 implying that this GCD is exactly of degree 7.

However, this way of computing g_1 and g_2 is not efficient. In fact it implies generally to compute in $K(\sqrt{D},\sqrt{-7})$, which is an extension of degree 4. We present a way for doing this elimination, which takes advantage of the symmetry of the problem to work on the smaller extension $K(\sqrt{-7D})$.

The basic remark is that, if the discriminant D is not a square, then f_1 and f_2 are conjugate, i.e. they are exchanged if one change the sign of $\sqrt{D}$. It follows that, if f_1 and f_2 are monic (which is obtained by dividing them by their leading coefficient), then $f_+(s_1, s_2) = f_1(s_1) + f_2(s_2)$ and $f_-(s_1, s_2) = (f_1(s_1) - f_2(s_2))\sqrt{D}$ are bivariate polynomials whose part depending on $\sqrt{D}$ is antisymmetric in s_1 and s_2, i.e. is a multiple of $s_1 - s_2$, while the part independent of $\sqrt{D}$ is symmetric.

This suggest to use f_+ and f_- for the elimination, that is, to compute g_1 (resp. g_2) as the GCD of the resultants with respect to t_2 (resp. t_1) of $f((t1 + t2)/7)$ and $f_\pm(-\frac{t_1+t_2}{14} + \frac{t_1-t_2}{2\sqrt{-7}}, -\frac{t_1+t_2}{14} - \frac{t_1-t_2}{2\sqrt{-7}})$, where $f_\pm$ is f_+ for the first resultant and f_- for the second.

With this way to proceed the elimination, the polynomials involved in the resultant computation have their coefficients in the extension of the base field by $\sqrt{-7D}$. It is useful to remark that this may also be obtained by replacing $\sqrt{-D}$ by $\sqrt{-7}$ in the definition of f_-. This has the advantage to have smaller coefficients if D is large.

It should be noted that the computation of g_1 and g_2 is a critical step in the computation of the roots: On typical examples, one needs around 30 seconds to compute the roots with an elimination starting from f_1 and f_2, while only 3 seconds are needed with the elimination starting from f_+ and f_-.

5.4 Computing u_1, u_2, u_4

Let $g_1 = t^7 + b_3 t^4 + b_4 t^3 + b_5 t^2 + b_6 t + b_7$ be the polynomial computed in the preceding section, which has, as roots, $u_1+u_2+u_4$ and its images under the action of the powers of σ. The fact that the coefficients of degree 5 and 6 are null is a consequence of the nullity of the sum of the roots of f. This may be proved by computing g_1 in the case of the generic polynomial $\Pi^6_{i=0}(x - x_i)$.

The b_i are invariants of the group of 21 elements. It appears that every invariant of this group, which is constructed from u_1, u_2, u_4, may be expressed in term of the b_i. [3] In fact, the method of Section 2.1 shows [3] This has not been proved, but it is true for all invariants we have constructed from

$$u_1 u_2 u_4 = -b_3/14 \tag{6}$$
$$u_1 u_2^3 + u_2 u_4^3 + u_4 u_1^3 = -b_4/7 \tag{7}$$
$$u_1^3 u_2^2 + u_2^3 u_4^2 + u_4^3 u_1^2 = -b_5/14 \tag{8}$$
$$u_1^5 u_2 + u_2^5 u_4 + u_4^5 u_1 = -b_6/7 - b_3^2/196 \tag{9}$$
$$u_1^7 + u_2^7 + u_4^7 = -b_7 - b_3 b_4/14 \tag{10}$$

This system of equation allows to compute u_1, u_2 and u_4. Before proceeding further, let us first remark that u_1, u_2 and u_4 may be arbitrarily permuted circularly: this amounts to use σ^2 instead of σ to label the roots. Similarly, u_1, u_2, u_4 and u_3, u_5, u_6 may be exchanged. This is equivalent to exchange f1 and f2 and thus also g1 and g_2. This amounts to replace σ by σ^3 to label the roots.

This system of equations allows to compute u_1 and to express rationally u_2 and u_4 in term of u_1. However several cases have to be considered.

If $b_3 = 0$, one of u_1, u_2, u_4 is null. As we have choice for labeling the u_i, we chose $u_4 = 0$, and Equations 7, 8, 9 become $u_1u_2^3 = -b_4/7$, $u_1^3u_2^2 = -b_5/14$, $u_1^5u_2 = -b_6/7$. Thus either $b_4 = b_5 = b_6 = 0$, another ui is null and the last one is given by Equation 10 or none of b_4, b_5, b_6 is null and u_1 and u_2 are not null and may be computed from Equation 7, 8 only.

Thus the different cases are the following ones.

- $b_3 = b_4 = b_7 = 0$. This implies $b_5 = b_6 = 0$ and $u_1 = u_2 = u_4 = 0$. This does not allow to express u_3, u_5, u_6 in term of u_1. Thus, in this case we exchange f_1 and f_2 and also g_1 and g_2. After this exchange we are no more in this case: if we were, all the u_i and thus all the roots of the septic would be equal to 0.
- $b_3 = b_4 = 0$, $b_7 \neq 0$.We choose $u_2 = u_4 = 0$ and Equation 10 gives $u_1 = -\sqrt[7]{b_7}$.
- $b_3 = 0$, $b_4 \neq 0$. We choose $u_4 = 0$. Thus u_1 and u_2 are not null. It is easy to deduce from Equations 7, 8 and 9 that $u_1 = \sqrt[7]{\frac{-b_5 b_6}{14 b_4}}$ and $u_2 = \frac{2u_1^2 b_4}{b_5}$. [4]

• $b_3 \neq 0$. This general case needs more attention than the preceding ones and will be detailed in the next paragraphs.

The elementary symmetric functions in u_1^7, u_2^7 and u_4^7 are invariant under the action of the group of order 21, and are function of the bi. The sum and the product have already be computed as Equations 10 and 6. The last elementary symmetric function $u_1^7u_2^7 + u_2^7u_4^7 + u_4^7u_1^7$ may be computed by the method of Section 2.1. This allows to express u_1 as the seventh root of a root of a cubic polynomial, but does not allows to express rationally u_2 and u_4 in term of u_1. Therefore we use another method to solve Equations 6 to 10.

As we have supposed $u_3 \neq 0$, Equation 6 may be solved in u4 and its solution may

u_1, u_2, u_4.

[4] There several possible formulas.These seem among the simplest ones.

be substituted in Equations 7 to 10 to get four polynomial equations in u_1, u_2 and the b_i.

The Grobner basis of this system, for the total degree ordering, may be computed in MAPLE with the option method=*fgb* in about 15 second and contains 474 polynomials, too much for our purpose. However, if we add the equation t $b_3 - 1 = 0$ to confirm that $b_3 \neq 0$, then the Grobner basis eliminating t is computed in 1.5 seconds and contains 154 polynomials which are independent of t. Starting from it, a Grobner basis for an ordering eliminating u_2 (in MAPLE, *lexdeg*($[u_2]$, $[u_1, b_7, b_6, b_5, b_4, b_3]$), *method=fgb*) gives three relations between the b_i, a polynomial of degree 3 in u_1^7 with coefficients depending on the bi and many polynomials which are linear in u_2. Among them the fifteenth has the lower degree in u_1 and has the shape $Au_2 + Bu_1^2$ where A and B are linear polynomials in u_1^7 with coefficients depending on the b_i.

These polynomials may be simplified by replacing them by their normal form by the Grobner basis of the relations between the b_i for the lexicographical ordering such $b_7 > b_6 > b_5 > b_4 > b_3$. The resulting relations are

$$u_1 = \sqrt[7]{U_1} \tag{11}$$

$$0 = U_1^3 + (b_7 + \frac{b_3 b_4}{14})U_1^2 + (-\frac{b_5^2 b_4}{14^2 7} - \frac{b_4^2 b_3^2}{14^2 49} + \frac{b_6 b_5 b_3}{14^2 7} - \frac{b_5 b_3^3}{14^4})U_1 + (\frac{b_3}{14})^7 \tag{12}$$

$$u_2 = -2u_1^2 \frac{14^3(7b_6b_5 + 2b_4^2b_3 - \frac{1}{2}b_5b_3^2)U_1 + A}{14^3(b_5b_4b_3 - 28b_6^2 - \frac{1}{14}b_3^4 - 4b_4^3)U_1 + B} \tag{13}$$

$$u_4 = \frac{-b_3}{14u_1u_2} \tag{14}$$

where

$$A = 28b_5b_4b_3^3 - 28b_4^3b_3^2 + 98b_5^3b_3 + b_3^6 + 196b_6b_5b_4b_3 - 196b_5^2b_4^2 + 7b_6b_3^4$$
$$B = b_4b_3^5 + 28b_6b_4b_3^3 - 28b_5b_4^2b_3^2 + 14b_5^2b_3^3.$$

Thus u_1 is the seventh root of a root of a cubic equation and u_2 and u_4 are expressed rationally in term of u_1 and the same root of this cubic equation. However, to avoid division by 0 we have to **define U_1 as a root of the quotient of the right hand side of Equation 12 by its GCD with the denominator in Equation 13**. This avoids a division by zero because we will shows that Equation 12 never has multiple roots.

Proposition 14. *The discriminant of Equation 12 is the square of*

$$\frac{b_5^2b_4^2b_3}{7^3 14^2} - \frac{b_5^3b_3^2}{14^5} - \frac{b_6b_5b_3^2b_4}{7^4 14} + \frac{b_3^7}{14^7} - \frac{b_4^4b_5}{7^4 14} - \frac{b_6b_5^3}{14^3 7} - \frac{b_3^3b_4^3}{14^2 7^4} + \frac{3b_5b_4b_3^4}{14^5 7} - \frac{b_6b_3^5}{14^4 7^2} + \frac{b_6b_4^3b_3}{7^4 14} \tag{15}$$

and is not null unless if $b_3 = b_4 = 0$.

It follows that, unless if $b_3 = b_4 = 0$, either Equation 12 has three distinct roots in $K(\sqrt{-7D})$ or its right hand side is irreducible with cyclic Galois group.

Proof. The discriminant of Equation 12 is the square of $(u_1^7 - u_2^7)(u_2^7 - u_4^7)(u_4^7 - u_1^7)$. To express this in term of the bi, we proceed as follows. First compute the Grobner basis G_1 of Equations 6 to 10 for an elimination ordering eliminating the u_i (1/3 second in MAPLE for the ordering *lexdeg*($[u_1, u_2, u_4]$, $[b_3, b_4, b_5, b_6, b_7]$, *method = fgb*) and the Grobner basis G_2 of the elements of G_1 which depend only on b_3, b_4, b_5, b_6, b_7, for the lexicographical ordering such that $b_7 > b_6 > b_5 > b_4 > b_3$. Then Polynomial 15 is obtained by taking the normal form by G_2 of the normal form by G_1 of $(u_1^7 - u_2^7)(u_2^7 - u_4^7)(u_4^7 - u_1^7)$.

Thus the discriminant of Equation 12 is a square in $K(\sqrt{-7D})$. This implies that, if it is irreducible, then its Galois group is cyclic. If the right hand side is factorized in a linear (in U_1) polynomial and a quadratic one, the quadratic one is not irreducible, because its discriminant is a square. In fact, the discriminant of a product is the product of the discriminants of the factors times the square of their resultants.

Thus it remains to prove that the discriminant is not null. Suppose that it is null. Then two roots are be equal, say $u_1^7 = u_2^7$, as permuting the indexes of the roots x_i permutes also the u_i. This double root is not null, as we have supposed that at most one of the ui is null. If ω is a primitive root of unit, we have thus $u_2 = \omega^i u_1$ for some i. Substituting this in Equation 6, solving it in u_4 and substituting the values of u_2 and u_4 in Equations 7 and 8 gives two equations of degree 9 in u_1 whose difference has degree 6. Thus u_1, and thus also u_2 and u_4 are in an extension L of degree at most 6 of $K(\sqrt{-7D})$.

We will prove in next section that either u_3, u_5, u_6 may be rationally expressed in term of u_1 or Equation 12 has a triple root. In the latter case we will prove that u_3, u_5 and u_6 belong to an extension of degree at most 6 of L. Thus, in both cases, all the u_i belong to an extension of K of degree prime to 7. The same is thus true for x_0 which is the quotient by 7 of the sum of the u_i, which proves that the input polynomial is not irreducible.

Corollary 15. *The root U_1 of Equation 12 belongs either to $K(\sqrt{-7D})$ or to an extension by a cubic root of $K(\sqrt{-3},\sqrt{-7D})$.*

Proof. The square root which appears in Cardano's formula for the roots of a cubic equation is the square root of the product of the discriminant, a square and −3.

5.5 Final computation of the roots

As the roots will be obtained by reverse Fourier transform of the u_i, for computing them we need to express u_3, u_5, u_6 rationally in term of u_1, u_2, u_4 and the invariants which have been already computed. For this purpose, we consider four invariants of the group of order 21, which may be expressed in term of the coefficients of f, f_1, f_2, f_3, g_1, g_2, using the method of Section 2.1.

Among these polynomials, f has its coefficients in K, g_1 and g_2 have their coefficients in $K(\sqrt{-7D})$, but the other ones have coefficients in $K(\sqrt{D})$. Thus we will consider $f^+ = f_1 + f_2$, which has its coefficients in K and $f^- = (f_1 - f_2)\sqrt{-7}$ which is the product by $\sqrt{(-7D)}$ of a septic with coefficients in K. We will denote by a_i (resp. b_i, c_i, d_i^+, d_i^-) the coefficient of degree 7−i of f (resp. g_1, g_2, f^+, f^-).

The roots of the septic f_3 are the elements of the orbit under the cyclic group of $x_1 + x_2 + x_4 - x_3 - x_5 - x_6$. Thus it changes of sign when one changes in it the signs both the variable and $\sqrt{D}$. Thus its coefficients of even degree are the product of an element of K by $\sqrt{D}$. We need only the product by $\sqrt{-7}$ of its coefficient of degree 2 which is thus in $K(\sqrt{-7D})$ and will be denoted by e_5. With these notations we get the following relations which are linear in u_3, u_5, u_6.

$$u_1u_6 + u_2u_5 + u_4u_3 = -7a_2 \tag{16}$$

$$u_4^2u_6 + u_1^2u_5 + u_2^2u_3 = -\frac{1}{14}b_3 + \frac{21}{4}d_3^+ - \frac{7}{4}d_3^- - 14a_3 \tag{17}$$

$$u_4u_2^2u_6 + u_1u_4^2u_5 + u_2u_1^2u_3 = \frac{1}{21}c_4 - \frac{1}{42}b_4 + \frac{49}{12}d_4^+ + \frac{49}{12}d_4^- - \frac{98}{3}a_4 \tag{18}$$

$$u_1^4u_3 + u_2^4u_6 + u_4^4u_5 = 7e_5 - \frac{1}{7}c_5 - \frac{3}{14}b_5 - \frac{343}{4}d_5^+ - \frac{343}{4}d_5^- + b_3a_2 - 343a_5 \tag{19}$$

Thus, if the determinant of the coefficients of u_3, u_5, u_6 in three of these equations is not null, then by solving this linear system, one gets a rational expression of u_3, u_5, u_6 in term of u_1, u_2, u_4.

These four determinants are invariant under the action of the group of order 21. Thus, using the method of the proof of Proposition 14, we may express them in term of the b_i:

$$\det(16,17,18) = -\frac{1}{7}b_6 - \frac{1}{49}b_3^2$$

$$\det(16,17,19) = -b_7 - \frac{4}{49}b_3b_4$$

$$\det(16,18,19) = -\frac{1}{49}b_4^2 - \frac{3}{196}b_3b_5$$

$$\det(17,18,19) = -\frac{1}{2744}b_3^3 + \frac{1}{98}b_4b_5 - \frac{1}{49}b_3b_5$$

It follows that if $b_3 = b_6 = 0$ one gets u_3, u_5, u_6 by solving Equations 16, 17, 19. If $b_3 = 0$, $b_6 \neq 0$, the first three equations give the result. If $b_3 \neq 0$, we will shows that the determinant of either Equations 16, 17, 18 or Equations 16, 18, 19 is not null.

Lemma 16. *If $b_3 \neq 0$ and the determinants* det(16, 17, 18) *and* det(16, 18, 19) *are both null, then $u_1^7 = u_2^7 = u_4^7$*

Proof. Let us consider the Grobner basis of the relations between the b_i, named G_2 in the proof of Proposition 14. The hypotheses is that we have three more relations $7b_6 + b_3^2 = 0$, $4b_4^2 + 3b_3b_5 = 0$ *and* $b_3v - 1 = 0$, the latter, which introduces a new variable, implying that $b_3 \neq 0$. Adding to G_2 the left hand sides of these relation, let G_3 be the Grobner basis the lexicographical ordering $v > b_7 > b_6 > b_5 > b_4 > b_3$. The first element of G_3 is the square of $112b_4^3 + 27b_3^4$. Let G_4 be the Grobner basis for the same ordering of the ideal which is obtained by adding this polynomial to G_4. This Grobner basis consists in 8 binomials.

Now, let us consider Equation 12, which has u_1^7, u_2^7 and u_4^7 as roots. It has the shape $U_1^3 + AU_1^2 + BU_1 + C$ where A,B,C are polynomials in the b_i. Its three roots are equal if and only if $3B - A^2$ and $27C - A^3$ are both null. As the normal forms by G_4 of these two polynomials is null the lemma is proved.

We are now ready to finish the proof of Proposition 14.

Proposition 17. *If the discriminant of Equation 12 is null and $b_3 \neq 0$, then the input septic is reducible.*

Proof. We have already proved that u_1, u_2, u_4 belong to an extension of K of degree prime to 6. If Equation 12 has a double root and a simple one, we have just shown that u_3, u_5, u_6 may be expressed rationally in term of u_1, u_2, u_4, and belong to the same field. As x_0 is the quotient by 7 of the sum of all u_i it belongs also to this field and the input septic is not irreducible

If Equation 12 has a triple root, we need further work.

If $u_1^7 = u_2^7 = u_4^7 \neq 0$, there are seventh roots of unit ω_1 and ω_4 such that $x_2 = \omega_2 u_1$ and $x_2 = \omega_4 u_1$. Thus Equation 16 becomes $u6 + \omega_2 u_5 + \omega_4 u_3 = h_1$ for some h_1 belonging to the field containing u_1, u_2 and u_4. Similarly, the analogous of Equations 17 and 18 where u_1, u_2, u_4 and u_6, u_5, u_3 are exchanged, become $u_3^2 + \omega_2 u_6^2 + \omega_4 u_5^2 = h_2$ and $u_3u_5^2 + \omega_4 u_6u_5^2 + \omega_2 u_6u_3^2 = h_3$. Thus we have three equations in u_3, u_5, u_6 of degrees 1, 2, 3. B´ezout theorem asserts that, if the number of solutions in an algebraically closed extension is finite, then it is at most 6, and the solutions belong to an extension of the field containing h_1, h_2, h_3, ω_2 and ω_4 which of degree at most 6. Thus it remains to prove that the number of solutions is finite to get that all the ui, and thus x_0 belong to an extension of K of degree prime to 7, that is that f is not irreducible.

To prove that the number of solutions is finite, one may use the linear equation to eliminate u_6 and obtain two equations in u_3, u_5, ω_2, ω_4, h_1, h_2, h_3. Considering ω_2, ω_4, h_1, h_2, h_3 as indeterminates, their resultant with respect to u_5 is easy to compute. It is a polynomial of degree 6 in u_3 whose leading coefficient is a polynomial in ω_2 and ω_4, which do not vanishes if ω_2 and ω_4 are substituted by seventh roots of unit. This may be proved by computing a Grobner basis , reduced to 1, of the ideal generated by this leading coefficient, $\omega_2^7 - 1$ and $\omega_4^7 - 1$. This may also be proved by obtaining 1 as the GCD of $\omega_4^7 - 1$ and the resultant with respect to ω_2 of $\omega_2^7 - 1$ and this leading coefficient.

We have now finished to describe how to compute the u_i in term of radical. The roots may be deduced by computing the inverse Fourier transform and, if the term of degree 6 of the input septic was not null, adding the mean value of the roots, i.e. $-a_1/7$ a_0 where a_1 and a_0 are the coefficients of degree 6 and 7 of this input septic.

Remark 18. To solve the linear system in the u_3, u_5, u_6 the best way seems to use Cramer's rules, because we have a simple form of the determinant which is independent from the u_i.

Remark 19. The invariant septic f_3 is only used in Equation 19. Thus it is not needed except if $b_3 = b_4 = 0$ or $b_3^2 + 7\,b_6 = 0$. It is thus better to compute it at the end and only if needed.

5.6 Conclusion

In summary we have proved the following.

Theorem 20. *A root of a solvable irreducible septic of discriminant D defined on a field K of characteristic different from 2, 3, 7, may be computed as an element of either an extension of $K(\sqrt{-7D})$ by a seventh root or as an element an extension by a seventh root of an extension of $K(\sqrt{-3},\sqrt{-7D})$ by a cubic root. The other roots belong to the extension of the preceding by a primitive seventh of unit, which belongs to an extension of $K(\sqrt{-3},\sqrt{-7})$ by a cubic root.*

This theorem is fully constructive, as we have described how to effectively compute the root. This procedure has been implemented and tested on various examples for all the cases which are considered in the algorithm. The typical time of computation is about three seconds.

The correctness of the output has been verified by substituting the roots in the input polynomial and either evaluating numerically the result to zero (floating point with a precision of 30 decimal digits) or simplifying it to 0 with MAPLE's instruction evala(convert(expression, RootOf)).

For saving space, we do not give explicitly the algorithm, but as its description is split on various sections, we summarize it as follows.

Starting from an irreducible septic,
Apply the Tschirnaus transformation $x -> x - T$ *to get a depressed septic.*
Compute the polynomial of degree 35 of the sums of three roots (Section 3.2).
Factorize it to test solvability and compute septics f_1 *and* f_2 *(Section 5.2).*
Compute the invariant septics g_1 *and* g_2 *(Section 5.3).*
If $g_1 = t^7$ *then exchange* f_1, g_1 *with* f_2, g_2.
$b_i := \text{coeff}(g_1, t, 7-i)$ *for* $i = 3, \ldots, 7$.
If $b_3 = b_4 = 0$ *then*
  $u_1 := -\sqrt[7]{b_7},\ u_2 := 0,\ u_4 = 0.$
  Compute the polynomial f_3 *(Section 5.3)*
  Compute u_3, u_5, u_6 *by Cramer's rules from Equations 16, 17, 19,*
If $b_3 = 0,\ b_4 \neq 0$ *then*
  $u_1 := \sqrt[7]{\frac{-b_5\,b_6}{14\,b_4}},\ u_2 := \frac{2\,u_1^2\,b_4}{b_5},\ u_4 := 0$
  Compute u_3, u_5, u_6 *by Cramer's rules from Equations 16, 17, 18,*
If $b_3 \neq 0$ *then*
  Use Equations 11 to 14 to define u_1, u_2, u_4, *choosing the root*
    in Equation 12 in order to avoid division by zero in Equation 13
  If $7\,b_6 + 49\,b_3^2 \neq 0$
    then compute u_3, u_5, u_6 *by Cramer's rules from Equations 16, 17, 18,*
    else
      Compute the polynomial f_3 *(Section 5.3)*
      Compute u_3, u_5, u_6 *by Cramer's rules from Equations 16, 18, 19.*
$\omega :=$ *the expression by radicals of a primitive 7th root of unit.*
The roots are

$$-T + \frac{u_1+u_2+u_3+u_4+u_5+u_6}{7},$$
$$-T + \frac{\omega\,u_1+\omega^2\,u_2+\omega^3\,u_3+\omega^4\,u_4+\omega^5\,u_5+\omega^8\,u_6}{7},\quad -T + \frac{\omega^2\,u_1+\omega^4\,u_2+\omega^6\,u_3+\omega\,u_4+\omega^3\,u_5+\omega^5\,u_6}{7},$$
$$-T + \frac{\omega^3\,u_1+\omega^6\,u_2+\omega^2\,u_3+\omega^5\,u_4+\omega\,u_5+\omega^4\,u_6}{7},\quad -T + \frac{\omega^4\,u_1+\omega\,u_2+\omega^5\,u_3+\omega^2\,u_4+\omega^6\,u_5+\omega^3\,u_6}{7},$$
$$-T + \frac{\omega^5\,u_1+\omega^3\,u_2+\omega\,u_3+\omega^6\,u_4+\omega^4\,u_5+\omega^2\,u_6}{7},\quad -T + \frac{\omega^6\,u_1+\omega^5\,u_2+\omega^4\,u_3+\omega^3\,u_4+\omega^2\,u_5+\omega\,u_6}{7}.$$

REFERENCES

[1] Bruen, A. A., Jensen, C. U., Yui, N., 1986. Polynomials with Frobenius groups of prime degree as Galois groups. II. J. Number Theory 24 (3), 305–359.

[2] Dummit, D. S., 1991. Solving solvable quintics. Math. Comp. 57 (195), 387–401.

[3] Geissler, K., Kluners, J., 2000. Galois group computation for rational polynomials.

[4] J. Symbolic Comput. 30 (6), 653–674, algorithmic methods in Galois theory.

[5] Hagedorn, T. R., 2000. General formulas for solving solvable sextic equations. J. Algebra 233 (2), 704–757.

[6] Landau, S., Miller, G. L., 1985. Solvability by radicals is in polynomial time. J. Comput. System Sci. 30 (2), 179–208.

[7] Lavallee, M. J., Spearman, B. K., Williams, K. S., 2005. Watson's method of solving a quintic equation. JP J. Algebra Number Theory Appl. 5 (1), 49–73.

[8] Lazard, D., 2004. Solving quintics by radicals. In: The legacy of Niels Henrik Abel. Springer, Berlin, pp. 207–225.

[9] Paxton Young, G., 1888. Solvable quintic equations with commensurable coefficients. Amer. Journal of Math. 10, 99–130.

AUTHORS

First Author – Mohammed A. Faggal, National Grid, Dammam, Saudi Arabia, Email: MAFaggal@ngrid.sa
Second Author – Daniel Lazard, UPMC Univ Paris 06, LIP6, F-75005, Paris, France, INRIA Paris-Rocquencourt, SALSA project team, F-78153 Le Chesnay, France, CNRS, LIP6, F-75005, Paris, France, Email: Daniel.Lazard@lip6.fr