Solving Quintics by Radicals

D. Lazard*
LIP6, Université P. et M. Curie, boite 168,
4 place Jussieu, 75252 Paris Cedex 05, France

November 7, 1997

Abstract

A formula is given for solving by radicals polynomials of degree 5 which are solvable by radicals. This formula is valid on any field of characteristic different from 2 and 5. It is implemented in Maple.

1 Introduction

Since Galois, it is well known that an equation is soluble by radicals iff its Galois group is soluble. This can be tested by looking if some auxiliary equation (resolvent) has a linear simple factor.

In the case of degree 5, Cayley has computed such a resolvent (called R_θ in this paper) which never has multiple factor. Thus, for testing if a fifth degree equation is soluble by radicals, it suffices to write Cayley's resolvent in a computer and to call the factorization package of any Computer Algebra system.

If the equation is soluble by radicals, it remains to explicitly write down the solution. When we began to write this paper we did not know any previous work on this subject for degree bigger than 4. François Morain bring our attention on [PY1888], where a method is given for solving quintics.

The aim of this paper is to provide a formula for the degree 5. It differs from [PY1888] method in several ways. A first but minor difference lies in the fact that he expresses the root as a sum of four fifth roots. Without specifying which determination of the roots have to be chosen, this gives 20 solutions, i.e. 15 in excess. This is a minor difference because it may be easily corrected from Paxton Young paper itself.

The second difference lies in genericity. In [PY1888] several cases are considered, depending on the values of the coefficients. In our formula the only branching instructions consist in choosing (twice) the sign of a square root in order to avoid that some denominators become zero. This means that our implementation in Maple is really a formula: Except these two

*E-mail: Daniel.Lazard@lip6.fr

choices of signs, the only operation which=h are involved are: $+$, $-$, $*$, $/$ and root extraction (one fifth, two square roots and the computation of the rational root of a polynomial degree 6). This means that our formula applies (in principle) also with symbolic coefficients. However testing equality with 0 for an algebraic expression depending of symbols is a difficult task; this has the consequence that our Maple program may provide a false answer in symbolic case, because of bad detection of zero.

A third difference is that our method may apply to any field of coefficients of characteristic different from 2 and 5. We have not verified if this is also true for Paxton-Young one.

A fourth difference, the most important in our opinion, is that our formula is presented in a systematic way, without ad hoc computational tricks. Thus, it would be possible, in theory, to extend it to degree 7 for example. However this would lead to horrific computations (The degree 6 resolvent for degree 5 should be replaced by a resolvent of degree 120).

Even for degree 5 the size of our formula shows that solving by radicals is the worst method, even when possible. In our opinion this is the main conclusion of our paper.

Finally, we prove that our formula is optimal in following sense : The field extension defined by the radicals appearing in our formula is always the smallest radical extension containing one root (resp. all the roots.

2 Notations and basic facts of Galois theory

In all this paper, we consider a base field $\mathbf{Q}$ of characteristic different from 2 and 5, which may be thinked of as the field of the rationals, but may be any other field.

We consider also a univariate *irreducible* polynomial f of degree d over $\mathbf{Q}$ which one wants to solve by radicals (in most of the paper, we will have $d = 5$). The *Galois group* $\mathcal{G}$ of f is the Galois group over $\mathbf{Q}$ of the field generated by all the roots of f.

The main result of Galois may be rephrased as : *"A polynomial is solvable by radicals iff its Galois group is solvable"*, a group $\mathcal{G}$ being *solvable* iff it contains a tower of subgroups $\{e\} = \mathcal{G}_0 \subset \mathcal{G}_1 \subset \cdots \subset \mathcal{G}_k = \mathcal{G}$ such each $\mathcal{G}_i$ is a normal subgroup of $\mathcal{G}_{i+1}$ and that each $\mathcal{G}_{i+1}/\mathcal{G}_i$ is an Abelian group.

To be more precise, we introduce d variables $x_0, \ldots, x_{d-1}$, corresponding to the d roots of f. The symmetric group $\mathcal{S}_d$ acts on the x_i and, by this action, the Galois group $\mathcal{G}$ of f is a subgroup of $\mathcal{S}_d$.

For simplification of notations, most indices will be assumed to be integers modulo d; this will be always the case when, other-way, the expression in which the index appears would not be defined. For example, $x_d = x_0$ and $x_{d+1} = x_1$

For solving by radicals, we will consider some polynomials in the x_i and we will use their invariance under some subgroup of the Galois group for expressing their values in term of the elementary symmetric functions, i.e. the coefficients of f.

The basic such polynomials are

$$s_0 = x_0 + x_1 + \cdots + x_{d-1} = \sum_{i=0}^{d-1} x_i$$

$$
\begin{aligned}
s_1 &= x_0 + \omega x_1 + \cdots + \omega^{d-1} x_{d-1} = \sum_{i=0}^{d-1} \omega^i x_i \\
s_k &= x_0 + \omega^k x_1 + \cdots + \omega^{k(d-1)} x_{k(d-1)} = \sum_{i=0}^{d-1} \omega^{ik} x_i \qquad \text{for } k = 2, \dots d-1
\end{aligned}
$$

where ω is a primitive d-th root of unity.

It is important to notice that the cyclic permutation $x_i \to x_{i-1}$ has the same action on the s_k as the multiplication by ω^k. Similarly, for a prime to d, the permutation $x_i \to x_{i/a}$ and the substitution $\omega \to \omega^a$ induce on the s_k the permutation $s_k \to s_{ak}$ (let us recall that indices are integer modulo d).

It follows that $S_1 := s_1^d$ and $S_k := s_k s_1^{d-k}$ are invariant under cyclic permutations of the indices. Solving the equation f is now reduced to compute the values of the S_k when the x_i are substituted by the roots of f. In fact, s_0 is easily expressed in term of the coefficients of f, and

$$
\begin{aligned}
s_1 &= \sqrt[d]{S_1} \\
s_k &= S_k / s_1^{d-k} \qquad \text{for } k > 1 \\
x_0 &= \frac{1}{d} \sum_{k=0}^{d-1} s_k \\
x_i &= \frac{1}{d} \sum_{k=0}^{d-1} \omega^{-ik} s_k \qquad \text{for } i > 0
\end{aligned}
$$

Notation. We denote by $\mathcal{S}_d$ the symmetric group of order d and by $\mathcal{C}_d$ the cyclic group of order d generated by the permutation $i \to i+1 \bmod d$. When d is fixed we will simply write $\mathcal{S}$ and $\mathcal{C}$. As we shall encounter many polynomials which, like the S_i, are invariant under the action of some group, we will need the following abbreviations. For any polynomial p in the x_i and any subgroup $\mathcal{G}$ of the symmetric group $\mathcal{S}_d$, we will denote by $\sum_{\mathcal{G}} p$ the sum of the polynomials of the orbit of p under $\mathcal{G}$. Thus for $d = 3$, we have

$$
\begin{aligned}
\sum_{\mathcal{C}} x_0 x_1^2 &= x_0 x_1^2 + x_1^2 x_2 + x_2 x_0^2 \\
\sum_{\mathcal{S}} x_0 x_1^2 &= \sum_{\mathcal{C}} x_0 x_1 (x_0 + x_1) = x_0 x_1^2 + x_1^2 x_2 + x_2 x_0^2 + x_0^2 x_1 + x_1^2 x_2 + x_2^2 x_0
\end{aligned}
$$

3 Invariants and Resolvents

It follows from last Section that solving by radicals reduces to compute the value of some polynomials invariant by some subgroup of the symmetric group (here by the cyclic group). This computation will be done by expressing them in term of elementary symmetric polynomials, i.e. in term of the coefficients of f. The main tool for this computation is the notion of resolvent.

As we are working with polynomials in d variables over $\mathbf{Q}$, let us set $R_d := \mathbf{Q}[x_1, \dots x_d]$, the ring of polynomials and $K_d := \mathbf{Q}(x_1, \dots x_d)$, the field of rational functions. For a subgroup $\mathcal{G}$ of $\mathcal{S}_d$, we denote by $R_d^{\mathcal{G}}$ the sub-ring of R_d consisting of the polynomials which are invariant under the action of $\mathcal{G}$, acting by permutation of the indices. Similarly $K_d^{\mathcal{G}}$ is the subfield of K_d of invariant rational functions.

It is well known that we have $R_d^{\mathcal{S}} = \mathbf{Q}[\sigma_1, \ldots, \sigma_d]$ and $K_d^{\mathcal{S}} = \mathbf{Q}(\sigma_1, \ldots, \sigma_d)$, where $\sigma_i = \sum_{\mathcal{S}} x_0 x_1 \cdots x_{i-1}$ is the i-th elementary symmetric function. This allows to express any symmetrical function of the roots of f in term of the coefficients of f.

Given two subgroups $\mathcal{G} \subset \mathcal{H}$ of $\mathcal{S}_d$, we call *resolvent invariant of* $\mathcal{G}$ *relatively to* $\mathcal{H}$ any element of $R_d^{\mathcal{G}}$ which generates the field extension $K_d^{\mathcal{G}}/K_d^{\mathcal{H}}$. We call *resolvent equation* or simply *resolvent* its minimal polynomial over $K_d^{\mathcal{H}}$. When $\mathcal{H}$ is not specified, it is assumed to be $\mathcal{S}_d$. If f is an univariate irreducible polynomial with a Galois group included in $\mathcal{H}$, a resolvent equation R becomes a polynomial in $\mathbf{Q}[X]$, by substituting the roots of f to the x_i. We denotes by R_f the result of this substitution. A resolvent R is said *separable* for f if R_f is square free. A resolvent is *always separable* if it is separable for all irreducible polynomials with Galois group included in $\mathcal{H}$.

For example, $\prod_{i<j}(x_i - x_j)$ is a resolvent invariant for the alternate group $\mathcal{A}_d$, and the corresponding resolvent is $x^2 - \Delta$ where Δ is the discriminant of the polynomial having the x_i as roots. This resolvent is always separable because f is never irreducible if its discriminant is null.

The interest of the resolvents is that they allow to test if a Galois group is contained in $\mathcal{G}$ and to express the polynomials invariant by $\mathcal{G}$ in term of a root of a polynomials with coefficients invariant by $\mathcal{H}$.

Theorem 1 *Let R be a resolvent of $\mathcal{G} \subset \mathcal{H}$ and f be a univariate polynomial of degree d.*

- *If the Galois group of f is included in $\mathcal{G}$, then R_f has a root in $\mathbf{Q}$.*
- *If R is separable for f and R_f has a root in $\mathbf{Q}$, then if the Galois group of f is included in $\mathcal{H}$, it is also included in G.*

We will need another theorem on invariants. Despite it is not new, we give a proof of it, because this proof will be used for our computations. This proof is based on Gröbner bases, for which we refer to [CLOS92].

Theorem 2 *Given a subgroup $\mathcal{G}$ of $\mathcal{S}_d$, the ring $R_d^{\mathcal{G}}$ is a free $R_d^{\mathcal{S}}$ module which has a base consisting in invariant homogeneous polynomials of degree at most $d(d-1)/2$*

Let us consider the elementary symmetric functions σ_i and let $e_1, \ldots, e_d$ be new indeterminates which will be viewed as "names" for the σ_i. We consider the ideal I in $\mathbf{Q}[x_0, \ldots, x_{d-1}, e_1, \ldots, e_d]$ generated by the $\sigma_i - e_i$. We will compute a Gröbner basis of I for any admissible ordering such that

- $x_0 < x_1 < \cdots < x_{d-1}$,
- $m_1 < m_2$ for any pair of monomials satisfying the same inequality for their total degrees in the x_i.

Lemma 1 *For such an ordering, a reduced Gröbner base of I is*

$$\begin{aligned} J &= \{x_0^d - e_1 x_0^{d-1} + \cdots + (-1)^{d-1} e_{d-1} x_0 + (-1)^d e_d, \\ &\quad C_{d-1}^{(2)} - e_1 C_{d-2}^{(2)} + \cdots + (-1)^{d-2} e_{d-2} C_1^{(2)} + (-1)^{d-1} e_{d-1}, \\ &\quad \ldots, \\ &\quad C_2^{(d-1)} - e_1 C_1^{(d-1)} + e_2, \\ &\quad C_1^{(d)} - e_1 = \sigma_1 - e_1\}, \end{aligned}$$

where $C_k^{(i)}$ is the sum of all monomials of degree k in $x_0, \ldots, x_{i-1}$.

Proof of the Lemma 1: The leading monomials of the polynomials in J are $x_0^d, x_1^{d-1}, \ldots, x_{d-1}$, which are pairwise coprime. It follows immediately that J is a reduced Gröbner base.

For showing that the $J \subset I$, it suffices to show that the elements of J become null when the e_i are replaced by the σ_i. Let J_i be the i-th element of J and $J_{i,k}$ be the result of the substitution of x_{i-1} by x_k in J_i. We prove that the $J_{i,k}$ for $k \geq i-1$ becomes null by the replacement of the e_j by the σ_j. This is clearly true for $i = 1$ and results by recursion from the formula $J_{i,k} - Ji = (x_k - x_{i-1}) J_{i+1,k}$ for $k \geq i$.

Finally, we have to prove that J generates I, i.e. that J is the complete Gröbner base of I. There are $n!$ monomials in the x_i which are irreducible by J. If J were not a Gröbner of I, there would be a polynomial in I, irreducible by J, and these $n!$ monomials would be linearly dependent over $\mathbf{Q}(\sigma_1, \ldots \sigma_d)$. This would be a contradiction to the fact of the Galois group of $\mathbf{Q}(x_1, \ldots x_d)$ over $\mathbf{Q}(\sigma_1, \ldots \sigma_d)$ is symmetric. $\diamondsuit$

Lemma 2 *Let $\mathcal{G}$ a sub-module of the symmetric group. The $\mathbf{Q}[e_1, \ldots e_d]$-module of the polynomials in the x_i which are invariant by $\mathcal{G}$ is generated by its elements such that their leading monomial after reduction by J is independent of the e_i.*

Proof: In Lemma 1, we have just specified the ordering on the monomial by being sharper than the partial ordering of the total degree in the x_i. We precise now the ordering by setting that monomials of the same total degree in the x_i are first compared by comparing their e_i part.

Let f be a polynomial invariant by $\mathcal{G}$ and g its normal form after reduction by J. Let E be the monomial in the e_i appearing in the leading term $\mathrm{lt}(g)$ of g and h be the homogeneous polynomial in the x_i such that hE is the part of g consisting in the monomials which are product of E by a monomial in the x_i of the same degree as $\mathrm{lt}(g)$. Above choice on the ordering implies that the monomials of g which are not in hE are lower than any monomial of hE, i.e. that hE is the beginning of g.

As g becomes invariant by $\mathcal{G}$ after substitution of the e_i by the σ_i, the polynomial $\sum_{\gamma \in \mathcal{G}} g^\gamma$, which is the sum of the orbit of g under $\mathcal{G}$ is reduced by J to $\mathrm{card}(\mathcal{G}) g$. Similarly, $H := \sum_{\gamma \in \mathcal{G}} h^\gamma$ is a polynomial invariant under $\mathcal{G}$. The reduction by J of both sums may be done in parallel, showing that H reduces to a polynomial with $\mathrm{card}(\mathcal{G}) h$ as leading part. Thus $f - EH/\mathrm{card}(\mathcal{G})$ reduces to a polynomial with a lower leading term than g.

Iterating this process shows immediately the Lemma. $\diamondsuit$

End of proof of Theorem 2: The leading terms of J being $\{x_0^d, x_1^{d-1}, \ldots, x_d\}$, any polynomial irreducible by J has degree in the x_i at most $d(d-1)/2$, and the same is true for the polynomials H of Lemma 2. Thus, it remains to show that one may extract extract a $\mathbf{Q}[e_1, \ldots, e_d]$-base from the set of these polynomials H.

This may be done effectively by following process. For each monomial m of degree at most $d(d-1)/2$ in the x_i, compute $M := \sum_{\gamma \in \mathcal{G}} m^\gamma$ and R the result of the reduction of M by J. If the leading term of R is independent of the e_i and is different of the leading terms of previous R, add M to the base.

The proof that the set thus defined is a basis is straightforward, by looking on the leading terms. $\diamondsuit$

This proof induces an algorithm for computing a basis of invariants and the decomposition of any invariant on this base: Compute the normal form under J of any orbit of monomial. The theorem says if it appears in a base. When enough such invariants with linearly independent first terms are obtained, one has got a basis. The decomposition of another invariant on this basis may easily be done by normal form computation.

The search of a base needs not to consider a lot of orbits of monomials, because the computation of the Hilbert series of the ring of invariants gives immediately the number of basis elements of each degree: This series is of the form $P(t)/\prod_{i=1}^{d}(1-t^i)$ where $P(t)$ is a polynomial in t. The coefficient of t^i in P is the number of basis elements of degree i.

This algorithm is not very efficient, but very short to implement in Maple and it works sufficiently for our purpose.

4 Equations of small degree

In this section, we will show how the polynomials s_i of Section 2 are useful to find again the classical formulae for equations of small degree, showing that these formulae may be deduced without tricks from a general method we will apply again for degree 5.

4.1 Degree 2

Let $f = ax^2 + bx + c$; we have

$$\omega = -1$$

$$\begin{aligned}
s_0 &= x_0 + x_1 = -b/a \\
S_1 &= (x_0 - x_1)^2 = (x_0 + x_1)^2 - 4x_0x_1 = (b/a)^2 - 4c/a \\
x_0 &= (s_0 + \sqrt{S_1})/2 \\
x_1 &= (s_0 - \sqrt{S_1})/2
\end{aligned}$$

Thus we obtain exactly the standard formulae.

4.2 Degree 3

Let us suppose that $f = x^3 + px + q$. The primitive third root of unit is as usually denoted by j.

The group $\mathcal{S}_3$ has only one subgroup $\mathcal{A}_3 = \mathcal{C}_3$. It has $(x_0 - x_1)(x_1 - x_2)(x_2 - x_0) = \sum_{\mathcal{C}}(x_0x_1^2 - x_0^2x_1)$ as a resolvent invariant with resolvent $X^2 - \Delta$, where Δ is a symmetric polynomial which becomes the discriminant $4p^3 + 27q^2$ after substituting the x_i by the roots of f.

However, to have a better formula, in which j does not appear, we will choose $(j - j^2)(x_0 - x_1)(x_1 - x_2)(x_2 - x_0)$ as a resolvent invariant; it has $X^2 + 3\Delta$ as resolvent. This choice is relevant because the conjugation of j, which exchange j and j^2, has the same action as the transposition of x_1 and x_2.

This allows us to express the S_i in term of this resolvent invariant and symmetric polynomials:

$$\begin{aligned}
S_1 &= (x_0 + jx_1 + j^2x_2)^3 \\
&= s_0^3 + \frac{3}{2}(j - j^2)\sum_{\mathcal{C}}(x_0^2x_1 - x_0x_1^2) - \frac{9}{2}\sum_{\mathcal{S}} x_0^2 \\
S_2 &= (x_0 + jx_1 + j^2x_2)(x_0 + j^2x_1 + jx_2) \\
&= s_0^2 - 3\sum_{\mathcal{S}} x_0x_1
\end{aligned}$$

Thus, after substituting the x_i by the roots of f, anything may be expressed in terms of p, q and $\sqrt{3\Delta} = 18\sqrt{\frac{p^3}{27} + \frac{q^2}{4}}$:

$$\begin{aligned}
s_1 &= 3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \\
S_2 &= -3p \\
s_2 &= -3p/s_1 \\
x_0 &= \frac{s_1}{3} - \frac{p}{s_1} \\
x_1 &= \frac{j^2s_1}{3} - \frac{jp}{s_1} \\
x_2 &= \frac{js_1}{3} - \frac{j^2p}{s_1}
\end{aligned}$$

This formula is only valid if $s_1 \neq 0$, because it appears as denominator. Thus, if $p = 0$, the determination of the square root has to be chosen in order that $s_1 \neq 0$. This is always possible when f is irreducible, because this implies $q \neq 0$.

5 Degree five

The transitive subgroups of $\mathcal{S} = \mathcal{S}_5$ are well known. There are:

- The alternate group $\mathcal{A}$ of order 60 and of index 2 in $\mathcal{S}$
- The meta-cyclic group $\mathcal{M}$ of order 20 and of index 6 in $\mathcal{S}$. It is the maximal solvable subgroup of $\mathcal{S}$. Its element act as $x_i \to x_{ai+b}$ (indices modulo 5 and $a \neq 0 \bmod 5$).

It is bi-transitive and has 6 conjugates, corresponding to the 6 permutations of the x_i fixing x_0 and x_1.

- The dyadic group $\mathcal{D}$ of order 10, of index 2 in $\mathcal{M}$ and of index 6 in $\mathcal{A}$. Its elements are those of $\mathcal{M}$ for which $a = \pm 1$.

- The cyclic group $\mathcal{C}$ of order 5 and of index 2 in $\mathcal{D}$, consisting of the elements $\mathcal{M}$ such that $a = 1$.

The meta-cyclic group $\mathcal{M}$ being the maximal solvable subgroup of $\mathcal{S}$, an equation is solvable by radicals iff its Galois group is contained in $\mathcal{M}$. This implies that a separable resolvent of $\mathcal{M}$ has a root in $\mathbf{Q}$. Thus our problem consists in expressing the roots of f in term of the coefficients of f and of this root.

As we have already expressed the roots of f in term of polynomials invariant by $\mathcal{C}$ in order to solve by radicals, we have to make the following

- To find relative resolvent invariants and the corresponding resolvents equations for each inclusion in the chain
$$\mathcal{C} \subset \mathcal{D} \subset \mathcal{M} \subset \mathcal{S}.$$
These resolvents will be of the form $X^2 - a$, except the last one which will be of degree 6.

- To express any polynomial invariant under one of these groups in term of the resolvent invariant and of polynomials invariants under the bigger group.

- This will finally express (through two square roots) our invariants by $\mathcal{C}$ in term of symmetric polynomials and of the root of the resolvent of degree 6 which will be in $\mathbf{Q}$ iff the polynomial f is solvable by radicals

As said above, this process starts by the fact that the root x_0 of $f = x^5 + px^3 + qx^2 + rx + s$ we want to compute is $(s_0 + s_1 + s_2 + s_3 + s_4)/5$ where

$$\begin{aligned}
s_0 &= x_0 + x_1 + x_2 + x_3 + x_4 = 0 \\
s_1 &= x_0 + \omega x_1 + \omega^2 x_2 + \omega^3 x_3 + \omega^4 x_4 \\
s_2 &= x_0 + \omega^2 x_1 + \omega^4 x_2 + \omega x_3 + \omega^3 x_4 \\
s_3 &= x_0 + \omega^3 x_1 + \omega x_2 + \omega^4 x_3 + \omega^2 x_4 \\
s_4 &= x_0 + \omega^4 x_1 + \omega^3 x_2 + \omega^2 x_3 + \omega x_4
\end{aligned}$$

where ω is a primitive 5-th root of unity.

The circular permutation $x_i \to x_{i-1}$ acts on the s_i as the multiplication by ω^i. It follows that the polynomials $S_1 := s_1^5, S_2 := s_2 s_1^3, S_3 := s_3 s_1^2$ and $S_4 := s_4 s_1$ are invariant under the cyclic permutations of the x_i. Thus, if $S_1 \neq 0$, the root x_0 is a rational function of the S_i and $\sqrt[5]{S_1}$.

We will need to consider two actions on the invariants: The permutation φ such $\varphi(x_i) = x_{2i}$ (let us recall that indices are computed modulo 5) and the conjugation ψ of ω acting as $\psi(\omega) = \omega^2$. *All the invariant we will compute, including the s_i and the S_i will be invariant* *under $\varphi \circ \psi = \psi \circ \varphi$.* This will imply that the invariants under $\mathcal{M}$, which appear in the final resolution will be independent of ω.

Thus the main difficulty of the solving process is to choose the best resolvent invariants. The resolvent invariants for $\mathcal{C}$ and $\mathcal{D}$ of lowest degree are of degrees 3 and 2 respectively. However they are not always separable because any invariant of $\mathcal{C}$ of degree less than 5 is null together with its conjugates by $\mathcal{M}$, when specialized for the equation $x^5 - a$.

Thus a resolvent invariant for $\mathcal{C}$ or $\mathcal{D}$ needs to be of degree at least 5 for being always separable. We explicit now such invariants.

Let $T' = (x_0 - x_1)(x_1 - x_2)(x_2 - x_3)(x_3 - x_4)(x_4 - x_0)$ and $U' = (x_0 - x_2)(x_1 - x_3)(x_2 - x_4)(x_3 - x_0)(x_4 - x_1)$. They are resolvent polynomials for $\mathcal{C}$ which are clearly always separable (if they would not, f would have a multiple root). For managing the relation between φ and ψ we take $T = (\omega - \omega^4)T' + (\omega^2 - \omega^3)U'$ as resolvent invariant for $\mathcal{C}$ relatively to $\mathcal{D}$, and we consider also $U = \psi(T) = (\omega^2 - \omega^3)T' - (\omega - \omega^4)U'$. They satisfy following properties:

- $\varphi(T) = -U \qquad \varphi(U) = -T$
- T and U are never both null (if they were, T' would be 0 and f not irreducible).
- If $\mathbf{Q}$ does not contains $\sqrt{-1}$, then $T^2 + U^2$ is never null (if not, $\sqrt{-1} = T/U$ would be in the field generated by the roots of f, and the complex conjugation would be in the Galois group; as φ^2 is, up to a circular permutation of the roots, the only involution of $\mathcal{M}$, it would be equal to complex conjugation, which impossible by $\varphi^2(T/U) = T/U$).

We do not know if this last property is true without hypothesis on $\mathbf{Q}$.

The most evident resolvent polynomial for $\mathcal{D}$ relatively to $\mathcal{M}$, is $T'U'$, the square root of the discriminant of f. It is always separable, but of rather high degree (10) and a resolvent polynomial of lower degree would lead to simpler formulae. On the other hand, $\sum_{\mathcal{C}} x_i x_{i+1}$ is the resolvent polynomial of least degree, but not always separable.

The best choice seems to be $\varepsilon = (\omega - \omega^2 - \omega^3 + \omega^4) \prod_{\mathcal{C}} (x_1 - x_2 - x_3 + x_4)$, which is of degree 5. It satisfies $\varphi(\varepsilon) = \psi(\varepsilon) = -\varepsilon$. Is is always separable; in fact, its resolvent equation is of the shape $x^2 - D$, and if it is not separable, some factor of ε, say $x_1 - x_2 - x_3 + x_4$, is null. It is now easy to extract an equation of degree 3 for x_0 from

$$\begin{aligned}
x_0 + x_1 + x_2 + x_3 + x_4 &= 0 \\
x_1 + x_4 - (x_2 + x_3) &= 0 \\
x_0(x_1 + x_2 + x_3 + x_4) + (x_1 + x_4)(x_2 + x_3) + x_1x_4 + x_2x_3 &= p \\
x_0((x_1 + x_4)(x_2 + x_3) + x_1x_4 + x_2x_3) & \\
+(x_1x_4 + x_2x_3)(x_2 + x_3) + x_2x_3(x_1 + x_4 - x_2 - x_3) &= -q
\end{aligned}$$

which shows that f is not irreducible.

Now, if we know how to compute polynomials in the x_i which are invariant under $\mathcal{M}$ (this will be the object of next section), we are able to solve f:

$\varepsilon = \sqrt{D}$ where D is such an invariant by $\mathcal{M}$.

$E = T^2 + U^2$ and $F = \varepsilon(T^2 - U^2)$ are invariant by $\mathcal{M}$. Thus $T = \sqrt{E + \frac{F}{\varepsilon}}$. If $T = 0$, which implies that $\varepsilon \in \mathbf{Q}$, one may change the determination of $\sqrt{D}$, i.e. the sign of ε in order that $T \neq 0$.

$G = \varepsilon TU$ is invariant by $\mathcal{M}$. Thus $U = \frac{G}{\varepsilon T}$.

Thus, the computation of resolvent invariants is reduced to the computation of 4 invariants by $\mathcal{M}$, and it remains to compute the S_i, which are invariant by $\mathcal{C}$. For each such a polynomial S, we consider the four following invariant by $\mathcal{M}$:

$$\begin{array}{rcl} I_1(S) & := & S + \varphi(S) + \varphi^2(S) + \varphi^3(S) \\ I_2(S) & := & \varepsilon(S - \varphi(S) + \varphi^2(S) - \varphi^3(S)) \\ I_3(S) & := & TS - U\varphi(S) - T\varphi^2(S) + U\varphi^3(S) \\ I_4(S) & := & US + T\varphi(S) - U\varphi^2(S) - T\varphi^3(S) \end{array}$$

from which one may easily deduce S by solving this linear system of determinant $-8\varepsilon(T^2 + U^2)$.

If $T^2 + U^2 = 0$ (which is not possible over the field of the rationals), one may replace the last invariant by

$$I_4'(S) := \varepsilon((T + 2U)S + (U - 2T)\varphi(S) - (T + 2U)\varphi^2(S) - (U - 2T)\varphi^3(S))$$

The determinant of the new system is $-16\varepsilon^2(TU - T^2 + U^2) = -16\varepsilon^2(G - F)$. As $TU - T^2 + U^2 = T'U'(\omega + \omega^4 - \omega^2 - \omega^3)$, this determinant is never null.

The computation of $I_1(S), I_2(S), I_3(S), I_4'(S)$ always allows to compute S on any field $\mathbf{Q}$ of characteristic different of 2 and 5. However, the degree of $I_4'(S_1)$ in the x_i is 15 instead of 10 for $I_4(S_1)$. This leads to a much more complicate formula. For this reason, we have only done the computation with $I_1(S), I_2(S), I_3(S), I_4(S)$, which gives a formula only proved for fields $\mathbf{Q}$ in which -1 is not a square.

6 Degree 5 — invariants of the meta-cyclic group

In preceding Section, we have reduced our problem to the computation of a number of invariants of the meta-cyclic group $\mathcal{M}$. We explain now how to compute them.

The proof of Theorem 2 contains an algorithm for computing a base of the ring of invariants of $\mathcal{M}$ and for expressing any such invariant on this base. This has been implemented in Maple as follows.

The function `morbit` of Figure 1 computes the sum of the orbit under $\mathcal{M}$ of any monom and reduces it by the Gröbner base J of Lemma 1 (called here `base`). Applied to the monomials $x_0^2x_1x_4, x_0^3x_1x_4, x_0^4x_1x_4, x_0^3x_1^2x_4^2, x_0^4x_1^2x_4^2$, this shows that the sums of the orbit of these monomial satisfy the condition of Lemma 2. Thus, the $R_d^{\mathcal{S}}$-module $R_d^{\mathcal{M}}$ of rank 6 has a basis consisting of 1 and these sums, namely

$$\begin{array}{rcl} i_4 & = & \sum_{\mathcal{C}} x_0^2(x_1x_4 + x_2x_3) \\ i_5 & = & \sum_{\mathcal{C}} x_0^3(x_1x_4 + x_2x_3) \\ i_6 & = & \sum_{\mathcal{C}} x_0^4(x_1x_4 + x_2x_3) \end{array}$$

```
with(grobner);
vars:=[x4,x3,x2,x1,x0,p,q,r,s]:
base:=[x0+x1+x2+x3+x4,                            # The Groebner base J
 x0^2+x0*x1+x0*x2+x0*x3+x1^2+x1*x2+x1*x3+x2^2+x2*x3+x3^2+p,
 x0^3+x0^2*x1+x0^2*x2+x0*x1^2+x0*x1*x2+x0*x2^2+x1^3+x1^2*x2+x1*x2^2
                                                +x2^3+x0*p+x1*p+x2*p+q,
 x0^4+x0^3*x1+x0^2*x1^2+x0*x1^3+x1^4+x0^2*p+x0*x1*p+x1^2*p+x0*q+x1*q+r,
 x0^5+x0^3*p+x0^2*q+x0*r+s]:

morbit:=proc(exp)  # sum of an orbit and reduction by the Groebner base
        sum(sum(subs(
            '[x0=x[b],x1=x['modp(a+b,5)'],x2=x['modp(2*a+b,5)'],
             x3=x['modp(3*a+b,5)'],x4=x['modp(4*a+b, 5)']]'
                     ,exp),a=1..4),b=0..4) ;
    subs([x[0]=x0,x[1]=x1,x[2]=x2,x[3]=x3,x[4]=x4],");
    sort(normalf(",base,vars)); primpart(")
end:

i4:= morbit(x_0^2*x_1*x_4); i5:= morbit(x_0^3*x_1*x_4);
i6:= morbit(x_0^4*x_1*x_4); i7:= morbit(x_0^3*x_1^2*x_4^2);
i8:= morbit(x_0^4*x_1^2*x_4^2);

reduc:=proc(exp)                # expression of an invariant on the base
        normalf(exp,base,vars);
        normalf(",[i8-i_8,i7-i_7,i6-i_6,i5-i_5,i4-i_4],vars);
        sort(")
end:
```

Figure 1: Maple computation

$$
\begin{aligned}
i_7 &= \sum_{\mathcal{C}} x_0^3(x_1^2x_4^2 + x_2^2x_3^2) \\
i_8 &= \sum_{\mathcal{C}} x_0^4(x_1^2x_4^2 + x_2^2x_3^2)
\end{aligned}
$$

The function `reduc` expresses any polynomial invariant by $\mathcal{M}$ as a linear combination of i_4, i_5, i_6, i_7 and i_8. Here, `i4`,... is the normal form (reduced by J) of these invariants, and `i_4`, ... is a name for them.

Thus, it remains to express these five invariants as a rational function of a resolvent invariant. We chose i_4 for such a resolvent invariant, because it has both advantages to be the simplest one and to be always separable (see below).

For expressing the i_α in term of i_4, we express first the $i_4 i_\alpha$ as linear combination of the i_α; this needs to apply function `reduc` to corresponding products of normal forms, which are polynoms in the x_i of degree at most 12. Then, by the successive substitutions of Figure 2, we get the expression of the powers of i_4 as linear expressions of $i_4, \ldots, i_8$. Thus solving the linear system {`g2, g3, g4, g5`} in {`i_5, i_6, i_7, i_8`} gives the expression of these invariants as a rational function of i_4.

It remains to computes the resolvent equation of i_4 and to show that it is always separable,

```
g2:=    i_4^2 = reduc(i4^2);
f2:=    i_4*i_5 = reduc(i4*i5);
f3:=    i_4*i_6 = reduc(i4*i6);
f4:=    i_4*i_7 = reduc(i4*i7);
f5:=    i_4*i_8 = reduc(i4*i8);
sub:=[i_5=op(2,f2)/i_4,i_6=op(2,f3)/i_4,i_7=op(2,f4)/i_4,i_8=op(2,f5)/i_4]:

g3:=    i_4^3  = sort(expand(subs(sub,g2,expand(i_4*op(2,g2)))));
g4:=    i_4^4  = sort(expand(subs(sub,g2,expand(i_4*op(2,g3)))));
g5:=    i_4^5  = sort(expand(subs(sub,g2,expand(i_4*op(2,g4)))));
```

Figure 2: Maple computation, continued

i.e. that the determinant of above linear system never vanishes. For computing the resolvent equation, it would suffice to find a linear relation between the powers of i_4, i.e. to eliminate `i_5, i_6, ,i_7, i_8` between `g2, g3, g4, g5` and also `g6` which should be computed in the same way. But for proving that i_4 is always separable, we proceed in another way.

Let

$$V := \sum_{\mathcal{C}} x_0 x_1 \qquad \text{and} \qquad W := \sum_{\mathcal{C}} x_0 x_2.$$

It is clear that V and W are invariant under γ and exchanged by φ. Thus $\theta := (V-W)^2$ is invariant under the action of $\mathcal{M}$. In fact $\theta = 4i_4 + p^2 + 12r$, and the resolvent equation of i_4 and its separability are easily deduced by translation from those of θ.

With notation of last Section, $(W-V)T'U'$ is invariant by $\mathcal{M}$ and thus may be expressed as a polynomial in θ with coefficients rational functions of p, q, r, s. In fact, this is a polynomial in θ, p, q, r, s:

$$\begin{aligned} P \;=\; & \frac{1}{32}(\theta^3 - (20r+3p^2)\theta^2 - (8p^2r - 16pq^2 - 240r^2 + 400sq - 3p^4)\theta \\ & -p^6 + 28p^4r - 16p^3q^2 - 176p^2r^2 - 80p^2sq + 224prq^2 - 64q^4 + 4000ps^2 + 320r^3 - 1600rsq) \end{aligned}$$

It follows that the resolvent equation for θ is $R_\theta = P^2 - \theta\Delta$, where Δ, the square of $T'U'$, is the discriminant of f.

If this resolvent R_θ would have a multiple root for some values of the coefficients of f, this root would have a multiplicity at least 5: In fact, if the polynomial f is irreductible, its Galois group contains a cyclic permutation, and this permutation acts as a cycle of order 5 on the conjugates of θ. As the multiple root may not have 5 distinct conjugates, this cycle fixes it, and its multiplicity is at least 5.

As $R_\theta = P^2 - \theta\Delta$, $R'_\theta = 2PP' - \Delta$ and $\Delta \neq 0$, such a multiple root is not a root of PP' and is not 0. From $R_\theta = R'_\theta = 0$ and $P \neq 0$, we deduce $P - 2\theta P' = 0$. Substituting in the derivatives of order $2, 3, 4$ which are expressions involving only P and its derivatives, we easily get the contradiction $P = 0$, proving that R_θ and, by translation, the resolvent of i_4 are alway separable.

7 The formula

In this section, we describe and explicit the formula deduced from preceding sections.

One want to solve the *irreducible* polynomial

$$f := x^5 + px^3 + qx^2 + rx + s.$$

It is solvable by radicals iff following polynomial R has a root i_4 in $\mathbf{Q}$, which may be tested by any factorization algorithm. Let us remark that, when expanded, R is monic of degree 6 in x and that all numeric coefficients are integer. Note also that the second factor of the second term (as written below) is the discriminant of f.

$$\begin{aligned}
R \;=\; & \frac{1}{4}(2x^3 + 8x^2r + (-6p^2r + 2pq^2 - 50qs + 24r^2)x \\
& \quad - 15p^2qs - 16p^2r^2 + 13pq^2r + 125ps^2 - 2q^4 - 200qrs + 64r^3)^2 \\
& - (x + 3r + \frac{p^2}{4})(108p^5s^2 - 72p^4qrs + 16p^4r^3 + 16p^3q^3s - 4p^3q^2r^2 - 900p^3rs^2 \\
& \quad + 825p^2q^2s^2 + 560p^2qr^2s - 128p^2r^4 - 630pq^3rs + 144pq^2r^3 - 3750pqs^3 \\
& \quad + 2000pr^2s^2 + 108q^5s - 27q^4r^2 + 2250q^2rs^2 - 1600qr^3s + 256r^5 + 3125s^4)
\end{aligned}$$

From now on, i_4 is a root of R in $\mathbf{Q}$, and we will express the roots of f as functions of i_4, p, q, r, s. Let us define i_5, i_6, i_7, i_8, related to i_4 by following equations.

$$\begin{aligned}
i_4^2 \;=\; & 5i_8 - 2pi_6 + 4qi_5 - 2p^2i_4 - 6p^2r + 2pq^2 + 10qs + 4r^2 \\
i_4^3 \;=\; & \frac{1}{2}((3p^2 - 20r)i_8 + (-pq - 50s)i_7 + (-3p^3 + 28pr - 12q^2)i_6 \\
& \quad + (3p^2q - 45ps - 6qr)i_5 + (-3p^4 + 36p^2r - 15pq^2 + 60qs - 32r^2)i_4 \\
& \quad - 6p^4r + 3p^3q^2 + 41p^2qs + 52p^2r^2 - 54pq^2r - 250ps^2 + 14q^4 + 140qrs - 80r^3) \\
i_4^4 \;=\; & (19p^2r - 9pq^2 + 225qs - 60r^2)i_8 + (15p^2s - 8pqr + 3q^3 + 100rs)i_7 \\
& + (-4p^3r + 4p^2q^2 - 105pqs - 16pr^2 + 29q^2r + 125s^2)i_6 \\
& + (-9p^3s + 17p^2qr - 8pq^3 + 140prs + 155q^2s - 68qr^2)i_5 \\
& + (-4p^4r + 4p^3q^2 - 79p^2qs - 16p^2r^2 + 15pq^2r - 25ps^2 + 4q^4 + 80qrs)i_4 \\
& + 6p^4qs - 22p^4r^2 + 16p^3q^2r - 4p^2q^4 - 404p^2qrs + 68p^2r^3 + \\
& \quad 132pq^3s + 42pq^2r^2 + 550prs^2 - 30q^4r - 50q^2s^2 + 20qr^2s + 16r^4 \\
i_4^5 \;=\; & \frac{1}{2}((15p^4r - 5p^3q^2 + 290p^2qs - 152p^2r^2 - 27pq^2r - 1375ps^2 + 22q^4 - 700qrs + 240r^3)i_8 \\
& \quad + (18p^4s - 11p^3qr + 3p^2q^3 - 530p^2rs + 110pq^2s + 124pqr^2 - 41q^3r - 2375qs^2 + 200r^2s)i_7 \\
& \quad + (-15p^5r + 5p^4q^2 - 212p^3qs + 168p^3r^2 - 83p^2q^2r + 325p^2s^2 \\
& \quad\quad + 10pq^4 + 1560pqrs - 176pr^3 - 620q^3s - 12q^2r^2 - 1500rs^2)i_6 \\
& \quad + (15p^4qr - 5p^3q^3 - 147p^3rs + 351p^2q^2s - 90p^2qr^2 - 43pq^3r \\
& \quad\quad - 3175pqs^2 - 420pr^2s + 20q^5 + 215q^2rs + 152qr^3 + 625s^3)i_5 \\
& \quad + (-15p^6r + 5p^5q^2 - 200p^4qs + 200p^4r^2 - 110p^3q^2r + 355p^3s^2 + 15p^2q^4 + 1728p^2qrs \\
& \quad\quad - 432p^2r^3 - 752pq^3s + 220pq^2r^2 - 200prs^2 - 43q^4r + 1825q^2s^2 - 2640qr^2s + 512r^4)i_4 \\
& \quad - 30p^6r^2 + 25p^5q^2r + 198p^5s^2 - 5p^4q^4 - 491p^4qrs + 364p^4r^3 + 181p^3q^3s - 286p^3q^2r^2 \\
& \quad\quad - 810p^3rs^2 + 95p^2q^4r + 3005p^2q^2s^2 + 4120p^2qr^2s - 1088p^2r^4 - 12pq^6 - 4095pq^3rs \\
& \quad\quad + 612pq^2r^3 - 15875pqs^3 + 900pr^2s^2 + 858q^5s - 34q^4r^2 + 10700q^2rs^2 - 6240qr^3s \\
& \quad\quad + 960r^5 + 6250s^4)
\end{aligned}$$

These equations are linear in i_5, i_6, i_7, i_8 and solving this linear system expresses these invariants as polynomials in i_4 with the determinant of the system as denominator. As i_4 is always separable, this determinant is never 0.

We do not give here the expression of i_5, i_6, i_7, i_8 as polynomials in i_4 because of their size: i_8 needs 90 lines in our Maple program.

With i_4, i_5, i_6, i_7, i_8 one computes

$$\begin{aligned}
D &= 40pi_8 - 120qi_7 + (-24p^2+100r)i_6 + (88pq - 300s)i_5 + (-24p^3+100pr+24q^2)i_4 \\
&\qquad - 80p^3r + 40p^2q^2 - 480pqs + 160pr^2 + 332q^2r + 125s^2 \\
E &= (3p^2+20r)i_6 + (-pq-50s)i_5 + (3p^3+12pr+3q^2)i_4 \\
&\quad + 4p^3r - 3p^2q^2 + 40pqs + 16pr^2 - 21q^2r + 125s^2 \\
F &= (-65p^2q + 875ps - 550qr)i_8 + (-58p^2r + 41pq^2 - 275qs + 440r^2)i_7 \\
&\quad + (85p^3q - 520p^2s - 298pqr + 366q^3 + 2100rs)i_6 \\
&\quad + (4p^3r - 73p^2q^2 + 2095pqs - 56pr^2 - 748q^2r - 4875s^2)i_5 \\
&\quad + (85p^4q - 418p^3s - 440p^2qr + 419pq^3 + 1590prs - 1040q^2s + 524qr^2)i_4 \\
&\quad - 12p^5s + 158p^4qr - 85p^3q^3 - 1462p^3rs - 159p^2q^2s + 142p^2qr^2 + 896pq^3r \\
&\qquad + 175pqs^2 + 2900pr^2s - 402q^5 - 1925q^2rs - 448qr^3 - 1875s^3 \\
G &= (-35p^2q - 250ps - 200qr)i_8 + (-22p^2r + 19pq^2 + 650qs - 40r^2)i_7 \\
&\quad + (15p^3q + 195p^2s + 68pqr - 6q^3 - 1100rs)i_6 \\
&\quad + (-4p^3r - 27p^2q^2 - 270pqs + 96pr^2 - 182q^2r + 3000s^2)i_5 \\
&\quad + (15p^4q + 213p^3s + 50p^2qr + pq^3 - 940prs + 515q^2s - 184qr^2)i_4 \\
&\quad + 12p^5s + 42p^4qr - 15p^3q^3 + 492p^3rs - 156p^2q^2s + 358p^2qr^2 - 246pq^3r \\
&\qquad + 2825pqs^2 - 1400pr^2s + 42q^5 + 550q^2rs - 232qr^3 - 1250s^3
\end{aligned}$$

and then

$$\begin{aligned}
\varepsilon &= \sqrt{5D} \\
T &= \sqrt{\frac{5}{2}(E + \frac{F}{\varepsilon})} \\
U &= \frac{5G}{T\varepsilon}
\end{aligned}$$

If $T = 0$, which implies that ε is in $\mathbf{Q}$, we change the sign of ε. In fact, if both T values would be 0, the same would be true for E, F and the values of the invariants T and U of preceding sections, which is impossible.

Consider now

$$\begin{aligned}
H &= 25\,(2i_5 - pq - 5s) \\
I &= 25\,(\,40pi_8 - 70qi_7 + (-24p^2+100r)i_6 + (68pq-300s)i_5 + (-24p^3+100pr-46q^2)i_4 \\
&\qquad - 80p^3r + 20p^2q^2 - 255pqs + 160pr^2 - 28q^2r + 125s^2\,) \\
J &= -25pi_8 - 25qi_7 + (-9p^2-60r)i_6 + (-7pq+525s)i_5 + (-p^3-96pr+11q^2)i_4 \\
&\qquad + 50p^3r - 7p^2q^2 - 145pqs - 308pr^2 + 128q^2r - 1000s^2 \\
K &= -125pi_8 + 75qi_7 + (67p^2-420r)i_6 + (-109pq+1175s)i_5 + (63p^3-412pr+27q^2)i_4 \\
&\qquad + 210p^3r - 79p^2q^2 - 415pqs - 676pr^2 + 496q^2r - 750s^2
\end{aligned}$$

which allows to define

$$Q_1 = \frac{5}{4}(H + \frac{I}{\varepsilon} + \frac{TJ+UK}{E})$$

$$P_1 = \sqrt[5]{Q_1}$$

From now on we need $P_1 \neq 0$. If this is not the case, we get it by changing the sign of one or two of above square roots, which is equivalent to one of the following substitutions or their composition applied to above formulae for Q_1 and P_2, P_3, P_4.

$$\varepsilon \to -\varepsilon \quad T \to U \quad U \to -T$$

$$T \to -T \quad U \to -U$$

With P_1, one computes

$$\begin{aligned}
P_{41} &= -5p \\
P_{42} &= 5\,(10i_7 - 4pi_5 - 14qi_4 - 4p^2q + 45ps - 72qr) \\
P_{31} &= -25q \\
P_{32} &= 25\,(-10i_8 + 2pi_6 - 22qi_5 + 2p^2i_4 + 20p^2r + 2pq^2 - 35qs - 40r^2) \\
P_{33} &= 5\,(35i_8 - 4pi_6 + 23qi_5 + (-6p^2 + 12r)i_4 - 58p^2r + 14pq^2 - 105qs + 76r^2) \\
P_{34} &= 5\,(5i_8 - 22pi_6 + 14qi_5 + (-18p^2 + 16r)i_4 - 34p^2r + 22pq^2 - 140qs + 68r^2) \\
P_{21} &= 5\,(3i_4 + 2p^2 - 16r) \\
P_{22} &= 25\,(-10qi_6 + (8p^2 - 50r)i_5 + (-2pq - 25s)i_4 + 8p^3q - 20p^2s - 26pqr + 70q^3 + 50rs) \\
P_{23} &= 25\,(-4pi_7 - qi_6 + 4ri_5 + (-3pq + 15s)i_4 + 26p^2s - 26pqr + 7q^3 - 40rs) \\
P_{24} &= 25\,(3pi_7 - 18qi_6 + 22ri_5 + (-14pq + 20s)i_4 + 18p^2s - 33pqr + 21q^3 + 30rs)
\end{aligned}$$

Then

$$\begin{aligned}
P_4 &= \frac{P_{41}}{2P_1} + \frac{P_{42}}{2\varepsilon P_1} \\
P_3 &= \frac{P_{31}}{4P_1^2} + \frac{P_{32}}{4\varepsilon P_1^2} + \frac{P_{33}T + P_{34}U}{10EP_1^2} \\
P_2 &= \frac{P_{21}}{4P_1^3} + \frac{P_{22}}{4\varepsilon P_1^3} + \frac{P_{23}T + P_{24}U}{10EP_1^3}
\end{aligned}$$

A root of f is then

$$x_0 = \frac{P_1 + P_2 + P_3 + P_4}{5}$$

The other roots may be obtained by changing the determination of the fifth root. They may also be obtained by

$$x = \frac{\omega P_1 + \omega^2 P_2 + \omega^3 P_3 + \omega^4 P_4}{5}$$

where ω is any primitive fifth root of unit, i.e. a root of $x^4 + x^3 + x^2 + x + 1$, easily solvable by radicals.

8 Optimality

In this section, we shall prove that our formula is optimal in the number of roots to extract, and, moreover, that the field extension defined by the roots in our formula is the (unique) smallest field in which root of f is expressible by radicals.

Definition 1 *A* simple radical extension *is a simple field extension $k(x)$ such x has a prime power in k. A* radical extension *is an extension obtained by a finite number of simple radical extensions.*

The main result of this section is the following.

Theorem 3 *Let f be a irreducible quintic polynomial over the field* $\mathbf{Q}$ *which is solvable by radicals. Let L be a radical extension of* $\mathbf{Q}$ *which contains a root x of f. Then L contains a radical extension containing x and isomorphic to the extension defined by our formula.*

We may suppose that $L = K(z)$ is a simple radical extension of some subfield K which is a radical extension of $\mathbf{Q}$ and does not contain any root of f: Otherwise, we could replace L by its smallest radical extension containing a root of f.

We prove now that $z = \sqrt[5]{y}$ for some $y \in K$: The Galois group over K of the field generated by the 5 roots of f is a subgroup of the Galois group of f, itself included in $\mathcal{M}$. As K does not contain any root of f, this subgroup has no fixed point and thus contain $\mathcal{C}$ and is transitive on the roots. Thus f is irreducible over K and $K(z)/K$ has a degree multiple of 5. As z has a prime power in K, we have

$$L = K(z) = K(\sqrt[5]{y}) = K(x)$$

Let ω be a primitive fifth root of unit. The conjugates of z over K are the $\omega^i z$ and ω is in the field generated by the conjugates of z. Thus, the splitting field of L over K is

$$K(\omega, z) = K(\omega, x) = K(x, x_1, x_2, x_3, x_4)$$

where $x, x_1, \ldots$ are all the roots of f.

It follows immediately that all radicals which appear in our formula are contained in $K(\omega, x)$, being polynomials in $\omega, x, x_1, \ldots$, and it remains to prove that they are in $K(x)$. For this we have three case to consider.

If $\omega \in K$ there is nothing more to prove.

If $\omega \notin K$ but $\sqrt{5} \in K$, we have $K(\omega) : K = 2$, $K(\omega, x) : K = 10$, and the Galois group of f over K is $\mathcal{D}$. Let ϑ be its unique element of order 2 which fixes x. It maps ω on ω^4 and x_i on x_{4-i} (for some numbering of the x_i). Thus it change the signs of $\omega - \omega^4, \omega^2 - \omega^3, T', U'$ and fixes T, U and ε. As these invariants are also fixed by the circular permutation on the roots of f, they are in K.

Finally, if $\sqrt{5} \notin K$, we have $K(\omega) : K = 4$, $K(\omega, x) : K = 20$, and the Galois group of f over K is $\mathcal{M}$. Let ϑ its element which fixes x and maps ω on ω^2. As it is of order 4, it acts on the roots of f as a circular permutation. If we chose the numbering of the x_i in order that it maps x_i on x_{2i}, it follows from the definition of the invariants T, U and ε, that they are fixed by ϑ, and thus that, in all cases, K contains all square roots of our formula. Thus, the theorem is proved.

Moreover, following characterization of the smallest radical extension containing all roots of f is immediate from what precedes.

Theorem 4 *The smallest radical extension containing all roots of a resoluble quintic f which is irreducible over $\mathbf{Q}$ is the extension generated by all roots of f and a primitive fifth root of unit ω. Our formula expresses all the roots of f in this extension.*

If ω is of degree 2^d over $\mathbf{Q}$ and if the Galois group of f over $\mathbf{Q}(\omega)$ is of order $5 \cdot 2^e$, this smallest radical extension is of degree $5 \cdot 2^{d+e}$ and is defined by $d+e$ square roots and one fifth root.

9 Implementation and conclusion

The formula of preceding Section has been implemented in Maple almost as it is described. The main difference is that the linear system to solve has been solved once for all. The implementation contains also all examples we know of quintics solvable by radicals.

This implementation is available by anonymous ftp and may be down-loaded from following address: `ftp.lip6.fr:/lip6/softs/Maple/quinticV2.gz`

As this implementation contains mainly polynomial expressions and root extractions, its translation to any computer algebra system is very easy.

However such an implementation leads to a side problem which is not so easy: *To verify the correctness of the solution which is provided.* This seems easy by substituting the solution in the quintic polynomial and simplifying to 0. But such a task needs three ingredients.

The first one is a precise semantic for the square and quintic roots. The one that we need is that given two occurrences of the same root, the same determination is chosen, whichever it is.

The second ingredient is that the number of root extractions which appears in the solution is kept minimal. If not, the determination of the exceeding roots may wrongly be chosen. We have already mentioned this about Paxton Young formula which involves four fifth roots implying 25 solutions. For this reason, we could not use Maple expression for the primitive fifth roots of unit. In fact the answer given by Maple to `solve(1+x+x^2+x^3+x^4)` is

$$\begin{array}{ll} -\frac{1}{4}+\frac{1}{4}\sqrt{5}+\frac{1}{4}\sqrt{-10-2\sqrt{5}}, & -\frac{1}{4}+\frac{1}{4}\sqrt{5}-\frac{1}{4}\sqrt{-10-2\sqrt{5}}, \\ -\frac{1}{4}-\frac{1}{4}\sqrt{5}+\frac{1}{4}\sqrt{-10+2\sqrt{5}}, & -\frac{1}{4}-\frac{1}{4}\sqrt{5}-\frac{1}{4}\sqrt{-10+2\sqrt{5}} \end{array}$$

This contains two different iterated square roots, and, consequently, Maple is unable to simplify to 0 the difference between the square of the first solution and any other solution. Thus, in our program, we have replaced these expressions by the powers of the first one.

The third ingredient is a good simplificator for expressions involving root extractions. From version V.3 on, Maple is able to verify the solution for the equations with numeric coefficients. Nevertheless this remains a long computation, especially when one want to verify all solutions and not only the one which does not involves fifth roots of unit.

For the case of equations with symbolic coefficients, there were already a problem for the simple case $x^5 - a = 0$. Maple was unable to test that some expressions involved in our formula were null, and provided a false result in this case. The problem lyed in the fact that, for Maple, $\sqrt{a^2} = csgn(a)a$, and has been easily solved by replacing `sqrt(exp)` by `sqrt(exp, symbolic)` which returns a when applyed to a^2.

Nevertheless, even with this patch, we were unable to verify the solution of the three non trivial examples of solvable quintics with symbolic coefficients, which are given in our program.

All of this enforces our opinion that solving by radicals, when possible, leads to expressions which are too huge to be useful.

Thus, in our opinion, the only usefulness for our program is to be a very good test for simplificators for radical expressions.

References

[CLOS92] D. Cox, J.Little and D. O'Shea. *Ideals, Varieties and Algorithms.* Undergraduate Texts in Mathematics (Springer-Verlag, 1992).

[PY1888] G. Paxton Young. Solvable Quintics Equations with Commensurable Coefficients. *Amer. Journal of Math.*, **10**(1888), 99–130.