

DECIDING THE NILPOTENCY OF THE GALOIS GROUP BY COMPUTING ELEMENTS IN THE CENTRE

PILAR FERNANDEZ-FERREIROS AND M. ANGELES GOMEZ-MOLLEDA

ABSTRACT. We present a new algorithm for computing the centre of the Galois group of a given polynomial $f \in \mathbb{Q}[x]$ along with its action on the set of roots of f , without previously computing the group. We show that every element in the centre is representable by a family of polynomials in $\mathbb{Q}[x]$. For computing such polynomials, we use quadratic Newton-lifting and truncated expressions of the roots of f over a p -adic number field. As an application we give a method for deciding the nilpotency of the Galois group. If f is irreducible with nilpotent Galois group, an algorithm for computing it is proposed.

1. INTRODUCTION

The existing algorithms for the determination of the Galois group of a polynomial present strong limitations when the degree of the polynomial grows up. Part of them requires the classification of the permutation groups with the same degree as the given polynomial. The others use factorization of polynomials over number fields, which is very inefficient for high degrees.

V. Acciario and J. Klüners [1] described a method for computing the conjugates of a root of an irreducible polynomial $f \in \mathbb{Q}[x]$ with abelian Galois group. Their method is based on some results using prime ramification and Frobenius automorphisms, and it uses the quadratic Newton-lifting as principal technique in order to avoid factorization of polynomials over number fields. When it is known that the Galois group of a polynomial is abelian, its computation becomes easier. This motivates the question about the possibility of applying special techniques to other classes of groups and, in case this is possible, how to determine, a priori, whether the Galois group of a given polynomial $f \in \mathbb{Q}[x]$ belongs to any of these classes.

In a previous paper [7] we gave a method, based on the techniques used by V. Acciario and J. Klüners in [1], to decide whether the Galois group of a given irreducible polynomial $f \in \mathbb{Q}[x]$ is abelian in polynomial time in the size of the coefficients of f (assuming the Extended Riemann Hypothesis).

In the present paper we extend such a method to the computation of the centre of the Galois group of any polynomial $f \in \mathbb{Q}[x]$, not necessarily irreducible. As an application, we obtain a way to determine whether the Galois group is nilpotent, by constructing a series of polynomials related to a central series of this group. Finally we propose a procedure to compute the Galois group of an irreducible polynomial

Received by the editor May 24, 2002 and, in revised form, March 16, 2003.

2000 *Mathematics Subject Classification*. Primary 12Y05; Secondary 68W30 and 11R32.

Partially supported by the grant DGESIC PB 98-0713-C02-02 (Ministerio de Educacion y Cultura).

once decided it is nilpotent. Some examples show the behaviour of this method to compute Galois groups of polynomials with high degree.

Since for every $f \in \mathbb{Q}[x]$ there exists a monic and squarefree polynomial in $\mathbb{Z}[x]$ with the same Galois group, we will assume throughout this paper that the given polynomial f is monic and squarefree with integer coefficients.

From now on, we will denote by n the degree of f , by $\text{Gal}(f)$ the Galois group of f over \mathbb{Q} and by $Z(\text{Gal}(f))$ the centre of $\text{Gal}(f)$. We represent by $\alpha_1, \dots, \alpha_n$ all the roots of f in a splitting field F over \mathbb{Q} whose ring of integers is S . We will say that f is normal when $F = \mathbb{Q}(\alpha)$ for any root α of f .

2. COMPUTATION OF THE CENTRE

Along this section, we will denote by f_1, \dots, f_r of respective degrees n_1, \dots, n_r all the irreducible factors of f in $\mathbb{Z}[x]$. For every $i \in \{1, \dots, r\}$, $\alpha_{i1}, \dots, \alpha_{in_i}$ will represent all the roots of f_i and α_i any fixed root of f_i .

We prove in subsection 2.1 that every element in $Z(\text{Gal}(f))$ is representable by a family of polynomials F_1, \dots, F_r . We present several properties of these polynomials which allow us to construct them by performing quadratic Newton-lifting. In subsection 2.2 we consider the number of primes needed to complete the computation of the centre. In subsection 2.3 the algorithm is described.

2.1. Polynomial representation of the central elements.

Proposition 1. *An element $\tau \in \text{Gal}(f)$ belongs to $Z(\text{Gal}(f))$ if and only if there exist r polynomials $F_1, \dots, F_r \in \mathbb{Q}[x]$ (not necessarily different) such that $F_i(\alpha_{ij}) = \tau(\alpha_{ij})$ for all $j = 1, \dots, n_i$ and for every $i = 1, \dots, r$.*

Moreover, for each element $\tau \in Z(\text{Gal}(f))$, the corresponding polynomial F_i , $i = 1, \dots, r$, can be uniquely chosen of degree smaller than n_i .

Proof. Let us consider an element $\tau \in Z(\text{Gal}(f))$ and, for every i , let H_i be the subgroup of $\text{Gal}(f)$ associated to $\mathbb{Q}(\alpha_i)$ by the Galois correspondence. For every $\sigma \in H_i$,

$$\sigma(\tau(\alpha_i)) = \tau(\sigma(\alpha_i)) = \tau(\alpha_i).$$

Thus, $\tau(\alpha_i) \in \mathbb{Q}(\alpha_i)$ and there exists a unique $F_i \in \mathbb{Q}[x]$ of degree smaller than n_i such that $F_i(\alpha_i) = \tau(\alpha_i)$. Since $\text{Gal}(f)$ acts transitively on the roots of f_i , $F_i(\alpha_{ij}) = \tau(\alpha_{ij})$ for every $j = 1, \dots, n_i$.

Reciprocally, we suppose that r polynomials F_1, \dots, F_r describe the action of an element $\tau \in \text{Gal}(f)$ on the roots of f . For every $\sigma \in \text{Gal}(f)$, every $i \in \{1, \dots, r\}$ and every root α_{ij} of f_i ,

$$\sigma\tau(\alpha_{ij}) = \sigma(F_i(\alpha_{ij})) = F_i(\sigma(\alpha_{ij})) = \tau(\sigma(\alpha_{ij})).$$

Therefore, $\tau\sigma = \sigma\tau$ and $\tau \in Z(\text{Gal}(f))$. □

Definition 1. A family of polynomials $F_1, \dots, F_r \in \mathbb{Q}[x]$ (not necessarily different) with degree $(F_i) < n_i$ such that there exists $\tau \in Z(\text{Gal}(f))$ satisfying $F_i(\alpha_{ij}) = \tau(\alpha_{ij})$ for all $i = 1, \dots, r$ and for every $j = 1, \dots, n_i$ will be called the family of polynomials associated to (τ, f) .

The polynomial F_i is the polynomial associated to (τ, f_i) .

In order to compute $Z(\text{Gal}(f))$ without previously computing the whole Galois group, our aim will be to determine, for every central element τ , the family of

polynomials associated to (τ, f) . For this, it is not enough to find a polynomial permuting the roots of f , as the following example shows.

Example 1. $f(x) = x^6 + x^5 + 4x^4 + x^3 + 2x^2 - 2x + 1 \in \mathbb{Q}[x]$ is irreducible.

If α is a root of f , then $-\frac{1}{2} - \frac{1}{2}\alpha - \frac{5}{2}\alpha^2 - 2\alpha^3 - \alpha^4 - \frac{1}{2}\alpha^5$ is also a root of f . Thus

$$F(x) = -\frac{1}{2} - \frac{1}{2}x - \frac{5}{2}x^2 - 2x^3 - x^4 - \frac{1}{2}x^5$$

permutes the roots of f .

In this case, $\text{Gal}(f)$ is isomorphic to the dihedral group of order 6. If $F(x)$ were representing an element in $\text{Gal}(f)$, by Proposition 1, this would belong to the centre. But since $Z(\text{Gal}(f))$ is trivial, we must conclude that the permutation defined by $F(x)$ does not belong to $\text{Gal}(f)$.

The rest of the section is devoted to presenting a characterization of the polynomials associated to central elements which allows us to compute them.

Proposition 2. *For each element $\tau \in Z(\text{Gal}(f))$ there exist infinitely many primes p not dividing $\text{disc}(f)$ such that*

$$\tau(u) \equiv u^p \pmod{pS} \text{ for every } u \in S.$$

The reciprocal is also true: if $\tau \in \text{Gal}(f)$ and $\tau(u) \equiv u^p \pmod{pS}$ for all $u \in S$ and for some prime p not dividing $\text{disc}(f)$, then $\tau \in Z(\text{Gal}(f))$.

Proof. The first assertion follows directly from Tchebotarev's density theorem by noting that $\tau \in Z(\text{Gal}(f))$, pS is the intersection of all the prime ideals of S lying over p and $\text{Gal}(f)$ acts transitively over all these primes [10], [14], [15].

Now let $\tau \in \text{Gal}(f)$ such that $\tau(u) \equiv u^p \pmod{pS}$ for every $u \in S$ and for a prime p not dividing $\text{disc}(f)$. Then $\sigma\tau\sigma^{-1}(u) \equiv u^p \pmod{pS}$ for every $u \in S$ and for all $\sigma \in \text{Gal}(f)$. In particular, for any root α of f , $\sigma\tau\sigma^{-1}(\alpha)$ and $\tau(\alpha)$ are roots of f such that $\sigma\tau\sigma^{-1}(\alpha) - \tau(\alpha) \in pS$. Since p does not divide $\text{disc}(f)$, it must be $\sigma\tau\sigma^{-1}(\alpha) = \tau(\alpha)$ and $\tau \in Z(\text{Gal}(f))$. \square

Definition 2. A prime p is said to be associated to $\tau \in Z(\text{Gal}(f))$ when it does not divide $\text{disc}(f)$ and $\tau(u) \equiv u^p \pmod{pS}$ for all $u \in S$.

It follows from Proposition 2 that, for every $i \in \{1, \dots, r\}$, the polynomial F_i associated to (τ, f_i) must satisfy $F_i(\alpha_i) \equiv \alpha_i^p \pmod{pS}$ for infinitely many primes p not dividing $\text{disc}(f)$.

Besides, since each polynomial F_i permutes the roots of f_i , it is known that $F_i(x) = a_{i,0} + a_{i,1}x + \dots + a_{i,n_i-1}x^{n_i-1} \in \mathbb{Q}[x]$ where $a_{i,j} = \frac{b_{i,j}}{d}$ with $b_{i,j} \in \mathbb{Z}$ for all $j = 0, \dots, n_i - 1$ and d the largest positive integer whose square divides $\text{disc}(f_i)$. A bound B_i on the absolute value of the $b_{i,j}$ is computable from f_i :

$$|b_{i,j}| \leq B_i = d \text{disc}(f_i)^{-\frac{1}{2}} (1 + |\alpha_i|_\infty) n_i (n_i - 1)^{\frac{n_i-1}{2}} |\alpha_i|_\infty^{n_i-1},$$

where $|\alpha_i|_\infty$ is the maximum of the absolute values of the roots of f_i [1], [6], [9], [11].

The following known result gives a way to compute the polynomials.

Proposition 3. *If p is a prime not dividing $\text{disc}(f)$ and \mathbb{Z}_p denotes the ring of p -adic integers, there exists, for every $i = 1, \dots, r$, a unique polynomial $H \in \mathbb{Z}_p[x]$*

verifying

- (i) $f_i(H(\alpha_i)) = 0$,
- (ii) $H(\alpha_i) \equiv \alpha_i^p \pmod p$,
- (iii) $\deg(H) \leq n_i - 1$.

We remark that $H \in \mathbb{Z}_p[x]$ is the p -adic limit of a sequence $\{H_k\}_{k \geq 0} \subseteq \mathbb{Z}[x]$ such that $H(x) \equiv H_k(x) \pmod{p^{2^k}}$ for all $k \geq 0$. This sequence can be built up to any k by means of quadratic Newton-lifting [1], [6], [9].

It is well known that if $k_0 \in \mathbb{N}$ such that $\sqrt{\frac{p^{2k_0}}{2}} > \max\{B_i, |\text{disc}(f_i)|\}$, there exists a unique polynomial of the form $\tilde{H}_{k_0} = \frac{1}{\text{disc}(f_i)}(c_0 + c_1x + \dots + c_{n_i-1}x^{n_i-1})$ such that $c_j \in \mathbb{Z}, |c_j| \leq \frac{p^{2k_0}}{2}$ for every $j = 1, \dots, n_i$ and $\tilde{H}_{k_0} \equiv H_{k_0} \pmod{p^{2k_0}}$.

We will say that \tilde{H}_{k_0} is a p -polynomial associated to f_i .

Since the polynomial F_i associated to (τ, f_i) satisfies the conditions in Proposition 3, it must be $F_i = H$. In particular, $F_i \equiv H_k \pmod{p^{2^k}}$ for every $k \geq 0$. Therefore, $F_i = \tilde{H}_{k_0}$ (see [3], [5] for the computation of \tilde{H}_{k_0}).

Once we have computed p -polynomials $\tilde{F}_1, \dots, \tilde{F}_r$ corresponding respectively to each irreducible factor f_i of f , it is possible that, for some $i \in \{1, \dots, r\}$, $\tilde{F}_i(\alpha_i)$ is not a root of f_i . Then, \tilde{F}_i does not define a permutation on the roots of f_i , it is not associated to (τ, f_i) for any $\tau \in Z(\text{Gal}(f))$ and we conclude that p is not associated to any $\tau \in Z(\text{Gal}(f))$. Otherwise, $\tilde{F}_i(\alpha_i)$ is a root of f_i for every $i = 1, \dots, r$ and the following theorem asserts that p is associated to a central element.

Theorem 1. *If p is a prime not dividing $\text{disc}(f)$ and, for every $i \in \{1, \dots, r\}$, there are polynomials $F_i \in \mathbb{Q}[x]$ satisfying*

- (i) $F_i(\alpha_i)$ is a root of f_i ,
- (ii) $F_i(\alpha_i) \equiv \alpha_i^p \pmod{pS_i}$ where S_i is the ring of integers of the splitting field of f_i over \mathbb{Q} ,

then there exists $\tau \in Z(\text{Gal}(f))$ such that $\tau(\alpha_{ij}) = F_i(\alpha_{ij})$ for all $j = 1, \dots, n_i$ and for every $i = 1, \dots, r$.

Proof. For every prime Q of S lying over p , there exists a unique element $\tau \in \text{Gal}(f)$ such that $\tau(u) \equiv u^p \pmod Q$ for every $u \in S$ [14].

For every root α_{ij} of f_i there exists $\sigma_{ij} \in \text{Gal}(f)$ such that $\sigma_{ij}(\alpha_i) = \alpha_{ij}$. If $F_i(\alpha_{ij}) \neq \tau(\alpha_{ij})$, $F_i(\alpha_{ij}) - \tau(\alpha_{ij}) \in S$ divides $\text{disc}(f)$ and, since

$$F_i(\alpha_{ij}) - \tau(\alpha_{ij}) = F_i(\alpha_{ij}) - \alpha_{ij}^p + \alpha_{ij}^p - \tau(\alpha_{ij}) = \sigma_{ij}(F_i(\alpha_i) - \alpha_i^p) + \alpha_{ij}^p - \tau(\alpha_{ij}) \in Q,$$

then $\text{disc}(f) \in Q \cap \mathbb{Q} = p\mathbb{Z}$, which constitutes a contradiction.

Thus, $\tau(\alpha_{ij}) = F_i(\alpha_{ij})$ for all $j = 1, \dots, n_i$ and for every $i = 1, \dots, r$. From Proposition 1, it follows that $\tau \in Z(\text{Gal}(f))$. □

Example 2. $f(x) = x^6 + x^4 - 2x^3 + x^2 - x + 1$ is irreducible. For the prime $p = 2$ we compute a p -polynomial F associated to f ,

$$\begin{aligned} F(x) = & - \frac{2336223622783712423189347007709618892}{14283} \\ & + \frac{2336223622783712423189347007709618892}{14283}x \\ & + \frac{4672447245567424846378694015419223501}{14283}x^2 \\ & + \frac{2336223622783712423189347007709618892}{14283}x^3 \\ & + \frac{134243967870148415446798365366539595182}{14283}x^5. \end{aligned}$$

Since f splits completely modulo 211,

$$f(x) \equiv (x + 8)(x + 119)(x + 121)(x + 189)(x + 84)(x + 112) \pmod{211},$$

we can label each root of f with its value modulo 211. If α denotes the root congruent to -8 modulo 211, then $F(\alpha) \equiv 161 \pmod{211}$, so that we can conclude that $F(\alpha)$ is not a root of f and F is not associated to any $\tau \in Z(\text{Gal}(f))$.

By considering $p = 59$, we obtain the p -polynomial $F = -x^3 - x + 1$. Using the 211-adic expansion of the roots of f , we check that $F(\alpha)$ is a root of f . Therefore F is associated to a central element τ . Just by looking at the factorization of f modulo 59,

$$f(x) \equiv (x^2 + 13x + 51)(x^2 + 4x + 16)(x^2 + 42x + 53) \pmod{59},$$

we deduce also that the order of τ is 2.

2.2. Bound on the needed number of primes. For every prime p not dividing $\text{disc}(f)$ we can compute p -polynomials F_1, \dots, F_r associated to f . As we have seen, F_1, \dots, F_r is the family of polynomials associated to (τ, f) for some $\tau \in Z(\text{Gal}(f))$ if and only if p is associated to τ . Since there are infinitely many primes p associated to each element $\tau \in Z(\text{Gal}(f))$, by computing polynomials for sufficiently many primes, we will be able to determine $Z(\text{Gal}(f))$, but how many primes must we try to determine the whole centre?

The Tchebotarev density theorem asserts that the density of the number of primes associated to an element $\tau \in Z(\text{Gal}(f))$ is $\frac{1}{|Z(\text{Gal}(f))|}$. Lagarias and Odlyzko in [10] presented explicit bounds for the absolute value of the least prime associated to a conjugacy class in the Galois group. The best bound assumes the Extended Riemann Hypothesis. The result, in terms of our problem, is the following:

There exists an effectively computable positive absolute constant c such that, for every element $\tau \in Z(\text{Gal}(f))$, there exists a prime p associated to τ such that

$$p \leq c(\log |\Delta|)^2,$$

where Δ is the discriminant of the splitting field of f over \mathbb{Q} .

Bach and Sorenson [2] improved this result by giving a more specific bound:

$$p \leq (4 \log |\Delta| + 2.5|\text{Gal}(f)| + 5)^2.$$

If s is the minimal number of roots of f generating F and a_i is the coefficient of x^i in f , then $\log |\Delta| \leq s|\text{Gal}(f)| \log |\text{disc}(f)|$ and Mahler's bound for $\text{disc}(f)$ [12] provides the inequality $|\text{disc}(f)| < n^n (\sum_{i=0}^n |a_i|)^{2n-2}$. Thus, the bound on the least prime associated to a central element is polynomial in the order of $\text{Gal}(f)$ and in the size of the coefficients of f .

The following example shows that, in some cases, we have enough criteria to compute the whole centre while checking only a few primes.

Example 3. Let $f(x) = x^6 + x^4 - 2x^3 + x^2 - x + 1$ be the polynomial in Example 2. Since we have found an element $\tau \in Z(\text{Gal}(f))$ of order 2 and a prime p not dividing $\text{disc}(f)$ not associated to a central element, we know that 2 divides $|Z(\text{Gal}(f))|$ and $\text{Gal}(f)$ is not abelian. Taking into account that the order of the centre of a transitive subgroup of Σ_n divides n , $|Z(\text{Gal}(f))|$ is a divisor of 6. Then it must be $|Z(\text{Gal}(f))| = 2$ and $Z(\text{Gal}(f)) = \langle \tau \rangle$.

2.3. Description of the algorithm.

Input: A monic squarefree polynomial $f \in \mathbb{Z}[x]$ of degree n .

Output: The elements of $Z(\text{Gal}(f))$ with their action on the roots of f .

- (1) Factorize f in $\mathbb{Z}[x]$ to get its irreducible factors f_1, \dots, f_r of degrees n_1, \dots, n_r , respectively.
- (2) Let C be a bound for the least prime associated to an element in $Z(\text{Gal}(f))$.
Set $q := 1$ and let Z be the trivial group.
- (3) Choose a prime p not dividing $\text{disc}(f)$ such that $q < p < C$.
If such a prime does not exist, the algorithm ends and $Z(\text{Gal}(f)) = Z$.
- (4) Compute p -polynomials F_1, \dots, F_r associated to f_1, \dots, f_r . For a root α_i of f_i , $i = 1, \dots, r$, check whether $F_i(\alpha_i)$ is also a root of f_i .
 - (4.1) If, for some $i = 1, \dots, r$, $F_i(\alpha_i)$ is not a root of f_i , p is not associated to any element in $Z(\text{Gal}(f))$. In particular,
Gal(f) is not abelian.
Set $q := p$ and go back to step (3).
 - (4.2) If $F_i(\alpha_i)$ is a root of f_i for every $i = 1, \dots, r$, p is associated to some element $\tau \in Z(\text{Gal}(f))$. The action of τ on each root α_{ij} of f_i is given by the evaluation $F_i(\alpha_{ij})$ for every $i = 1, \dots, r$. Set $Z := \langle Z, \tau \rangle$. If $|Z| = n_1 n_2 \cdots n_r$, the algorithm ends.
Gal(f) = Z , Gal(f) is abelian.
Let b be a bound on $|Z(\text{Gal}(f))|$ (see Section 3). If $|Z| = b$, the algorithm ends and

$$Z = Z(\text{Gal}(f)).$$

Else set $q := p$ and go back to step (3).

Since the computation of a p -polynomial associated to f_i runs in polynomial time in the size of f_i and p [1] and the primes in step (3) are bounded by a polynomial expression in $|Z(\text{Gal}(f))|$ and the size of the coefficients of f , we conclude that the algorithm runs in polynomial time in the size of f and a given bound on $|Z(\text{Gal}(f))|$.

3. SOME SHORTCUTS TO ACCELERATE THE COMPUTATION

We show in this section how, in many cases, we can discard a prime p as associated to a central element and avoid the computation of p -polynomials by looking at the factorization of f modulo p . We will assume that f is irreducible.

3.1. Degree of the irreducible factors modulo p . If $\tau \in Z(\text{Gal}(f))$ and p is a prime associated to (τ, f) , the degrees of the irreducible factors of f modulo p are the lengths of the orbits of the action of $\langle \tau \rangle$, the Galois group of f over $\mathbb{Z}/p\mathbb{Z}$, on the roots of f . From the obvious result below, it follows that all the irreducible factors of f modulo p have the same degree.

Lemma 1. *Let G be a transitive subgroup of the symmetric group Σ_n . If $\tau \in Z(G)$ and $\tau = \tau_1 \cdots \tau_s$ is the decomposition of τ into disjoint cycles, including cycles of length 1 which represent the elements fixed by τ , all the cycles τ_1, \dots, τ_s have the same length.*

This fact shows directly that the Galois group of the polynomial in Example 2 is not abelian by looking at its factorization modulo 7:

$$f(x) \equiv (x^2 + 3x + 5)(x + 1)(x + 4)(x^2 + 6x + 6) \pmod{7}.$$

The number of linear factors appearing in the factorizations of $f \pmod p$ for different primes p is also useful for getting a bound on $|Z(\text{Gal}(f))|$:

Lemma 2. *If p_1, \dots, p_m are primes not dividing $\text{disc}(f)$ such that, for each $i = 1, \dots, m$, f has exactly a_i linear factors modulo p_i and $\gcd(a_1, \dots, a_m) = k$, then $|\text{Aut } \mathbb{Q}(\alpha)|$ is a divisor of k . In particular, $|Z(\text{Gal}(f))|$ divides k .*

Thus, if f is the polynomial of degree 6 above, by looking at its factorization modulo 7, we conclude that $|Z(\text{Gal}(f))|$ divides 2.

3.2. Repetitions in the coefficients of the irreducible factors modulo p .

We will show that, for all primes p associated to an element in $Z(\text{Gal}(f))$ except for a finite set, there is a certain type of regularity in the repetitions of the coefficients of the factors of f modulo p .

If f is irreducible and p is a prime associated to some element $\tau \in Z(\text{Gal}(f))$ of order r , we suppose the roots $\alpha_1, \dots, \alpha_n$ of f ordered in such a way that

- α_1 is arbitrarily chosen at the beginning,
- for $2 \leq i \leq n/r$, α_i is arbitrarily chosen among the roots not belonging to the set

$$\{\tau^l(\alpha_m) : 1 \leq m < i, 0 \leq l \leq r - 1\},$$

- for $1 \leq j \leq \frac{n}{r}$ and $0 \leq i \leq r - 1$, $\alpha_{\frac{n}{r}i+j} = \tau^i(\alpha_j)$.

Then

- (1) f factors modulo p into $\frac{n}{r}$ irreducible polynomials given by

$$(x - \pi(\alpha_i))(x - \pi(\tau(\alpha_i))) \cdots (x - \pi(\tau^{r-1}(\alpha_i)))$$

where $i = 1, \dots, \frac{n}{r}$ and π is the canonical projection of S onto S/pS .

- (2) If, for every $k = 1, \dots, r$, $e_k(x_1, \dots, x_r)$ denotes the k -th elementary symmetric function on x_1, \dots, x_r , the polynomial

$$g_k(x) = \prod_{i=1}^{n/r} (x - e_k(\alpha_i, \tau(\alpha_i), \dots, \tau^{r-1}(\alpha_i)))$$

belongs to $\mathbb{Z}[x]$. Moreover, since all its roots are conjugate, g_k is a power of t_k , the minimal polynomial over \mathbb{Q} of

$$e_k(\alpha_1, \tau(\alpha_1), \dots, \tau^{r-1}(\alpha_1)).$$

Proposition 4. *Let p be a prime associated to $\tau \in Z(\text{Gal}(f))$ not dividing $\text{disc}(t_k)$. Then the coefficients of x^{r-k} in the irreducible factors of $f \pmod p$ are repeated as many times as the multiplicity of the roots of g_k .*

Proof. The roots of $g_k \pmod p$ are the coefficients of x^{r-k} in each irreducible factor of f . If p does not divide $\text{disc}(t_k)$, the projections of the different roots of g_k remain different. Therefore the coefficients of x^{r-k} in the irreducible factors of f modulo p are repeated as many times as the multiplicity of the roots of g_k . □

Note that, since g_k does not depend on the prime p associated to τ , the repetitions in the coefficients of x^{r-k} of the factors of $f \pmod p$ must be of the same type for every prime associated to τ not dividing $\text{disc}(t_k)$.

In Example 3,

$$f(x) \equiv (x^2 + 3)(x^2 + 2x + 4)(x^2 + 3x + 3) \pmod{5}.$$

The independent coefficient 3 appears in two factors while 4 appears in only one. This means that either 5 divides the disc(t_2) or 5 is not associated to any element in the centre. Since there are only finitely many primes dividing the discriminant, we can decide to avoid Newton-lifting and look for another prime.

When, for some $k = 0, \dots, r-1$, two different coefficients of x^{r-k} appear repeated in the irreducible factors of $f \pmod{p}$ a different number of times, we will say that the factorization of $f \pmod{p}$ presents irregular repetitions.

Example 4. We apply the algorithm to the irreducible polynomial

$$\begin{aligned} f(x) = & x^{18} - 6x^{17} + 6x^{16} + 27x^{15} - 51x^{14} - 66x^{13} + 155x^{12} + 321x^{11} \\ & - 1009x^{10} + 742x^9 + 1266x^8 - 4815x^7 + 4951x^6 + 573x^5 \\ & - 2347x^4 - 737x^3 + 625x^2 + 334x + 43. \end{aligned}$$

By means of the shortcuts above we will determine $Z(\text{Gal}(f))$ by computing p -polynomials only for four primes.

$$\begin{aligned} f(x) \equiv & (x^3 + x^2 + 29x + 3)(x^3 + 32x^2 + 26x + 11)(x^3 + 11x^2 + 26x + 22) \\ & \times (x + 18)(x + 22)(x + 1)(x + 11)(x + 36)x(x + 33)(x + 4)(x + 40) \pmod{43}. \end{aligned}$$

By Lemma 2, $|Z(\text{Gal}(f))|$ divides 9. None of the first fifty prime numbers provide irreducible factors of f of degree 9 and only the following give all the factors of degree 3 without presenting irregularities:

$$37, 97, 103, 109, 127, 151, 163 \text{ and } 181.$$

Computing a 37-polynomial associated to f , we check that 37 is not associated to any element in $Z(\text{Gal}(f))$.

Associated to some $\tau_1 \in Z(\text{Gal}(f))$, we get a 97-polynomial

$$\begin{aligned} F(x) = & \frac{327247032733772000482235685}{648093112708411873363341182} - \frac{1105734151931157856747325823}{324046556354205936681670591} x \\ & + \frac{518774928596588725084579087}{324046556354205936681670591} x^2 + \frac{546125327753152214669363531}{24926658181092764360128507} x^3 \\ & + \frac{22218900759518128027669770063}{648093112708411873363341182} x^4 - \frac{41666065358891058820973080838}{324046556354205936681670591} x^5 \\ & + \frac{2539397652812721437896761189}{24926658181092764360128507} x^6 - \frac{11593995086999898649807888087}{648093112708411873363341182} x^7 \\ & - \frac{6855549177050245491181709934}{324046556354205936681670591} x^8 + \frac{6945738360859535948751982282}{324046556354205936681670591} x^9 \\ & - \frac{3762600491452618807415809089}{648093112708411873363341182} x^{10} - \frac{2066102342372030983878154103}{648093112708411873363341182} x^{11} \\ & + \frac{6792232866897061982981543}{648093112708411873363341182} x^{12} + \frac{367102182220650714893166968}{324046556354205936681670591} x^{13} \\ & - \frac{331887278209162895030714199}{648093112708411873363341182} x^{14} - \frac{99571260388811737246268927}{648093112708411873363341182} x^{15} \\ & + \frac{42102461982125822289341469}{324046556354205936681670591} x^{16} - \frac{13632428315441178444012723}{648093112708411873363341182} x^{17}. \end{aligned}$$

We set $Z = \langle \tau_1 \rangle$ and $|Z| = 3$. Going back to step (3) of the algorithm, we check that 103 is not associated to any central element. Later, we find a 109-polynomial F associated to some $\tau_2 \in Z(\text{Gal}(f))$. Now $Z = \langle \tau_1, \tau_2 \rangle$ has order 9 and it is not cyclic. Since $|Z(\text{Gal}(f))|$ is bounded by 9, it follows that $\text{Gal}(f) = \langle \tau_1, \tau_2 \rangle$.

With the help of GAP [8] we know that, among the 983 classes of transitive subgroups of Σ_{18} , only four have centre of order 9. The centre of two of them is cyclic, so that the only options for $\text{Gal}(f)$ are 18t17 and 18t79.

4. DECIDING THE NILPOTENCY OF GALOIS GROUPS

In this section we make use of the computation of central elements in order to decide whether $\text{Gal}(f)$ is nilpotent by constructing a series of polynomials related to a central series of this group.

In subsection 4.1 we define the derived polynomials of f and show that they can be computed by determining the minimal polynomial over \mathbb{Q} of a primitive element of a suitable extension. By successive construction of derived polynomials, we can compute a series of polynomials which, in case f is normal, is strongly related with a central series of $\text{Gal}(f)$.

In subsection 4.2 we give an algorithm to decide the nilpotency of the Galois group of any polynomial with rational coefficients.

Throughout this section we will assume that the polynomial f is irreducible and we will denote by α a fixed root of f . The reducible case will be reduced to this one at the end of the section. If K is an intermediate field of F/\mathbb{Q} and H a subgroup of $\text{Gal}(f)$, we will denote by K^H the subfield of K fixed elementwise by each element of H .

4.1. Derived polynomials and central series. Once we have computed a nontrivial element $\tau \in Z(\text{Gal}(f))$, we know a first subgroup $\langle \tau \rangle$ of a central series of G . To determine a second subgroup of a central series, it is enough to find (if it exists) a nontrivial element in $Z(\text{Gal}(f)/\langle \tau \rangle)$. For this, we will try to construct a polynomial whose Galois group is $\text{Gal}(f)/\langle \tau \rangle$.

Definition 3. If there exists a nontrivial element $\tau \in Z(\text{Gal}(f))$ and β is an algebraic integer such that $\mathbb{Q}(\alpha)^{\langle \tau \rangle} = \mathbb{Q}(\beta)$, the minimal polynomial $g \in \mathbb{Z}[x]$ of β over \mathbb{Q} will be called a derived polynomial from f by τ .

Applying the Fundamental Theorem of Galois Theory to the extension F/\mathbb{Q} , we obtain

Proposition 5. *Let g be a derived polynomial from f by some $\tau \in Z(\text{Gal}(f))$ of order r . Then, g has degree $\frac{n}{r}$ and $\text{Gal}(g)$ is a quotient of $\text{Gal}(f)$. When f is normal, g is also normal and $\text{Gal}(g) = \text{Gal}(f)/\langle \tau \rangle$.*

Proof. Let S be the subgroup of $\text{Gal}(f)$ corresponding to $\mathbb{Q}(\alpha)$. It is enough to check that $S\langle \tau \rangle$ corresponds to $\mathbb{Q}(\alpha)^{\langle \tau \rangle}$, $[\text{Gal}(f) : S\langle \tau \rangle] = n/r$, and $\text{Gal}(g) \approx \text{Gal}(f)/\text{Core}(S\langle \tau \rangle)$. \square

Then, when f is normal, the problem of looking for a polynomial whose Galois group is $\text{Gal}(f)/\langle\tau\rangle$ is solved as soon as a derived polynomial is computed. In the nonnormal case, the search for such a polynomial implies several difficulties since the order of $\text{Gal}(f)/\langle\tau\rangle$ and the smallest degree of an irreducible polynomial whose Galois group is $\text{Gal}(f)/\langle\tau\rangle$ are unknown.

Example 5. $f(x) = x^{12} - x^6 - x^2 - 1$ is irreducible, $\text{Gal}(f) = 12T293$, $|\text{Gal}(f)| = 46080$ and $|Z(\text{Gal}(f))| = 2$ (see [13]).

Using GAP [8], we have checked that there does not exist any transitive group of degree smaller than 24 isomorphic to $\text{Gal}(f)/Z(\text{Gal}(f))$. Thus there exists no irreducible polynomial of degree smaller than 24 with Galois group $\text{Gal}(f)/Z(\text{Gal}(f))$. In particular, none of the derived polynomials from f have the desired Galois group.

However, we will see that derived polynomials are a useful tool for our purposes. Once we know a nontrivial element $\tau \in Z(\text{Gal}(f))$, the following proposition leads us to obtain a derived polynomial from f by τ .

Proposition 6. *Let $\tau \in Z(\text{Gal}(f))$ be an element of order $r > 1$. Then, $\mathbb{Q}(\alpha)^{\langle\tau\rangle} = \mathbb{Q}(e_1(\alpha, \tau), \dots, e_r(\alpha, \tau))$ where $e_i(\alpha, \tau)$ denotes the i -th elementary symmetric function of $\{\alpha, \tau(\alpha), \dots, \tau^{r-1}(\alpha)\}$ for every $i \in \{1, \dots, r\}$.*

As is well known, there exist infinitely many $(r-1)$ -tuples of integers (a_2, \dots, a_r) such that

$$e_1(\alpha, \tau) + a_2 e_2(\alpha, \tau) + \dots + a_r e_r(\alpha, \tau)$$

is a primitive element of $\mathbb{Q}(e_1(\alpha, \tau), \dots, e_r(\alpha, \tau))/\mathbb{Q}$. On the other hand, for any given $(r-1)$ -tuple of integers (a_2, \dots, a_r) , $e_1(\alpha, \tau) + a_2 e_2(\alpha, \tau) + \dots + a_r e_r(\alpha, \tau)$ is a primitive element of $\mathbb{Q}(\alpha)^{\langle\tau\rangle}$ if and only if it has exactly n/r conjugates because $\frac{n}{r} = [\mathbb{Q}(\alpha)^{\langle\tau\rangle} : \mathbb{Q}]$.

In order to compute the minimal polynomial of a primitive element already determined, we can use the p -adic expression of the roots of f for a suitable prime p (see [4]).

Definition 4. A series of polynomials

$$g_0 = f, g_1 = g, g_2, \dots, g_m$$

such that, for $i = 1, \dots, m$, g_i is a derived polynomial from g_{i-1} by some nontrivial element in $Z(\text{Gal}(g_{i-1}))$ and g_m either has degree 1 or $Z(\text{Gal}(g_m))$ is trivial will be called a series of derived polynomials from f . When the degree of g_m is 1, we will say that the series is complete. We will refer to the polynomials $g_1 = g, g_2, \dots, g_m$ as derived polynomials of f .

Proposition 7. *Let $g_0 = f, g_1, \dots, g_m$ be a series of derived polynomials of f . If $\text{Gal}(f)$ is nilpotent, then the series is complete. When f is normal, the reciprocal is also true: if f is normal and the series is complete, then $\text{Gal}(f)$ is nilpotent.*

Proof. Since $\text{Gal}(g_m)$ is a quotient of $\text{Gal}(f)$, when $\text{Gal}(f)$ is nilpotent, either $Z(\text{Gal}(g_m))$ is not trivial or $\text{Gal}(g_m)$ is trivial and then the degree of g_m is 1. Let us assume now that f is normal and the degree of g_m is 1. From Proposition 5, $\text{Gal}(g_i)$ is of the form $\text{Gal}(f)/H_i$ and H_i/H_{i-1} is a cyclic subgroup of $Z(\text{Gal}(g_{i-1}))$ for every $i = 1, \dots, m$, with $H_m = \text{Gal}(f)$. Then

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_{m-1} \triangleleft \text{Gal}(f)$$

is a central series of $\text{Gal}(f)$. \square

There are nonnormal polynomials with a complete series of derived polynomials whose Galois group is not nilpotent:

Example 6. $f(x) = x^6 + x^4 - x^3 - 2x^2 + x + 1$ is irreducible and $\text{Gal}(f) = 6T5$ (see [13]) is not nilpotent. Since $6T5$ has order 18, f is not normal. However,

$$\begin{aligned} g_0(x) &= f = x^6 + x^4 - x^3 - 2x^2 + x + 1, \\ g_1(x) &= x^2 + 3, \\ g_2(x) &= x - 1 \end{aligned}$$

is a complete series of derived polynomials from f .

The previous result gives a method for deciding whether the Galois group of a normal polynomial is nilpotent. However, two questions remain unsolved: how to decide, in advance, whether a given polynomial is normal and how to decide the nilpotency in the nonnormal case. The general method will be exposed in the next paragraph.

4.2. Nilpotency of the Galois group of a polynomial. We will assume that f is irreducible of degree $n = p_1^{m_1} \cdots p_s^{m_s}$ where s, m_1, \dots, m_s are positive integers and p_1, \dots, p_s are distinct primes.

Proposition 8. *If $\text{Gal}(f)$ is nilpotent,*

- (a) p_1, \dots, p_s are the only prime divisors of the order of $\text{Gal}(f)$ and there exists at least one element $\tau \in Z(\text{Gal}(f))$ of order p_i for each $i = 1, \dots, s$,
- (b) there exists a derived polynomial \tilde{g}_i of f of degree $p_i^{m_i}$ for each $i = 1, \dots, s$.

Proof. (a) It suffices to take into account that $|Z(\text{Gal}(f))|$ divides n and the elementary properties of nilpotent groups.

(b) Let us fix $i \in \{1, \dots, s\}$. For each prime divisor p_j of n different from p_i , there exists $\tau_j \in Z(\text{Gal}(f))$ of order p_j and a derived polynomial g_j of degree $\frac{n}{p_j}$ such that $\text{Gal}(g_j)$ is nilpotent. Applying the same procedure successively to g_j , a derived polynomial \tilde{g}_i of degree $p_i^{m_i}$ will be obtained. \square

From this result, it is easy to see that the Galois group of the polynomial of degree 18 in Example 4 is not nilpotent. Following the steps described in the proof, we can construct, if they exist, derived polynomials of f , $\tilde{g}_1, \dots, \tilde{g}_s$ of degrees $p_1^{m_1}, \dots, p_s^{m_s}$, respectively.

Example 7. For the irreducible polynomial

$$\begin{aligned}
 f(x) = & x^{72} - 23x^{71} + 184x^{70} - 225x^{69} - 5483x^{68} + 30704x^{67} + 13044x^{66} - 623096x^{65} + 1466262x^{64} \\
 & + 5156167x^{63} - 28692315x^{62} + 637737x^{61} + 268019636x^{60} - 439552468x^{59} - 1333892130x^{58} \\
 & + 4760576310x^{57} + 1919149440x^{56} - 28087306812x^{55} + 21785662978x^{54} + 103327855886x^{53} \\
 & - 193358366332x^{52} - 199561023659x^{51} + 848657247161x^{50} - 166112223678x^{49} \\
 & - 2236894567362x^{48} + 2467200252462x^{47} + 2901130319607x^{46} - 8094285660644x^{45} \\
 & + 2772836800425x^{44} + 12579392127673x^{43} - 22931462037981x^{42} + 6244874681055x^{41} \\
 & + 46979264837861x^{40} - 85534578381569x^{39} + 6834272402154x^{38} + 177623721558930x^{37} \\
 & - 247215610663730x^{36} + 14513888378477x^{35} + 405430878100266x^{34} - 651681888729020x^{33} \\
 & + 309037433848077x^{32} + 682964083193431x^{31} - 1465980110888206x^{30} + 898472126091157x^{29} \\
 & + 729409996703855x^{28} - 1810845158613785x^{27} + 1414800185812152x^{26} + 107550799384398x^{25} \\
 & - 1606918488180510x^{24} + 1456064707707072x^{23} + 403274703835174x^{22} - 1357241529160791x^{21} \\
 & + 110662000936722x^{20} + 917810273926986x^{19} - 144511480285596x^{18} - 650632477508129x^{17} \\
 & + 257719825346877x^{16} + 251277847069086x^{15} - 196748594221017x^{14} + 22038660480818x^{13} \\
 & + 39039097969879x^{12} - 58349598149779x^{11} + 27343290355593x^{10} + 17816276262087x^9 \\
 & - 17573412515707x^8 - 741377168381x^7 + 4180989901176x^6 - 710370862789x^5 \\
 & - 373096550602x^4 + 115279398831x^3 + 8294164606x^2 - 5139464562x + 435549967
 \end{aligned}$$

we have computed derived polynomials of degrees 8 and 9:

$$\begin{aligned}
 \tilde{g}_1(x) = & x^8 + 9x^7 + 144x^6 + 2500x^5 + 6328x^4 - 78627x^3 - 263585x^2 + 619550x + 2182813, \\
 \tilde{g}_2(x) = & x^9 - 58x^8 + 1126x^7 - 7906x^6 + 5274x^5 + 91426x^4 - 39428x^3 - 382650x^2 - 294609x - 27019.
 \end{aligned}$$

If, for some $i \in \{1, \dots, s\}$, there does not exist any derived polynomial of degree $p_i^{m_i}$, then $\text{Gal}(f)$ cannot be nilpotent. Theorem 2 below states a reciprocal: if such derived polynomials exist for every $i \in \{1, \dots, s\}$ and they have nilpotent Galois groups, then $\text{Gal}(f)$ is nilpotent.

Theorem 2. For every $i \in \{1, \dots, s\}$, let \tilde{g}_i be a derived polynomial of f of degree $p_i^{m_i}$. Then

- (a) $\text{Gal}(\tilde{g}_i) \approx \text{Gal}(f)/N_i$, with N_i a normal subgroup of $\text{Gal}(f)$ of order $p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_s^{k_s}$ where $k_1, \dots, k_{i-1}, k_{i+1}, \dots, k_s$ are positive integers.
 - (b) $\text{Gal}(f)$ can be embedded in $\text{Gal}(\tilde{g}_1) \times \cdots \times \text{Gal}(\tilde{g}_s)$.
 - (c) $\text{Gal}(f)$ is nilpotent if and only if $\text{Gal}(\tilde{g}_i)$ is nilpotent for every $i = 1, \dots, s$.
- Moreover, if $\text{Gal}(f)$ is nilpotent

$$\text{Gal}(f) \approx \text{Gal}(\tilde{g}_1) \times \cdots \times \text{Gal}(\tilde{g}_s).$$

Proof. It is enough to prove (a). Then (b) and (c) follow directly.

Let $f = g_0, g_1, g_2, \dots, \tilde{g}_i$ be an incomplete derived series such that, for every $j \in \{1, \dots, i\}$, g_j is derived from g_{j-1} by a central element of $\text{Gal}(g_{j-1})$ whose order is a prime. This prime must be distinct from p_i since g_i has degree $p_i^{m_i}$.

If $p_1 \neq p_i$ is the order of the central element τ which leads to obtain g_1 from f , then $\text{Gal}(g_1) = \text{Gal}(f)/H_1$ where H_1 is the normal subgroup of $\text{Gal}(f)$ associated, by the Galois correspondence, to the normal closure in F of $\mathbb{Q}(\alpha)^{\langle \tau \rangle}$ over \mathbb{Q} . Thus, for every $\sigma \in H_1$ and for every root α_j of f , σ fixes the polynomial

$$(x - \alpha_j)(x - \tau(\alpha_j)) \cdots (x - \tau^{p_1-1}(\alpha_j))$$

and there exists some integer k_j such that $\sigma(\alpha_j) = \tau^{k_j}(\alpha_j)$. Since τ^{k_j} has order either p_1 or 1, we can conclude that the disjoint cycles of the permutation induced by σ on the roots of f have length either p_1 or 1. Therefore H_1 is a p_1 -group.

If g_2 has been obtained from g_1 by an element in $Z(\text{Gal}(f)/H_1)$ of prime order $p_2 \neq p_1$, then $\text{Gal}(g_2) = (\text{Gal}(f)/H_1)/(H_2/H_1) \approx \text{Gal}(f)/H_2$ for some normal subgroup H_2 of $\text{Gal}(f)$ containing H_1 . By the above reasoning, H_2/H_1 is a p_2 -group and the order of H_2 is of the form $p_2^{a_2} p_1^{a_1}$, for some positive integers a_1, a_2 . Following the same reasoning up to \tilde{g}_i , we conclude the thesis. \square

The problem of deciding the nilpotency of the Galois group of an irreducible polynomial of degree $n = p_1^{m_1} \cdots p_s^{m_s}$ is thus reduced to deciding the nilpotency of s polynomials of degree $p_1^{m_1}, \dots, p_s^{m_s}$. The following theorem decides the nilpotency of the Galois group of an irreducible polynomial whose degree is a power of a prime.

Theorem 3. *If $f \in \mathbb{Z}[x]$ is irreducible of degree p^m , where m is a positive integer and p a prime, and $g_0 = f, g_1, \dots, g_k$ is any derived series of f , then $\text{Gal}(f)$ is nilpotent if and only if the series is complete.*

Proof. If $\text{Gal}(f)$ is nilpotent, the series is complete by Proposition 7.

If the series is complete, for every $i = 1, \dots, k$, $\text{Gal}(g_i)$ is a quotient of $\text{Gal}(f)$ by some normal subgroup H_i . Since the degree of g_k is 1, $\text{Gal}(f) = H_k$. The reasoning used in the proof of Theorem 2 (a) shows now that H_k is a p -group. \square

Example 8. Let f be the polynomial of degree 72 in Example 7, and let \tilde{g}_1, \tilde{g}_2 be the derived polynomials of degrees 8 and 9 already computed. Since there exists a complete series of derived polynomials of \tilde{g}_1 ,

$$\begin{aligned} g_0(x) = \tilde{g}_1(x) &= x^8 + 9x^7 + 144x^6 + 2500x^5 + 6328x^4 - 78627x^3 \\ &\quad - 263585x^2 + 619550x + 2182813, \\ g_1(x) &= x^4 - 9x^3 + 215x^2 - 1533x + 3193, \\ g_2(x) &= x^2 + 9x + 237, \\ g_3(x) &= x - 9, \end{aligned}$$

and a complete series of derived polynomials of \tilde{g}_2 ,

$$\begin{aligned} g'_0(x) = \tilde{g}_2(x) &= x^9 - 58x^8 + 1126x^7 - 7906x^6 + 5274x^5 + 91426x^4 \\ &\quad - 39428x^3 - 382650x^2 - 294609x - 27019, \\ g'_1(x) &= x^3 + 58x^2 + 1091x + 6607, \\ g'_2(x) &= x - 58, \end{aligned}$$

we can conclude that $\text{Gal}(f)$ is nilpotent. Any of the existing methods determines quickly the Galois groups of \tilde{g}_1 and \tilde{g}_2 . Using the Computer Algebra System **Magma**, we have obtained that $\text{Gal}(\tilde{g}_1) = 8T35$ and $\text{Gal}(\tilde{g}_2) = 9T17$. From Theorem 2, $\text{Gal}(f) = 8T35 \times 9T17$.

The reducible case. If the given polynomial f is reducible and f_1, \dots, f_r are all its irreducible factors over \mathbb{Q} , for every $i \in \{1, \dots, r\}$, $\text{Gal}(f_i)$ is a quotient of $\text{Gal}(f)$ and $\text{Gal}(f)$ is a subgroup of $\text{Gal}(f_1) \times \cdots \times \text{Gal}(f_r)$. Thus, $\text{Gal}(f)$ is nilpotent if and only if $\text{Gal}(f_i)$ is nilpotent for every $i = 1, \dots, r$.

5. COMPUTING NILPOTENT GALOIS GROUPS

Let f be an irreducible polynomial of degree $n = p_1^{m_1} \cdots p_s^{m_s}$ such that $\text{Gal}(f)$ is nilpotent. By Theorem 2, $\text{Gal}(f) = \prod_{i=1}^s \text{Gal}(\tilde{g}_i)$ with \tilde{g}_i as in Proposition 8. If the degrees of the derived polynomials \tilde{g}_i are small, several methods can be used to compute their Galois groups. Our aim in this section is to give some results which make possible the computation of these groups in case the degrees are too high.

Throughout this section we will be assuming that $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial of degree $n = p^m$, m a positive integer, p a prime and that $\text{Gal}(f)$ is a p -group.

Let $f = g_0, g_1, \dots, g_m$ be a complete series of derived polynomials of f . For every $j = 1, \dots, m$, let us denote by $\tau_j \in Z(\text{Gal}(g_{j-1}))$ the element of order p such that g_j is a derived polynomial from g_{j-1} by τ_j . Then, the degree of g_i is p^{m-i} for every $i = 0, 1, \dots, m$. We denote by β_0 any fixed root of f and by β_j ($j = 1, \dots, m$) the primitive element of $\mathbb{Q}(\beta_{j-1})^{\langle \tau_j \rangle} / \mathbb{Q}$ which is a root of g_j .

Among the polynomials in the series there exists at least one such that it is normal and the expression of its roots as polynomials in a fixed one is known. Let $i \in \{0, \dots, m-2\}$ be the smallest index such that g_{i+1} satisfies both conditions. A factorization of g_i over $\mathbb{Q}(\beta_i)$ can be obtained as follows:

Let $\beta_{i,1}, \beta_{i,2}, \dots, \beta_{i,p^{m-i-1}}$ be roots of g_i such that $\beta_{i,1} = \beta_i$ and

$$\beta_{i,j} \notin \bigcup_{l=1}^{j-1} \{\beta_{i,l}, \tau_{i+1}(\beta_{i,l}), \dots, \tau_{i+1}^{p-1}(\beta_{i,l})\}, \text{ for every } j = 2, \dots, p^{m-i-1}.$$

It is clear that, for every $j = 1, \dots, p^{m-i-1}$, the polynomial

$$h_j(x) = (x - \beta_{i,j})(x - \tau_{i+1}(\beta_{i,j})) \cdots (x - \tau_{i+1}^{p-1}(\beta_{i,j})) \in \mathbb{Q}(\beta_{i,j})[x],$$

belongs to $\mathbb{Q}(\beta_{i,j})^{\langle \tau_{i+1} \rangle}[x]$.

Lemma 3. For every $j = 1, \dots, p^{m-i-1}$,

- (a) $\mathbb{Q}(\beta_{i,j})^{\langle \tau_{i+1} \rangle} = \mathbb{Q}(F(\beta_{i,j}))$, where $F \in \mathbb{Q}[x]$ is a polynomial such that $\beta_{i+1} = F(\beta_i)$.
- (b) $h_j(x) \in \mathbb{Q}(\beta_i)[x]$.

Proof. (a) Let $\sigma \in \text{Gal}(g_i)$ be such that $\beta_{i,j} = \sigma(\beta_i)$. Then $\mathbb{Q}(\beta_{i,j})^{\langle \tau_{i+1} \rangle} \supseteq \mathbb{Q}(F(\beta_{i,j}))$ because

$$\tau_{i+1}(F(\beta_{i,j})) = \tau_{i+1}\sigma(F(\beta_i)) = \sigma\tau_{i+1}(F(\beta_i)) = \sigma(F(\beta_i)) = F(\beta_{i,j}).$$

Let $\delta = a_0 + a_1\beta_{i,j} + \cdots + a_{n-1}\beta_{i,j}^{n-1} \in \mathbb{Q}(\beta_{i,j})^{\langle \tau_{i+1} \rangle}$. Then

$$\sigma^{-1}(\delta) = a_0 + a_1\beta_i + \cdots + a_{n-1}\beta_i^{n-1} \in \mathbb{Q}(\beta_i)^{\langle \tau_{i+1} \rangle} = \mathbb{Q}(F(\beta_i))$$

and $\delta \in \mathbb{Q}(F(\sigma(\beta_i))) = \mathbb{Q}(F(\beta_{i,j}))$. Thus, $\mathbb{Q}(\beta_{i,j})^{\langle \tau_{i+1} \rangle} \subseteq \mathbb{Q}(F(\beta_{i,j}))$.

(b) $F(\beta_{i,j})$ is clearly a conjugate root of $F(\beta_i) = \beta_{i+1}$. Since g_{i+1} is normal, $F(\beta_{i,j}) \in \mathbb{Q}(\beta_{i+1}) \subseteq \mathbb{Q}(\beta_i)$. □

Since

$$g_i(x) = \prod_{j=1}^{p^{m-i-1}} h_j(x),$$

we have a factorization of g_i in factors of degree p in $\mathbb{Q}(\beta_i)[x]$, not necessarily irreducible. To obtain the complete factorization of g_i over $\mathbb{Q}(\beta_i)$, it will be enough to factorize every $h_j(\beta_i, x)$. In fact, it is enough to factorize at most $m - i - 1$ polynomials h_j .

Proposition 9. *It is enough to factorize over $\mathbb{Q}(\beta_i)$, at most $m - i - 1$ polynomials of the set $\{h_j : 2 \leq j \leq p^{m-i-1}\}$ to either find an irreducible h_j or to obtain the expression of all roots of g_i as polynomials in β_i .*

Proof. The roots of $h_1, \beta_1, \tau_{i+1}(\beta_1), \dots, \tau_{i+1}^{p-1}(\beta_1)$ are already expressed as polynomials in β_1 . If h_2 is irreducible over $\mathbb{Q}(\beta_1)$, we have finished. Else, $[\mathbb{Q}(\beta_{i,2}, \beta_1) : \mathbb{Q}(\beta_1)] < p$ and, since $\text{Gal}(f)$ is a p -group, $\beta_{i,2} \in \mathbb{Q}(\beta_i)$. Thus, h_2 splits over $\mathbb{Q}(\beta_1)$ and a polynomial $F_2 \in \mathbb{Q}[x]$ such that $\beta_{i,2} = F_2(\beta_i)$ is obtained. If $\sigma_2 \in \text{Gal}(f)$ such that $\beta_{i,2} = \sigma_2(\beta_i)$, then $F_2^k(\beta_i) = \sigma_2^k(\beta_i) \forall k \in \mathbb{N}$.

Since the order of σ_2 is a power of p , it should be $F_2^k(\beta_i) \neq \beta_i$ for all $k \in \{1, \dots, p-1\}$. Thus, $F_2^k(\beta_i)$ ($k = 0, \dots, p-1$) are roots of p different polynomials h_j so that the expression as a polynomial in β_i of every root of each one of them is known.

If none of these elements is a root of h_3 and h_3 is irreducible over $\mathbb{Q}(\beta_i)$, we have finished. Otherwise, we have computed a polynomial $F_3 \in \mathbb{Q}[x]$ such that $\beta_{i,3} = F_3(\beta_i)$. Now, the elements $F_3^l(F_3^k(\beta_i))$ with $l, k \in \{0, \dots, p-1\}$ are roots of p^2 different polynomials h_j .

Following this procedure for suitable polynomials h_j , in at most $m - i - 1$ steps, either we found an irreducible h_j or we have expressed the roots of g_i as polynomials in β_i . \square

Once we have obtained the factorization of g_i over $\mathbb{Q}(\beta_i)$, two cases must be considered:

- (a) If g_i is normal, we can repeat the procedure in order to obtain the factorization of g_{i-1} over $\mathbb{Q}(\beta_{i-1})$. In case the given polynomial f is normal, by applying the procedure successively, we will compute all the roots of f as polynomials in a fixed root α and the action of $\text{Gal}(f)$ over the roots of f will be completely determined.

Example 9. For the polynomial f with

$$\begin{aligned} f(x) = & x^{32} + 12x^{31} + 106x^{30} + 762x^{29} + 4501x^{28} + 23172x^{27} + 105726x^{26} + 429558x^{25} \\ & + 1583950x^{24} + 5291262x^{23} + 16128592x^{22} + 45110268x^{21} + 115127237x^{20} \\ & + 270291402x^{19} + 582395138x^{18} + 1138858482x^{17} + 2072373423x^{16} \\ & + 3339356088x^{15} + 5104133120x^{14} + 6550655310x^{13} + 8709819533x^{12} \\ & + 8087807202x^{11} + 10487671054x^{10} + 5838840108x^9 + 11660348108x^8 \\ & + 850939482x^7 + 12278527700x^6 + 1253298582x^5 + 21565514729x^4 \\ & + 2539603896x^3 + 14646941278x^2 - 19604530770x + 14880828169, \end{aligned}$$

the following complete series of derived polynomials is obtained:

$$\begin{aligned}
 g_0(x) &= f(x), \\
 g_1(x) &= x^{16} - 88x^{15} + 3592x^{14} - 89880x^{13} + 1534245x^{12} - 18798648x^{11} \\
 &\quad + 169203094x^{10} - 1123693646x^9 + 5434741275x^8 - 18472069830x^7 \\
 &\quad + 40879975322x^6 - 49002722446x^5 + 13382022899x^4 \\
 &\quad + 13993156410x^3 + 13450036750x^2 + 22230868650x + 6726610525, \\
 g_2(x) &= x^8 + 88x^7 + 3388x^6 + 74296x^5 + 1012608x^4 + 8760608x^3 + 46885056x^2 \\
 &\quad + 141731200x + 185178880, \\
 g_3(x) &= x^4 - 88x^3 + 2932x^2 - 43824x + 248384, \\
 g_4(x) &= x^2 + 88x + 2012, \\
 g_5(x) &= x - 88.
 \end{aligned}$$

If β_4 is a root of g_4 , the other is $-88 - \beta_4$. We will construct the polynomials h_j in order to factorize g_3 over $\mathbb{Q}(\beta_3)$, taking into account that g_4 is a derived polynomial from g_3 by a central element defined by

$$F(x) = -\frac{1342}{3} + \frac{185}{3}x - \frac{11}{4}x^2 + \frac{1}{24}x^3$$

and that $\beta_4 = -\beta_3 - F(\beta_3)$.

$$h_1(x) = x^2 + \left(-\frac{188}{3}\beta_3 + \frac{1342}{3} + \frac{11}{4}\beta_3^2 - \frac{1}{24}\beta_3^3\right)x - \frac{31048}{3} + \frac{4136}{3}\beta_3 - \frac{121}{2}\beta_3^2 + \frac{11}{12}\beta_3^3.$$

The polynomial h_2 , with its coefficients already expressed in $\mathbb{Q}(\beta_3)$, is

$$h_2(x) = x^2 + \left(-\frac{1606}{3} + \frac{188}{3}\beta_3 - \frac{11}{4}\beta_3^2 + \frac{1}{24}\beta_3^3\right)x + \frac{33808}{3} - \frac{4136}{3}\beta_3 + \frac{121}{2}\beta_3^2 - \frac{11}{12}\beta_3^3.$$

It is obvious, by the definition of h_1 , that its roots in $\mathbb{Q}(\alpha_3)$ are β_3 and $F(\beta_3)$. By factorizing h_2 over $\mathbb{Q}(\beta_3)$, we obtain the other two roots of g_3 , which is a normal polynomial:

$$\frac{1}{24}\beta_3^3 - \frac{1342}{3} + \frac{185}{3}\beta_3 - \frac{11}{4}\beta_3^2, \quad \frac{1474}{3} - \frac{185}{3}\beta_3 + \frac{11}{4}\beta_3^2 - \frac{1}{24}\beta_3^3.$$

Proceeding analogously, we compute the factorization of g_2 over $\mathbb{Q}(\beta_2)$. It results in being normal. Repeating the procedure for g_2 we notice that

$$\begin{aligned}
 h_3(x) &= x^2 + x \left(-\frac{179490164839105768452185675424697605839}{185347178664986085100401643308566231921032820} \beta_1^{15} + \dots \right. \\
 &\quad \left. \dots + \frac{854045242894993492140064641842903536835698212919}{1056478918390420685072289366858827521949887074} \right) \\
 &\quad + \frac{71242838066206222811864261243176861602767}{1056478918390420685072289366858827521949887074} \beta_1^{15} + \dots \\
 &\quad \dots - \frac{237913066936491262315054409263679q10684892349922901}{4225915673561682740289157467435310087799548296}
 \end{aligned}$$

is irreducible over $\mathbb{Q}(\beta_1)$.

- (b) If g_i is not normal, there exists $j \in \{2, \dots, p^{m-i-1}\}$ such that h_j does not split over $\mathbb{Q}(\beta_i)$. Then, we should have $[\mathbb{Q}(\beta_{i,j}, \beta_i) : \mathbb{Q}(\beta_i)] = p$ and h_j is irreducible over $\mathbb{Q}(\beta_i)$. Since $\mathbb{Q}(\beta_i) \subset \mathbb{Q}(\alpha)$ and $\beta_{i,j} \notin \mathbb{Q}(\alpha)$, $\beta_{i,j}$ is algebraic of degree p over $\mathbb{Q}(\alpha)$.

According to this remark, the extension $\mathbb{Q}(\alpha, \beta_{i,j})/\mathbb{Q}$ has degree p^{m+1} . If we construct a primitive element of $\mathbb{Q}(\alpha, \beta_{i,j})/\mathbb{Q}$, we can apply to its minimal polynomial \bar{f} the procedure applied to f . If the order of $\text{Gal}(f)$ is p^{m+1} , it will be computed by factorizing successively the derived polynomials of \bar{f} as described above. Otherwise, another element $\bar{\beta}$ will be found

such that $\mathbb{Q}(\alpha, \beta_{i,j}, \bar{\beta})$ has degree p^{m+2} over \mathbb{Q} . If $|\text{Gal}(f)| = p^{m+M}$, the algorithm will end after M steps.

Example 10. The polynomial \bar{f} given by

$$\begin{aligned} & x^{64} - 328x^{63} + 52880x^{62} - 5583316x^{61} + 434025006x^{60} - 26476342816x^{59} + 1319178102464x^{58} \\ & - 55172027907840x^{57} + 1975474132701615x^{56} - 61459358137894896x^{55} \\ & + 1680447375678738240x^{54} - 40745258028613470296x^{53} + 882355784953015567856x^{52} \\ & - 17163505100912929251840x^{51} + 301264979553827236666810x^{50} \\ & - 4789002034108430073611012x^{49} + 69137735239670011548314377x^{48} + \dots \\ & \dots \\ & \dots - 9260037844716710773725440191295122498545540503880x^3 \\ & + 4991638593737595331295518768298177130709528859622x^2 \\ & - 1616803360329159026514072447671092735965334919544x \\ & + 399960888789264880213405327854257750094429927501 \end{aligned}$$

is the minimal polynomial of a primitive element of $\mathbb{Q}(\alpha, \beta_{1,3})$ over \mathbb{Q} , where α and $\beta_{1,3}$ are, respectively, roots of f and h_3 in Example 9. Thus, the polynomial f of degree 32 has the same Galois group as \bar{f} .

Repeating the described procedure for the polynomial \bar{f} , we have been able to obtain the 32 polynomials h_j of degree 2 and to compute the 64 roots of \bar{f} in $\mathbb{Q}(\bar{\alpha})$, for any fixed root $\bar{\alpha}$ of \bar{f} .

6. CONCLUSIONS

We have presented an algorithm for deciding whether the Galois group of a given polynomial $f \in \mathbb{Q}[x]$ is nilpotent, by computing nontrivial elements in $Z(\text{Gal}(f))$. Since the computation of elements in the centre is fast in practice, the decision procedure is quite efficient.

The problem of the determination of $\text{Gal}(f)$, once it has been decided that it is nilpotent, has been reduced, in case the degree of f is not a power of a prime, to derived polynomials of smaller degree whose Galois groups are, in many cases, computable in a reasonable time by the existing methods. When the degree of f is a power of a prime p and is too high to apply them, we have proposed a method for computing the Galois group, which is a p -group. The hardest part of this method is the factorization of a certain number of polynomials of degree p (Proposition 9) over a root field of the corresponding derived polynomial. However, the procedure has allowed us to study the Galois group of many polynomials which cannot be handled by other methods.

7. ACKNOWLEDGMENTS

We wish to thank the French CNRS-UMS MEDICIS for providing us with the use of their computers, on which we have performed most computations.

REFERENCES

- [1] V. Acciaro, J. Klüners, *Computing automorphisms of abelian number fields*, Math. Comp. 68, 227, 1179-1186, 1999. MR **99i**:11099
- [2] E. Bach, J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. 65, 1717-1735, 1996. MR **97a**:11143
- [3] G. E. Collins, M. E. Encarnación, *Efficient rational number reconstruction*, J. Symb. Comput. 20, 287-297, 1995. MR **97c**:11116

- [4] H. Darmon, D. Ford, *Computational verification of M_{11} and M_{12} as Galois group over \mathbb{Q}* , Comm. Algebra 17, 2941-2943, 1989. MR **91b**:11146
- [5] J. D. Dixon, *Exact solution of linear equations using p -adic expansions*, Numer. Math. 40, 137-141, 1982. MR **83m**:65025
- [6] J. D. Dixon, *Computing subfields in algebraic number fields*, J. Austral. Math. Society 49, 434-448, 1990. MR **91h**:11156
- [7] P. Fernández-Ferreirós, M.A. Gómez-Molleda, *A method for deciding whether the Galois group is abelian*, Proc. ISSAC 2000, C. Traverso ed., ACM Press, 2000. MR **2002e**:12004
- [8] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.2; Aachen, St. Andrews, 1999. (<http://www-gap.dcs.st-and.ac.uk/~gap>)
- [9] J. Klüners, *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*, Dissertation Ph. D. Thesis, Berlin, 1997.
- [10] J. C. Lagarias, A. M. Odlyzko, *Effective version of the Chebotarev density theorem*, Algebraic number fields (L-functions and Galois properties), A. Fröhlich ed., pp. 409-464, Academic Press, London, 1977. MR **56**:5506
- [11] S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput. 14, 184-195, 1985. MR **86d**:11102
- [12] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11, 257-262, 1964. MR **29**:3465
- [13] G. Malle, B.H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, 2000. MR **2000k**:12004
- [14] D. A. Marcus, *Number fields*, Universitext, Springer Verlag, 1977. MR **56**:15601
- [15] P. Stevenhagen, H. W. Lenstra Jr., *Chebotarëv and his density theorem*, The Mathematical Intelligencer 18, no. 2, 1996. MR **97e**:11144

DEPARTAMENTO DE MATEMÁTICAS, ESTADÍSTICA Y COMPUTACIÓN, FACULTAD DE CIENCIAS,
UNIVERSIDAD DE CANTABRIA, 39005 SANTANDER, SPAIN

E-mail address: ferreirp@matesco.unican.es

DEPARTAMENTO DE MATEMÁTICAS, ESTADÍSTICA Y COMPUTACIÓN, FACULTAD DE CIENCIAS,
UNIVERSIDAD DE CANTABRIA, 39005 SANTANDER, SPAIN

E-mail address: gomezma@matesco.unican.es