A method for deciding whether the Galois group is abelian

Pilar Fernandez-Ferreiros *
Departamento de Matemáticas,
Estadística y Computación
Universidad de Cantabria
Santander, Spain
ferreirp@matesco.unican.es

Maria de los Angeles Gomez–Molleda *
Departamento de Matemáticas,
Estadística y Computación
Universidad de Cantabria
Santander, Spain
gomezma@matesco.unican.es

ABSTRACT

We propose a polynomial time algorithm to decide whether the Galois group of an irreducible polynomial $f \in \mathbb{Q}[x]$ is abelian, and, if so, determine all its elements along with their action on the set of roots of f. This algorithm does not require factorization of polynomials over number fields. Instead we shall use the quadratic Newton–Lifting and the truncated expressions of the roots of f over a p–adic number field $\mathbb{Q}_p$, for an appropriate prime p in $\mathbb{Z}$.

1. INTRODUCTION

Let us assume that $f \in \mathbb{Z}[x]$ is a monic irreducible polynomial of degree n, and let G_f be its Galois group over $\mathbb{Q}$, regarded as a permutation group acting on the roots of f.

H. W. Lenstra [12] states that there is a polynomial time algorithm that given f decides whether G_f is abelian, and if so, determines G_f. The proof is based on the observation that a transitive abelian permutation group of degree n has order n, applied to a theorem of S. Landau [10], which states the following:

> *There is a deterministic algorithm that given f and a positive integer b decides whether the Galois group G_f has order at most b, and if so gives a complete list of elements of G_f, and that runs in time $(b+l)^{O(1)}$, where l is the length of the data specifying f.*

The algorithm consists in performing successive factorizations of polynomials over finite algebraic extensions of $\mathbb{Q}$.

Regards this procedure to decide whether the Galois group of a polynomial is abelian, V. Acciaro and J. Klüners [1] remark that it is not very efficient (and, therefore, cannot solve large problems) due to the big complexity of the existing factorization algorithms over algebraic number fields. Acciaro and Klüners are interested in deciding whether G_f is abelian in the sense that they describe a method to compute the conjugates of a root α of a monic irreducible polynomial f with abelian Galois group. This is equivalent to the computation of the automorphisms of $L = \mathbb{Q}[\alpha]$ over $\mathbb{Q}$, where L is the splitting field of f over $\mathbb{Q}$ when G_f has order n. Their method is based on some results concerning prime ramification and Frobenius automorphisms, and it uses the quadratic Newton-Lifting (see [6, 8, 11]) as its principal technique.

In this paper, based on the method of Acciaro and Klüners previously described, we present a polynomial time algorithm to decide whether G_f is abelian and, in this case, to determine G_f. Briefly, our algorithm consists in applying the method of Acciaro and Klüners to the polynomial f assuming G_f is abelian (even if it is not the case), in order to describe the roots of f as a polynomial function of a fixed root α. If one of the steps of the mentioned method fails when applied to f, we will conclude that G_f is not abelian. Otherwise, if all the steps are satisfactorily fulfilled, we will conclude that G_f is abelian. Moreover, in this case, we will give all the elements of G_f along with their action on the roots of f.

Our algorithm does not require factorizations of polynomials over number fields. We will use, instead, the quadratic Newton-Lifting, and will determine, by using the Hensel-Lifting, truncated expressions of the roots of f over a p-adic number field $\mathbb{Q}_p$, for an appropriate prime $p \in \mathbb{Z}$. This prime p will be easy to find because of the assumption that G_f is abelian (if such a prime does not appear "easily" we shall conclude that G_f is not abelian).

Sections 2, 3 and 4 provide different tools allowing us to validate the results obtained in every step in order to confirm their "goodness". The algorithm is presented in section 5 and section 6 is devoted to showing some examples.

For the basic concepts of algebraic number theory used in this paper we refer the reader to [14] and for the questions of p-adic analysis to [3].

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

ISSAC 2000, St. Andrews, Scotland
©2000 ACM 1-58113-218-2/ 00/ 0008 $5.00

2. NOTATION

Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n, with $\alpha_1, \ldots, \alpha_n$ its n roots. When we fix any one of these roots, it will be denoted by α.

We will denote by G_f the Galois group of f over $\mathbb{Q}$, regarded as a transitive permutation group acting on the roots $\alpha_1, \ldots, \alpha_n$ of f. The centre of G_f will be represented by $Z(G_f)$.

The splitting field of f over $\mathbb{Q}$ is $L = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$. G_f has order n if and only if any of the roots of f is a primitive element of L over $\mathbb{Q}$, that is, $L = \mathbb{Q}[\alpha]$.

From now on d will be the discriminant of f, and d_L the discriminant of L over $\mathbb{Q}$.

The ring of integers of L will be denoted by S. It is well known that $S \subseteq \frac{1}{d_L}\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. When $L = \mathbb{Q}[\alpha]$, we have $S \subseteq \frac{1}{d}\mathbb{Z}[\alpha]$.

We will denote by $\mathcal{A}$ the set of polynomials $F \in \mathbb{Q}[x]$ of degree strictly smaller than n, such that $F(\alpha)$ is a root of f:

$$\mathcal{A} = \{F \in \mathbb{Q}[x] : deg(F) < n,\ F(\alpha) \text{ is a root of } f\}.$$

3. ABELIAN GALOIS GROUPS

As we have pointed out in the introduction, an abelian transitive subgroup of the permutation group Σ_n has order n. This is an important fact that makes our problem easier to solve, since it implies that any root α of f is a primitive element of the splitting field: thus every root of f can be described as a polynomial function of α.

PROPOSITION 1. *If G_f is abelian then G_f has order n.*

PROOF. $\forall i \in \{1, \ldots, n\}$, $|G_f| = |Stab(\alpha_i)||\text{Orbit of } \alpha_i|$, where $Stab(\alpha_i)$ is the stabilizer in G_f of α_i.

Since G_f is transitive then the orbit of α_i has length n and $Stab(\alpha_j) = \tau Stab(\alpha_i)\tau^{-1}$, where $\tau \in G_f$ such that $\tau(\alpha_i) = \alpha_j$.

If G_f is abelian, then $Stab(\alpha_j) = Stab(\alpha_i)\ \forall j \in \{1, \ldots, n\}$. But $\sigma \in Stab(\alpha_i)\ \forall i$ implies $\sigma = id$.

Then, $|G_f| = 1.n = n$. □

4. SOME PREVIOUS RESULTS

Throughout this section we will consider the case when the Galois group of f over $\mathbb{Q}$ has n elements, i.e., $|G_f| = n$.

Our first task consists in giving some results about transitive Galois groups of order n, which will be necessary in further discussions. Next, we will state some known results concerning prime ramification and Galois groups. We will only give the proofs (in some cases just part of them) when they can provide some useful information in order to understand the description of the algorithm.

LEMMA 1. *If G is a transitive subgroup of Σ_n of order n then, for each pair (α_i, α_j) of $\{\alpha_1, \ldots, \alpha_n\}$, there exists one and only one $\sigma \in G_f$ such that $\sigma(\alpha_i) = \alpha_j$.*

PROOF. Since G is transitive, there exists at least one element $\sigma_j \in G$ such that $\sigma_j(\alpha_i) = \alpha_j$. Because for every $k = 1, \ldots, n$ there exists $\sigma_k \in G$ such that $\sigma_k(\alpha_i) = \alpha_k$ and $k \neq k' \Rightarrow \sigma_k \neq \sigma_{k'}$, we have n different elements of G, that is, all the elements of G. So, only σ_j can apply α_i onto α_j. □

COROLLARY 1. *If G is a transitive subgroup of Σ_n of order n, and $\sigma, \tau \in G$ such that $\sigma(\alpha_i) = \tau(\alpha_i)$ for some $i \in \{1, \ldots, n\}$ then $\sigma = \tau$.*

PROOF. $\sigma(\alpha_i) = \tau(\alpha_i) \Rightarrow \tau^{-1}\sigma(\alpha_i) = \alpha_i$.

As there is only one element of G which fixes α_i, and the identity does this, $\tau^{-1}\sigma = id$. This implies that $\tau = \sigma$. □

LEMMA 2. *Let us assume that G_f is a transitive subgroup of Σ_n of order n, and let α be a root of f. If $\mathcal{A} = \{F \in \mathbb{Q}[x] : deg(F) < n,\ F(\alpha)$ is a root of $f\}$, then the mapping*

$$\begin{array}{rccc} \psi: & \mathcal{A} & \longrightarrow & G_f \\ & F & \to & \sigma_F \end{array}$$

(σ_F is the only element of G_f such that $\sigma_F(\alpha) = F(\alpha)$) is a bijection.

PROOF. It is easy to prove that ψ is well defined.

- ψ is surjective:

  If $\sigma \in G_f$ then there exists α_i, a root of f, such that $\sigma(\alpha) = \alpha_i$. Since $|G_f| = n = [L : \mathbb{Q}]$, we have $L = \mathbb{Q}[\alpha]$ and α_i is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. So, there exists $F \in \mathcal{A}$ such that $\alpha_i = F(\alpha)$. And then $\sigma = \sigma_F$.

- ψ is injective:

  $\sigma_{F_1} = \sigma_{F_2} \Rightarrow F_1(\alpha) = F_2(\alpha)$ and because $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a base of L over $\mathbb{Q}$, $F_1 = F_2$.

□

PROPOSITION 2. *Let G be a transitive subgroup of Σ_n. G is of order n if and only if every element of G splits into disjoint cycles of the same length.*

PROOF.

$\underline{\Rightarrow:}$ $G \leq \Sigma_n$ transitive of order n.

If $\sigma \in G$ and $\sigma = \sigma_1 \ldots \sigma_r$ is its decomposition in disjoint cycles, let $l_k = \min\{l_1, \ldots, l_r\}$ where l_i is the length of σ_i, $(i = 1, \ldots, r)$.

Let $\beta \in \{\alpha_1, \ldots, \alpha_n\}$ be moved by σ_k. Then

$$\sigma^{l_k}(\beta) = \sigma_1^{l_k} \ldots \sigma_r^{l_k}(\beta) = \beta \quad \Rightarrow \quad \sigma^{l_k} = 1 \quad \Rightarrow$$
$$\Rightarrow \sigma_i^{l_k} = id, \quad \forall i \quad \Rightarrow \quad l_i \leq l_k, \quad \forall i \quad \Rightarrow \quad l_i = l_k, \quad \forall i.$$

$\underline{\Leftarrow:}$ G is transitive and every $\sigma \in G$ splits into disjoint cycles of the same length:

Because G is transitive, once fixed α there exist $\sigma_1, \ldots, \sigma_n$ such that $\sigma_i(\alpha) = \alpha_i\ \forall i = 1, \ldots, n$. So, $|G| \geq n$.

Moreover, if $|G| > n$ then there exist $\sigma, \tau \in G$, $\sigma \neq \tau$, such that $\sigma(\alpha) = \tau(\alpha)$. Then, $\sigma\tau^{-1}$ has a cycle of length 1, and so, $\sigma\tau^{-1} = id$. □

COROLLARY 2. *Let $p \in \mathbb{Z}$ be a prime such that $p \nmid d$. If $|G_f| = n$ then all the factors in the factorization of f in $(\mathbb{Z}/p\mathbb{Z})[x]$ have the same degree.*

PROOF. If $|G_f| = n$ then every $\sigma \in G_f$ splits into disjoint cycles of the same length. It is a well–known result [7, 16] that the Galois group $\overline{G}_f$ of f over $\mathbb{Z}/p\mathbb{Z}$ is cyclic and generated by a product of disjoint cycles whose lengths are the degrees of the factors of f in $(\mathbb{Z}/p\mathbb{Z})[x]$, and $\overline{G}_f$ is a subgroup of G_f for a certain order of the roots of f. So, the factors of f in $(\mathbb{Z}/p\mathbb{Z})[x]$, must have all the same degree. □

Now, we will treat some questions concerning the Galois group G_f in connection with ramification theory and ideal factorization (see [14]).

PROPOSITION 3. *Let us assume that p is a prime of $\mathbb{Z}$ which does not divide the discriminant of f, and that Q is a prime ideal of S lying over p.*

Let D be the decomposition group of Q over p:

$$D = \{\sigma \in G_f : \sigma Q = Q\},$$

and $\overline{G}$ the Galois group of S/Q over $(\mathbb{Z}/p\mathbb{Z})$. Then

$$\begin{array}{rccc} \varphi: & D & \to & \overline{G} \\ & \sigma & \to & \overline{\sigma} \end{array}$$

with

$$\overline{\sigma}(u+Q) = \sigma(u) + Q \quad \forall u \in S$$

is a group isomorphism.

COROLLARY 3. *For every prime p such that $p \not| d$ and for every prime Q of S lying over p, there exists a unique $\sigma \in G_f$ such that $\sigma(u) \equiv u^p \bmod Q$ for all $u \in S$.*

PROOF. Since $\overline{G}$ is cyclic, generated by an element $\overline{\tau}$ such that $\overline{\tau}(u+Q) = u^p + Q$ for all $u \in S$, its inverse image by the isomorphism

$$\begin{array}{rccc} \varphi: & D & \to & \overline{G} \\ & \tau & \to & \overline{\tau} \end{array}$$

satisfies $\tau(u) + Q = u^p + Q$ for all $u \in S$: that is, $\tau(u) \equiv u^p \bmod Q$ for all $u \in S$.

On the other hand, if there exists $\sigma \in G_f$ such that $\sigma(u) \equiv u^p \bmod Q$ for all $u \in S$, σ satisfies the condition $\sigma(Q) \subseteq Q$ and then $\sigma(Q) = Q$. So, $\sigma \in D$ and $\overline{\sigma} = \overline{\tau}$.

By the previous proposition, $\sigma = \tau$, and so τ is the unique element in G_f verifying this condition. □

The previous corollary says that every prime p gives an element of G_f for each prime of S lying over p. The next result, Chebotarev Density Theorem, states that every element of G_f can be obtained from a prime p, in fact, from an infinite number of primes.

PROPOSITION 4 (CHEBOTAREV DENSITY THEOREM). *For every $\sigma \in G_f$ there exist infinitely many primes $p \in \mathbb{Z}$, with $p \not| d$, such that $\sigma(u) \equiv u^p \bmod Q$ for all $u \in S$, for some prime ideal Q lying over p.*

For the elements of the centre of the Galois group G_f, something more can be stated.

PROPOSITION 5. *If $\sigma \in Z(G_f)$ then there exist infinitely many primes $p \in \mathbb{Z}$ such that $p \not| d$ and $\sigma(u) \equiv u^p \bmod pS$ for all $u \in S$.*

PROOF. By the Tchebotarev Density Theorem there exist infinitely many primes p with the conditions of the statement and such that $\sigma(u) \equiv u^p \bmod Q$, where Q is a prime of S lying over p. Let us fix p one of these primes and assume that $pS = Q_1 \dots Q_r$, with $Q_1 = Q$.

Since for every $i \in \{1, \dots, r\}$ there exists $\tau_i \in G_f$ such that $Q_i = \tau_i(Q)$, from $\sigma(u) \equiv u^p \bmod Q$, we obtain that $\sigma\tau_i(u) = \tau_i\sigma(u) \equiv \tau_i(u)^p \bmod Q_i$ and then $\sigma(u) \equiv u^p \bmod Q_i$ for all $u \in S$ and $i = 1, \dots, n$.

So, $\sigma(u) \equiv u^p \bmod Q_1 \dots Q_r = pS$ for all $u \in S$. □

T next result, due to Lagarias and Odlyzko [9], gives a bound for the number of primes necessary to find a given element in G_f.

PROPOSITION 6 (LAGARIAS AND ODLYZKO BOUND). *There exists an effectively computable bound B depending on L such that each automorphism $\sigma \in G_f$ verifies $\sigma(\alpha) \equiv \alpha^p \bmod Q$, where Q is a prime lying over p, for at least one prime p smaller than B.*

The best possible bounds are obtained accepting the validity of the Extended Riemann Hypothesis. Acciaro and Klüners [1] propose

$$B := (4log|d_L|) + 2.5n + 5)^2,$$

obtained as a consequence of the explicit bounds of Bach and Sorenson [2].

We will refer to B as the "bound of Lagarias and Odlyzko".

Remember that when $|G_f| = n$, $d_L = d$.

5. DESCRIPTION OF THE METHOD

In this section we present an algorithm deciding, given $f \in \mathbb{Q}[x]$ irreducible, whether its Galois group is abelian or not. Since every polynomial with rational coefficients can be easily replaced by another monic polynomial with integer coefficients and the same Galois group over $\mathbb{Q}$, the input of our algorithm will be always a monic irreducible polynomial with integer coefficients.

The idea will consist in applying the method described by Acciaro and Klüners in [1] to determine the conjugate roots of α when G_f is abelian, although we do not know in advance if G_f is indeed abelian. The different steps of the algorithm lead towards the acceptance or rejection of the abelianity of G_f.

The following proposition is in the basis of the method of Acciaro and Klüners.

PROPOSITION 7. *Let $p \in \mathbb{Z}$ be a prime which does not divide d. If G_f is abelian then there exists a unique $F \in \mathcal{A}$ such that*

$$F(\alpha) \equiv \alpha^p \bmod pS.$$

PROOF. Since G_f abelian, $G_f = Z(G_f)$. By using corollary 3, for Q a prime lying over p, there exists a unique $\sigma \in G_f$ such that $\sigma(\alpha) \equiv \alpha^p \bmod Q$. In the proof of the proposition 5 we saw that $\sigma(\alpha) \equiv \alpha^p \bmod pS$. So, the polynomial F corresponding to σ verifies the required conditions.

Next we prove the uniqueness of F: if $H \in \mathbb{Q}[x]$ such that

$$H(\alpha) \equiv \alpha^p \bmod pS$$

then $F(\alpha) = H(\alpha)$ because p does not divide d. Therefore $F = H$. □

The next subsection describes how to compute the polynomial F in the previous proposition when a prime p is given and G_f is known to be abelian in advance.

5.1 The Newton-Lifting method

Given $p \in \mathbb{Z}$ a prime not dividing d, if G_f is abelian then we know, by proposition 7, that there exists $F \in \mathbb{Q}[x]$ of degree strictly smaller than n such that $F(\alpha)$ is a root of f and $F(\alpha) \equiv \alpha^p \bmod pS$. Thus, $f(\alpha^p) \equiv 0 \bmod pS$.

Newton-Lifting method allows us to compute a polynomial $F_k \in \mathbb{Z}[x]$ of degree strictly smaller than n such that

$$f(F_k(\alpha)) \equiv 0 \bmod p^{2^k} S, \text{ and } F_k(\alpha) \equiv \alpha^p \bmod pS.$$

Since $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a base of $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$ α^p can be expressed as a polynomial in α of degree smaller than n:

$$\alpha^p = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}.$$

Denoting $F_0(\alpha) = \overline{a}_0 + \overline{a}_1\alpha + \cdots + \overline{a}_{n-1}\alpha^{n-1}$, $a_i \equiv \overline{a}_i \bmod p$, $\overline{a}_i \in \{0, 1, \ldots, p-1\}$, then

$$F_k(\alpha) \equiv F_{k-1}(\alpha) - \frac{f(F_{k-1}(\alpha))}{f'(F_{k-1}(\alpha))} \bmod p^{2^k} S, \ k \geq 1.$$

Since $F(\alpha)$ is a root of f, and all the roots of f belong to $S \subseteq \frac{1}{d}\mathbb{Z}[\alpha]$, then F must be of the form

$$F(x) = \frac{1}{d}(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}), \ c_i \in \mathbb{Z}.$$

Assuming

$$dF_k = \sum_{i=0}^{n-1} c_{i,k}\alpha^i$$

($c_{i,k} \in \{0, 1, \ldots, p^{2^k} - 1\}$), it is known that if the coefficients of dF are in the interval $(-K, K]$, and $2K < p^{2^k}$, then

$$c_i = \begin{cases} c_{i,k} & \text{if} \quad c_{i,k} < p^{2^k}/2 \\ c_{i,k} - p^{2^k} & \text{if} \quad c_{i,k} \geq p^{2^k}/2 \end{cases}.$$

Acciaro and Klüners in [1] give a bound for the absolute value of the coefficients of dF:

$$|c_i| \leq d^{1/2} n (n-1)^{(n-1)/2} |\alpha_1|_\infty^{n(n-1)/2+1} := K,$$

so that if $2K \leq p^{2^k}$, we can recover F from F_k.

For the details of the method to do the computations, we refer the reader to [1, 6, 8]. When recovering F from F_k, this can be done without computing the discriminant d, by using the reconstruction techniques of rational numbers shown in [1, 4, 5].

So, we shall apply Newton-Lifting to our given polynomial f in order to obtain F for a certain prime p. But, since we do not know if G_f is abelian or not, it may happen that $F(\alpha)$ is not a root of f. In this case, we shall conclude that G_f is not abelian.

If $F(\alpha)$ is a root of f, we continue by applying this method until all the roots of f are described as polynomial functions of α, or the bound of Lagarias and Odlyzko is reached. The problem has been reduced to decide whether $F(\alpha)$ is a root of f or not, the topic of the next subsection.

5.2 p–adic expansion of the roots of f

A way of checking if $F(\alpha)$ is a root of f is by using the p–adic expansion of the roots of f.

PROPOSITION 8. *There exist infinitely many primes $p \in \mathbb{Z}$ which do not divide d and such that f splits completely in $(\mathbb{Z}/p\mathbb{Z})[x]$. For each one of these primes, f has n different roots in $\mathbb{Z}_p$, the ring of p–adic integers.*

PROOF. The first assertion is a consequence of Chebotarev Density Theorem: since the identity is an element of $Z(G_f)$, there exist infinitely many primes p in $\mathbb{Z}$ which do not divide d and such that $id(u) \equiv u^p \bmod pS$ gives the identity automorphism of S/pS. Then, f splits completely in $(\mathbb{Z}/p\mathbb{Z})[x]$.

For the second assertion, if $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ are the n roots of $f \bmod p$, since

$$f(\overline{\alpha}_i) \equiv 0 \bmod p,$$

we have that $|f(\overline{\alpha}_i)|_p < 1$ and because $p \nmid d$, $f'(\overline{\alpha}_i) \not\equiv 0 \bmod p$, that is, $|f'(\overline{\alpha}_i)|_p = 1$.

By Hensel's Lemma (see [3]), there exists $\alpha_i \in \mathbb{Z}_p$ such that $f(\alpha_i) = 0$ and $\alpha_i \equiv \overline{\alpha}_i \bmod p$. □

The elements of $\mathbb{Z}_p$ can be expressed as infinite sums of powers of p with coefficients in $\{0, \ldots, p-1\}$:

$$\mathbb{Z}_p = \{\sum_{m=0}^{\infty} a_m p^m : a_m \in \{0, \ldots, p-1\}\}.$$

For every root α_i of f we can construct its expression in $\mathbb{Z}_p$ by applying the following rule:

$$b_0 = \overline{\alpha}_i$$

$$b_{m+1} \equiv b_m - \frac{f(b_m)}{f'(b_m)} \bmod p^{m+1} \ (0 \leq m \leq k-1).$$

b_k is an integer number, so that it can be expressed through division by p in the form

$$b_k = a_0 + a_1 p + \ldots a_k p^k$$

with $a_0 = b_0$.

We have (see Hensel's Lemma in [3]) that

$$\alpha_i = a_0 + a_1 p + \ldots a_k p^k + O(p^{k+1}).$$

(For the operations with p-adic numbers see [13].)

Since when $|G_f| = n$ then all the factors of f in $(\mathbb{Z}/p\mathbb{Z})[x]$ have the same degree, to assure that all the factors of f are linear in $(\mathbb{Z}/p\mathbb{Z})[x]$ it will be enough to find a prime p of $\mathbb{Z}$ which does not divide d and such that f has a root in $\mathbb{Z}/p\mathbb{Z}$.

Let $f_0 = f(0)$, $\{p_1, \ldots, p_s\}$ the set of primes which divide d, and c a multiple of $p_1 \ldots p_s$. Then $f(f_0 c) = f(0)r$, where $r \equiv 1 \bmod p_i$, for all $i \in \{1, \ldots, s\}$. If $r \neq \pm 1$ and p is a prime dividing r, then f has a root in $\mathbb{Z}/p\mathbb{Z}$ and p does not divide d. On the other hand, there exists only a finite number of multiples c of $p_1 \cdots p_s$ such that $r = \pm 1$. Anyway, it will usually be enough to choose a prime divisor of $f(b)$, for any $b \in \mathbb{Z}$, and which does not divide d.

If $F(\alpha)$ is a root of f then

$$F(\overline{\alpha}) \equiv \overline{\alpha}_i \bmod p$$

for only one $i \in \{1, \ldots, n\}$, where p is a prime verifying the conditions of the proposition. Then, by computing the p–adic expansion of α and α_i up to a certain power k of p, we will able to decide whether $F(\alpha) = \alpha_i$ by just checking if $F(\alpha) \equiv \alpha_i \bmod p^k$.

It is sufficient to choose a power k such that some separable polynomial $H \in \mathbb{Z}[x]$, which has $F(\alpha) - \alpha_i$ as a root, has its coefficients in the interval $(-\frac{p^k}{2}, \frac{p^k}{2}]$: if $F(\alpha) - \alpha_i \equiv 0 \bmod p^k$, then $H_k = H \bmod p^k$ has a null independent term, and then the same occurs to H, because it can be recovered from H_k given the bound for its coefficients. So, $F(\alpha) - \alpha_i = 0$. By the same reasoning, if $F(\alpha) - \alpha_i \not\equiv 0 \bmod p^k$ then $F(\alpha) - \alpha_i \neq 0$. Notice that k will be polynomial in the size of f, because the product $\prod_{j,l \in \{1,\ldots,n\}} (x - (F(\alpha_j) - \alpha_l)) \in \mathbb{Z}[x]$ is a polynomial of degree n^2 with has $F(\alpha) - \alpha_i$ as a root.

The following theorem relates the properties of Galois groups or order n with the results concerning the restriction of the automorphisms in G_f to automorphisms of S/pS for integer primes p not dividing d. It provides a way to determine the center of a Galois group of order n, and we will use this fact to conclude that G_f is abelian when we have obtained all the roots of f as polynomial functions of a fixed root.

THEOREM 1. *Let $F \in \mathbb{Q}[x]$ with $deg(F) < n$ and $F(\alpha)$ a root of f. If $|G_f| = n$ then the following facts are equivalent:*

(i) $F(\alpha_i) = \sigma_F(\alpha_i)$ for all $i = 1, \ldots, n$.

(ii) $\sigma_F \in Z(G_f)$.

(iii) $\exists p \in \mathbb{Z}$ prime, $p \nmid d$, such that $F(\alpha) \equiv \alpha^p \bmod pS$.

PROOF.
(i) $\Leftrightarrow$ (ii): Let σ_i be the element of G_f such that $\sigma_i(\alpha) = \alpha_i$. Then:

$$\sigma_F(\alpha_i) = \sigma_F(\sigma_i(\alpha)) = \sigma_F \sigma_i(\alpha)$$

and

$$\varphi_F(\alpha_i) = F(\alpha_i) = F(\sigma_i(\alpha)) = \sigma_i(F(\alpha)) = \sigma_i \sigma_F(\alpha)$$

Therefore

$$\sigma_F(\alpha_i) = \varphi_F(\alpha_i)\ \forall i = 1, \ldots, n \quad \Leftrightarrow$$
$$\Leftrightarrow \quad \sigma_F \sigma_i(\alpha) = \sigma_i \sigma_F(\alpha)\ \forall i = 1, \ldots, n \quad \Leftrightarrow$$
$$\Leftrightarrow \quad \sigma_F \sigma_i = \sigma_i \sigma_F\ \forall i = 1, \ldots, n \quad \Leftrightarrow \quad \sigma_F \in Z(G_f).$$

(ii) $\Rightarrow$ (iii): By proposition 5, if $\sigma_F \in Z(G_f)$ then there exist infinitely many primes $p \in \mathbb{Z}$ such that $p \nmid d$ and $\sigma_F(u) \equiv u^p \bmod pS$ for all $u \in S$.

In particular, there exists $p \in \mathbb{Z}$ prime such that $\sigma_F(\alpha) \equiv \alpha^p \bmod pS$ and, since $\sigma_F = F(\alpha)$, we have that $F(\alpha) \equiv \alpha^p \bmod pS$.

(iii) $\Rightarrow$ (ii): If $Q_1, \ldots, Q_r$ are the primes in S lying over p then $F(\alpha) \equiv \alpha^p \bmod pS$ and therefore $F(\alpha) \equiv \alpha^p \bmod Q_i$ for all $i = 1, \ldots, r$.

Since $\sigma_F(\alpha) = F(\alpha)$, the restriction of σ_F, for every Q_i, is a Frobenius automorphism of S/Q_i over $\mathbb{Z}/p\mathbb{Z}$. Therefore, $\sigma_i^{-1} \sigma_F \sigma_i = \sigma_F$ for all $\sigma_i \in G_f$, and $\sigma_F \in Z(G_f)$. □

5.3 The algorithm

Input: A monic irreducible polynomial $f \in \mathbb{Z}[x]$.

Output: The elements of the Galois group G_f and their action on the roots of f if G_f is abelian and, otherwise, the statement that G_f is not abelian.

(1) Any polynomial $F \in \mathcal{A}$ is of the form

$$F = \frac{1}{d} \sum_{i=0}^{n-1} c_i x^i.$$

Consider a bound K for the absolute values of the c_i's:

$$|c_i| \leq |d|^{1/2} n(n-1)^{(n-1)/2} |\alpha_1|_\infty^{n(n-1)/2+1} := K.$$

(This is a theoretical bound: it can be improved heuristically). The computation of the discriminant can be avoided by using Mahler's bound: if $f(x) = \sum_{i=0}^n a_i x^i$ then

$$|d| < n^n \left(\sum_{i=0}^n |a_i|\right)^{2n-2}.$$

Set $C := \{\alpha\}$ and $m := 0$.

(2) Choose a prime p of $\mathbb{Z}$ not dividing the discriminant d of f and such that

$$p < (4 \log(|d|) + 2.5n + 5)^2 =: B,$$

where B is the Lagarias and Odlyzko bound.

(3) Factorize f into irreducible factors modulo p.

(3.1) If the irreducible factors modulo p have different degrees then $|G_f| \neq n$, and so, G_f is not abelian. **Return "G_f is not abelian".**

(3.2) If all the irreducible factors modulo p have the same degree then go to step (4).

(4) Compute an integer k such that $p^{2^k} > 2K$.

(5) Apply Newton-Lifting to $F(\alpha) \equiv \alpha^p \bmod pS$.

A polynomial F of degree smaller than n is obtained.

(5.1) If $F(\alpha)$ is not a root of F, then G_f is not abelian. **Return "G_f is not abelian".**

(5.2) If $F(\alpha)$ is a root of F go to step (6).

(6) Set $C := C \bigcup \{F^l(\alpha) : l \in \mathbb{N}\}$, where F^l is the composition of F l times. C is the set of roots of f obtained as polynomial functions of α during the procedure.

(6.1) If $\#C = n$ then G_f is abelian and the action of all its elements over the roots of f has been explicitely determined.
Return "G_f is abelian" and END.

(6.2) If $\#C < n$, go to step (7).

(7) Set m:=m+1.

m is the number of primes not dividing d and smaller than B that have been chosen during the procedure. Let M be the total number of primes not dividing d and smaller than B.

(7.1) If $m < M$ then go to step (2) and choose another prime.

(7.2) If $m = M$ then G_f is not abelian.
Return "G_f is not abelian".

5.4 Correctness of the algorithm

Next the correctness of the algorithm is shown. In the algorithm, the decisions about the abelianity of G_f appear in steps (3.1), (5.1), (6.1) and (7.2).

Correctness of (3.1): By corollary 2, if the irreducible factors of f modulo p have different degrees then $|G_f| \neq n$. Due to proposition 1, G_f abelian implies $|G_f| = n$ and we can conclude in this case that G_f is not abelian.

Correctness of (5.1): Assume that G_f is abelian. Then, as shown by Acciaro and Klüners in [1], by applying Newton-Lifting to $F(\alpha) \equiv \alpha^p \bmod pS$, we obtain a polynomial F of degree smaller than n such that $F(\alpha)$ is a root of f. But this is a contradiction because in step (5.1) $F(\alpha)$ is not a root of f. So, we can conclude that G_f is not abelian.

Correctness of (6.1): If $\#C = n$ then we have obtained all the roots of f as polynomial functions of α. This shows up that α is a primitive element of the splitting field L of f over $\mathbb{Q}$. So, $|G_f| = n$.

Let F_j be the polynomials obtained in step (5) for every chosen prime and such that $F_j(\alpha) = \alpha_j$. We are within the conditions of theorem 1 and $F_j(\alpha) \equiv \alpha^p \bmod pS$ for some prime p which does not divide d. Then, by theorem 1, $\sigma_{F_j} \in Z(G_f)$ and $\sigma_{F_j}(\alpha_i) = F_j(\alpha_i)$ for all $i = 1, \ldots, n$. This implies that we have an element of the center of G_f and moreover we know its action on the roots of f.

We have also that $F_j^l(\alpha_i) = \sigma_{F_j}^l(\alpha_i)$ for all $i = 1, \ldots, n$ and $l \in \mathbb{N}$, and $\sigma_{F_j}^l \in Z(G_f)$ for all $l \in \mathbb{N}$, because $Z(G_f)$ is a group.

Since for every root α_i of f there exists a pair $(j, l) \in \mathbb{N} \times \mathbb{N}$ verifying $\alpha_i = F_j^l(\alpha)$ (because $\#C = n$), we have $\sigma_{F_j}^l(\alpha) = \alpha_i$, and thus we have n different elements of $Z(G_f)$. Since $|G_f| = n$ we conclude that $G_f = Z(G_f)$ and G_f is abelian. Moreover, we know the action on the roots of f of every automorphism of G_f.

Correctness of (7.2): By proposition 6, if $|G_f| = n$ then each automorphism $\sigma \in G_f$ verifies $\sigma(\alpha) \equiv \alpha^p \bmod Q$ where Q is a prime lying over p, for some prime $p < (4log|d|+2.5n+5)^2$.

If G_f is abelian then $\sigma(\alpha) \equiv \alpha^p \bmod pS$. By Lemma 2 there exists $F \in \mathcal{A}$ such that $\sigma = \sigma_F$ and then $F(\alpha) \equiv \alpha^p \bmod pS$.

Therefore, if G_f is abelian and we have gone through all the primes smaller than B not dividing the discriminant, we must have found all the roots of f as polynomial functions of α. Otherwise, G_f is not abelian.

5.5 Remark

The factorization of f modulo a prime p is a cheap operation, so it is interesting to factorize f modulo several primes as a way to discard that G_f has order n, or to see the cycle type of the automorphisms associated to those primes.

6. EXAMPLES

EXAMPLE 1.

$$f_1(x) = x^6 - 32x^4 + 160x^3 - 320x^2 + 384x - 256$$

$p = 7$ is a prime which does not divide the discriminant of f_1, and

$$f_1 \equiv (x+2)(x+6)(x^2+3x+6)(x^2+3x+5) \bmod (7).$$

Since the factors of $f_1 \bmod (7)$ have different degrees, we can conclude that G_{f_1} is not abelian.

EXAMPLE 2.

$$f_2(x) = x^6 - 42x^4 + 80x^3 + 441x^2 - 1680x + 4516$$

$p = 5$ is a prime which does not divide the discriminant and

$$f_2 \equiv (x^3 + 4x + 3)(x^3 + 4x + 2) \bmod (5).$$

$k \in \mathbb{N}$ such that $5^{2^k} > 2K$ can be taken as $k = 6$.

Applying Newton-Lifting we obtain

$$\begin{aligned} dF(x) \;=\; & -9645354591859453240701x^5 \\ & +9741221266805364035660x^4 \\ & +1162450959966338295578 5x^3 \\ & +5015977851630218245820x^2 \\ & -1153791572506696752738 5x \\ & -476632324842757706770 \end{aligned}$$

Since $f_2(2) = 2952 = 2^3\ 3^2\ 41$, $f_2 \equiv x^2(x+1)^4 \bmod 2$ and $f_2 \equiv (x+1)^6 \bmod 3$, 2 and 3 divide the discriminant. But $f_2 \equiv (x+21)(x+17)(x+39)(x+11)(x+32)(x+3) \bmod 41$. So, $p = 41$ is a prime which does not divide d and f_2 splits completely modulo 41.

Let α be the root of f_2 in $\mathbb{Z}_{41}$ which is congruent to 20 modulo 41. It is easy to check that $F(20) \equiv -13 \bmod 41$ and since -13 is not a root of f_2 modulo 41, we can conclude that $F(\alpha)$ is not a root of f_2. So, G_{f_2} is not abelian.

EXAMPLE 3.

$$f_3(x) = x^8 - 2x^6 + 4x^4 - 8x^2 + 16$$

Since

$$f_3 \equiv (x^4+2x^3+x^2+3x+4)(x^4+5x^3+x^2+4x+4) \bmod (7),$$

$p = 7$ *is a prime not dividing the discriminant.* $k \in \mathbb{N}$ *such that* $7^{2^k} > 2K$ *can be taken as* $k = 6$.

Applying Newton-Lifting we obtain

$$dF(x) = 134217728000000x^7.$$

Since $f_3(3) = 5371 = 41\ 131$, *this time* f_3 *will be factorized modulo* 131*:* $f_3 \equiv (x+88)(x+43)(x+126)(x+79)(52+x)(x+5)(x+3)(x+128) \bmod (131)$. *Let* α *be the root of* f_3 *which is congruent to* 43 *modulo* 131.

It is easy to check that $F(\alpha) \equiv 79 \bmod 131$ *which is another root of* f_3 *modulo* 131. *Using the* 131*–adic expansion of the roots of* f_3, *we can check that* $F(\alpha)$ *is a root of* f_3. *Since* f_3 *has two factors of degree* 4 *modulo* 7, *the corresponding element of* G_f *must be a product of two cycles of order* 4 *and thus we can obtain the other* 2 *roots of* f_3 *in terms of* α*:* $F^2(\alpha)$ *and* $F^3(\alpha)$. *These are, effectively, the roots of* f_3 *congruent to* 3 *and* 126 *modulo* 131.

Next we choose now another prime: $p = 3$. *Then we obtain*

$$dF_2(x) = -536870912000000x^3.$$

Now it is checked that $F_2(\alpha)$ *is the root of* f_3 *congruent to* 5 *modulo* 131. *The other roots obtained are the roots congruent to* 3 *and* 52 *modulo* 131.

Next we choose now another prime: $p = 19$. *And* f_3 *is now factorized modulo* 19*:*

$$f_3 \equiv (x^2+5x+17)\cdot(x^2+11x+17)\cdot \cdot(x^2+14x+17)\cdot(x^2+8x+17) \bmod (19).$$

Then we obtain

$$\begin{aligned} dF_3(x) \quad = \quad & 134217728000000x^7 - 268435456000000x^5 \\ & +536870912000000x^3 - 1073741824000000x \end{aligned}$$

Now $F_3(\alpha)$ *is the root of* f_3 *congruent to* 3 *modulo* 131, *which we have already obtained before.*

So, we choose again another prime, for example, $p = 23$. *Then,*

$$dF_4(x) = 536870912000000x^3,$$

which agrees with $-dF_2(x)$. *It can be checked that* $F_4(\alpha)$ *is the root of* f_3 *congruent with* 88 *modulo* 131, *which is the last root of* f *to be described in terms of* α.

Therefore we conclude that G_f *is abelian.*

7. COMPLEXITY

Acciaro and Klüners in [1] conclude that their algorithm runs in time that is polynomial in the size of p and $f(x)$ for a given prime p.

We will apply their method to, at most, all the primes smaller than $(4log|d| + 2.5n + 5)^2$.

Mahler's bound on the discriminant of a polynomial shows that, if $f(x) = \sum_{i=0}^{n} a_i x^i$, then

$$|d| < n^n (\sum_{i=0}^{n} |a_i|)^{2n-2}.$$

Therefore every prime to be used is smaller than

$$(4n\log(n) + (2n-2)\log(\sum_{i=0}^{n} |a_i|) + 2.5n + 5)^2,$$

which is also an upper bound on the number of primes.

So, the algorithm of Acciaro and Klüners runs in polynomial time in the size of f.

The other steps of our algorithm that we must take into account are the verification of $F(\alpha)$ as a root of f, and the factorization modulo a prime p: but it is known that these operations are also polynomial in the size of f and p, and with the same reasoning as before, we can conclude that our algorithm runs in polynomial time in the size of f.

8. REFERENCES

[1] V. Acciaro, J. Klüners, *Computing automorphisms of abelian number fields*, Math. Comp. 68, no. 227, 1179-1186, 1999.

[2] E. Bach, J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. 65 (1996), 1717-1735.

[3] J. W. S. Cassels, *Local fields*, London Math. Soc., Student Texts 3, Cambridge University Press, 1986.

[4] G. E. Collins, M. E. Encarnación, *Efficient racional number reconstruction*, J. Symb. Comput. 20, 287-297, 1995.

[5] J. D. Dixon, *Exact solution of linear equations using p-adic expansions*, Numer. Math. 40, 137-141, 1982.

[6] J. D. Dixon, *Computing subfields in algebraic number fields*, J. Austral. Math. Society 49, 434-448, 1990.

[7] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Springer-Verlag, 1974.

[8] J. Klüners, *Über die Berechnung von Automorphismen und Teilkörpern algebraischer Zahlkörper*, Dissertation Ph. D. Thesis, Berlin, 1997.

[9] J. C. Lagarias, A. M. Odlyzko, *Effective version of the Chebotarev density theorem*, in Algebraic number fields (L-functions and Galois properties), A Frolich ed., pp. 409-464, Academic Press, London, 1977.

[10] S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput. 14, 184-195, 1985.

[11] S. Lang, *Algebra*, Addison-Wesley, Reading, Massachusetts, 1974.

[12] H. W. Lenstra, *Algorithms in algebraic number theory*, Bulletin of the Am. Math. Society, vol 26, no. 2, April 1992.

[13] K. Mahler, *p-adic numbers and their functions*, Cambridge University Press, 1981.

[14] D. A. Marcus, *Number fields*, Universitext, Springer Verlag, 1977.

[15] P. Stevenhagen, H. W. Lenstra Jr., *Chebotarëv and his density theorem*, The Mathematical Intelligencer, vol. 18, no. 2, 1996.

[16] B. L. van der Waerden, *Modern Algebra, vol I*, 1953.