Upper Bounds on the Complexity of some Galois Theory Problems

V. Arvind and Piyush P Kurur
Institute of Mathematical Sciences, C.I.T Campus,
Chennai 600113, India
{arvind,ppk}@imsc.res.in

December 19, 2018

Abstract

Assuming the generalized Riemann hypothesis, we prove the following complexity bounds: The order of the Galois group of an arbitrary polynomial $f(x) \in \mathbb{Z}[x]$ can be computed in $\mathrm{P}^{\#\mathrm{P}}$. Furthermore, the order can be approximated by a randomized polynomial-time algorithm with access to an NP oracle. For polynomials f with solvable Galois group we show that the order can be computed exactly by a randomized polynomial-time algorithm with access to an NP oracle. For all polynomials f with abelian Galois group we show that a generator set for the Galois group can be computed in randomized polynomial time.

1 Introduction

A fundamental problem in computational algebraic number theory is to determine the Galois group of a polynomial $f(x) \in \mathbb{Q}[x]$. Formally, in this paper we study the computational complexity of the following problem:

Problem 1.1. *Given a nonzero polynomial $f(x)$ over the rationals $\mathbb{Q}$,*

(a) determine the Galois group of f over $\mathbb{Q}$.

(b) determine the order of the Galois group of f over $\mathbb{Q}$.

An *extension* of a field K is a field L that contains K (written L/K). If L/K is a field extension then L is a vector space over K and its dimension, denoted by $[L : K]$ is called its *degree*. If $[L : K]$ is finite then L/K is a *finite* extension. If L/M and M/K are finite extensions then $[L : K] = [L : M].[M : K]$.

Let $K[x]$ denotes the ring of polynomials with indeterminate x and coefficients from the field K. A polynomial $f(x) \in K[x]$ is *irreducible* if it has no nontrivial factor over K. The *splitting field* K_f of a polynomial $f(x) \in K[x]$ is the smallest extension L of K such that f factorizes into linear factors in L.

An extension L/K is *normal* if for any irreducible polynomial $f(x) \in K[x]$, f either splits in L or has no root in L. An extension L/K is *separable* if for all irreducible polynomials $f(x) \in K[x]$ there are no multiple roots in L. A normal and separable finite extension L/K is called a *Galois extension*.

An *automorphism* of a field L is a field isomorphism $\sigma : L \to L$. The *Galois group* $Gal\,(L/K)$ of a field extension L/K is the subgroup of the group of automorphisms of L that leaves K fixed: i.e. for every $\sigma \in Gal\,(L/K)$, $\sigma(a) = a$ for all $a \in K$. By the Galois group of a polynomial $f \in K[x]$ we mean $Gal\,(K_f/K)$.

Roots of polynomials over $\mathbb{Q}$ are *algebraic numbers*. The *minimal polynomial* $T \in \mathbb{Q}[x]$ of an algebraic number α is the unique monic polynomial of least degree with α as a root. *Algebraic integers* are roots of monic polynomials in $\mathbb{Z}[x]$. A *number field* is a finite extension of $\mathbb{Q}$. For an algebraic number α, $\mathbb{Q}(\alpha)$ denotes the smallest number field that contains α. If $f(x)$ is the minimal polynomial of α then $\mathbb{Q}(\alpha)$ can be identified with the quotient $\mathbb{Q}[x]/(f(x)\mathbb{Q}[x])$. Every number field K has an element α such that $K = \mathbb{Q}(\alpha)$ (see [7, Theorem 4.6 Chap.V]). Such elements are called *primitive* elements of the field K.

Let $f \in \mathbb{Q}[x]$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}_f$. A well known lemma [14] states that $\mathbb{Q}_f$ has a primitive element of the form $\sum_{i=1}^{n} c_i\alpha_i$ for integers c_i. The proof actually yields a probabilistic version which states that $\sum_{i=1}^{n} c_i\alpha_i$ is primitive for most c_i.

Lemma 1.2. *Let $f \in \mathbb{Q}[x]$ be a degree n polynomial with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. For a random choice of integers $c_1, c_2, \ldots, c_n$ such that $size(c_i) \leq n^2$ the algebraic integer $\theta = \sum_{i=1}^{n} c_i\alpha_i$ is such that $L = \mathbb{Q}(\theta)$ with probability $1 - \frac{1}{2^{O(n^2)}}$.*

A polynomial $f(x) \in \mathbb{Q}[x]$ is said to be solvable by radicals if the roots of f can be expressed, starting with the coefficients of f, using only field operations and taking r^{th} roots for integer r. Galois showed that a polynomial is solvable by radicals if and only if its Galois group is solvable.

Let L be a number field and O_L be the ring of algebraic integers in L. We can write O_L as $O_L = \{\sum_{i=1}^{N} a_i\omega_i \mid a_i \in \mathbb{Z}\}$ where $\omega_1, \omega_2, \ldots, \omega_N$ is its $\mathbb{Z}$-basis. The *discriminant* d_L of the field L is defined as the determinant of the matrix $(\mathrm{Tr}(\omega_i\omega_j))_{i,j}$ where $\mathrm{Tr} : L \to \mathbb{Q}$ is the trace map. The discriminant d_L is always a nonzero integer. Let T be any polynomial of degree N. Then the discriminant $d(T)$ of the polynomial T is defined as $d(T) = \prod_{i \neq j}(\theta_i - \theta_j)$, where $\theta_1, \theta_2, \ldots, \theta_N$ are the N distinct roots of T (i.e. all the conjugates of θ). The following is important property that relates $d(T)$ and d_L ([2, Proposition 4.4.4]).

Proposition 1.3. *Let L be a number field and T be the minimal polynomial of a primitive element θ of L. Then $d_L \mid d(T)$. More precisely, $d(T) = d_L \cdot t^2$, for an integer t.*

Let size(a) denote the length of the binary encoding of an integer a. For a rational $r = p/q$ such that $gcd(p, q) = 1$, let size(r) = size(p) + size(q). A polynomial is encoded as a list of its coefficients. For a polynomial $f(x) =$

$\sum a_i x^i \in \mathbb{Q}[x]$ we define size$(f) = \sum$size(a_i). Thus, for an algorithm taking a polynomial f as input, the input size is $size(f)$.

For any polynomial $g(x) = a_0 + a_1 x + \ldots + a_n x^n$ in $\mathbb{Z}[x]$, let $|g|_2 = \sqrt{\sum a_i^2}$. Applying an inequality [4] which bounds every root η of g by $|g|_2$, we obtain the following.

Theorem 1.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n with splitting field L. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f. Consider an element of the form $\theta = \sum c_i \alpha_i$, $c_i \in \mathbb{Z}$, and let T be the minimal polynomial of θ. Then $|d(T)| \leq (2c|f|_2)^{N^2}$, where $c = \max\{|c_i| : 1 \leq i \leq n\}$. As a consequence, $d_L \leq (2^{n^2}|f|_2)^{n!^2}$ and $\log d_L \leq (n+1)!^2$.size(f).*

The Galois group of a polynomial $f(x) \in K[x]$ is completely determined by its action on the roots of f in K_f. We assume w.l.o.g throughout this paper that f is square-free. Otherwise, we can replace f by $f/gcd(f.f')$ which is square-free with the same Galois group. Thus, if we label the n distinct zeroes of f, we can consider the Galois group as a subgroup of the symmetric group S_n. Notice that this subgroup is determined only up to conjugacy (as the labeling of the zeroes of f is arbitrary). Since every subgroup of S_n has a generator set of size $n-1$ (c.f. [12] and [9]), we can specify the Galois group in size polynomial in n. By computing the Galois group of a polynomial f we mean finding a small generator set (polynomial in n) for it as a subgroup of S_n.

We now state Landau's result on computing the Galois group of a polynomial f. Its worst case running time is exponential in size(f).

Theorem 1.5 ([5])**.** *Given a polynomial $f \in F[x]$, where the number field F is given as a vector space over $\mathbb{Q}$, the Galois group G of f over F can be computed in time polynomial in $|G|$ and* size(f).

The extended abstract is organized as follows: In Sect. 2 we explain the Chebotarev density theorem in a form that is useful to us. In Sect. 3 we give a polynomial time algorithm making a single query to #P to compute the order of the Galois group of a polynomial $f(x) \in \mathbb{Q}$. In Sect. 4 we show that if the polynomial is solvable by radicals the order of its Galois group can be computed by a randomized algorithm with an NP oracle. Finally in Sect. 5 we show that if the Galois group of f is abelian then it can be computed by a randomized polynomial time algorithm. For the definitions of various complexity classes the reader can consult any complexity theory text like [1].

2 Chebotarev Density theorem

The main tool in the proofs of our complexity results is the Chebotarev density theorem. In this section we explain the theorem statement and also state it in a form that is suitable for our applications.

Let L be a Galois number field and O_L be the ring of algebraic integers in L. Let $n = [L : \mathbb{Q}]$ be the degree of L. For any prime $p \in \mathbb{Q}$ consider the principal

ideal pO_L generated by p (which we denote by p). The ideal p factorizes in O_L as $p = \mathfrak{p}_1^e \mathfrak{p}_2^e \ldots \mathfrak{p}_g^e$ for some positive integer e. For each i, $O_L/\mathfrak{p}_i$ is a finite field extension of $\mathbb{F}_p$ with p^f elements for some positive integer f. Furthermore $efg = n$.

The prime p is said to be *ramified* in L if $e > 1$ and *unramified* otherwise. It is a basic fact about number fields that a prime p is ramified in L if and only if p divides the discriminant of L (see [11, Theorem 1, pg. 238]).

Let p be an unramified prime with factorization $p = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_g$ in O_L. Corresponding to the Frobenius automorphism of the finite field $O_L/\mathfrak{p}_i$, there is an element denoted $\left(\frac{L/\mathbb{Q}}{\mathfrak{p}_i}\right)$ in the Galois group $G = Gal\,(L/\mathbb{Q})$ known as the Frobenius element of $\mathfrak{p}_i$, for $i = 1, 2, \ldots, g$. Furthermore, it is known that the set

$$\left[\frac{L/\mathbb{Q}}{p}\right] = \left\{\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right) : \mathfrak{p}|p\right\}$$

is a conjugacy class in the Galois group G. For any conjugacy class C of G let $\pi_C(x)$ be the number of unramified primes less that x such that $\left[\frac{L/\mathbb{Q}}{p}\right] = C$. We have the following theorem:

Theorem 2.1 (Chebotarev's density theorem)**.** *Let $L/\mathbb{Q}$ be a Galois extension and $G = Gal\,(L/\mathbb{Q})$ be its Galois group. Then for every conjugacy class C of G, $\pi_C(x)$ converges to $\frac{|C|}{|G|} \cdot \frac{x}{\ln x}$ as $x \to \infty$.*

In order to apply the above theorem in a complexity-theoretic context, we need the following effective version due to Lagarias and Odlyzko [3] proved assuming the GRH.

Theorem 2.2. *Let $L/\mathbb{Q}$ be a Galois extension and $G = Gal\,(L/\mathbb{Q})$ be its Galois group. If the GRH is true then there is an absolute constant x_0 such that for all $x > x_0$:*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\frac{x}{\ln x}\right| \leq \frac{|C|}{|G|} x^{1/2} \ln d_L + x^{1/2} \ln x . |G|.$$

An unramified prime p such that $\left[\frac{L/\mathbb{Q}}{p}\right] = \{1\}$ is called a *split prime*. By definition, $\pi_1(x)$ denotes the number of split primes $p \leq x$.

Corollary 2.3. *Let $G = Gal\,(L/\mathbb{Q})$ for a Galois extension $L/\mathbb{Q}$. If the GRH is true then there is an absolute constant x_0 such that for all $x > x_0$:*

$$\left|\pi_1(x) - \frac{1}{|G|}\frac{x}{\ln x}\right| \leq \frac{1}{|G|} x^{1/2} \ln d_L + x^{1/2} \ln x . |G|.$$

3 Computing the order of Galois Groups

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n without multiple roots and let L denote the splitting field of f. Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the set of roots of f.

As mentioned before, the Galois group $G = Gal\,(L/\mathbb{Q})$ can be seen as a subgroup of S_n. Each $\sigma \in G$, when considered as a permutation in S_n, can be expressed as a product of disjoint cycles. Looking at the lengths of these cycles we get the *cycle pattern* $\langle m_1, m_2, \ldots, m_n \rangle$ of σ, where m_i is the number of cycles of length i, $1 \leq i \leq n$. We have $n = \sum_{i=1}^{n} m_i$.

If p is a prime such that $p \nmid d(f)$, we can factorize $f = g_1 g_2 \ldots g_s$ into its distinct irreducible factors g_i over $\mathbb{F}_p$. Looking at the degrees of these irreducible factors we get the *decomposition pattern* $\langle m_1, m_2, \ldots, m_n \rangle$ of $f (\text{mod } p)$, where m_i is the number of irreducible factors of degree i.

We now state an interesting fact from Galois theory (see [14, page 198] and [7, Theorem 2.9, Chap. VII]).

Theorem 3.1. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n such that $d(f) \neq 0$, and let L denote its splitting field. Let $G = Gal\,(L/\mathbb{Q})$. Let p be a prime such that $p \nmid d(f)$. Then there is a conjugacy class C of G such that for each $\sigma \in C$ the cycle pattern of σ is the same as the decomposition pattern of f factorized over $\mathbb{F}_p$. Furthermore, if $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are the n roots of f in its splitting field and if $\mathbb{F}_{p^m}$ is the extension of $\mathbb{F}_p$ where $f \pmod p$ splits then there is an ordering of the roots $\{\alpha'_1, \alpha'_2, \ldots, \alpha'_n\}$ of f in $\mathbb{F}_{p^m}$ such that for all indices k and l, $\sigma(\alpha_k) = \alpha_l$ if and only if the Frobenius automorphism $x \mapsto x^p$ of $\mathbb{F}_{p^m}$ maps α'_k to α'_l.*

For any prime p that divides the order of the Galois group there is an element whose order is divisible by p. This can happen only if there is a prime q such that the decomposition pattern of $f \pmod q$ contains only the integers p and 1 (using Theorem 3.1). Furthermore using the effective Chebotarev density theorem (Theorem 2.2) we can show that there is a q with size $size(f)^{O(1)}$ satisfying the above property. So to check whether p divides the order of the Galois group we guess such a q. This leads to the following theorem.

Theorem 3.2. *Assuming GRH, the following problem is in* NP*: Given a prime $p \leq n$, and a monic polynomial $f \in \mathbb{Z}[x]$ with $d(f) \neq 0$ as input, test if p divides the order of the Galois group of f. As a consequence, the set of prime factors of $|Gal\,(\mathbb{Q}_f/\mathbb{Q})\,|$ can be computed in* P^{NP}.

Now for the main result of this section.

Theorem 3.3. *Assuming GRH, the order of the Galois group of a monic polynomial $f \in \mathbb{Z}[x]$ can be computed in* $\mathrm{P}^{\#\mathrm{P}}$.

The algorithm first count the number of split primes (with a certain exponentially small error) less than a suitably large x ($size(x) = size(f)^{O(1)}$) using a

single #P query. The order of the Galois group is the nearest integer to $\frac{1}{\pi_1(x)} \frac{x}{\ln x}$ which can be computed in polynomial time.

To the best of our knowledge, this is the first polynomial-space bounded algorithm for the problem. Next we consider the approximate counting problem.

Definition 3.4. *A randomized algorithm $\mathcal{A}$ is an r-approximation algorithm for a #P function f with error probability $\delta < \frac{1}{2}$ if for all $x \in \{0,1\}^*$:*

$$Prob_y \left[|1 - \frac{\mathcal{A}(x,y)}{f(x)}| \leq r(|x|) \right] \geq 1 - \delta,$$

where y is a uniformly chosen random string used by the algorithm $\mathcal{A}$ on input x.

Stockmeyer [13] showed that for any #P function there is a $n^{-O(1)}$-approximation $\mathrm{BPP}^{\mathrm{NP}}$ algorithm. We can use Stockmeyer's result to approximate $\pi_1(x)$ within an inverse polynomial error and use this approximation instead. This yields the algorithm in the following theorem.

Theorem 3.5. *Let $f(x) \in \mathbb{Z}[x]$ be a degree n polynomial, G be its Galois group, and s denote size(f). For any constant $c > 0$ there is a $\mathrm{BPP}^{\mathrm{NP}}$ algorithm that computes an approximation A of $|G|$ such that*

$$\left(1 - \frac{1}{s^c}\right) A \leq |G| \leq \left(1 + \frac{1}{s^c}\right) A.$$

with probability greater than $\frac{2}{3}$.

We now derive a useful lemma as an immediate consequence of the above result.

Lemma 3.6. *Let f and g be monic polynomials in $\mathbb{Z}[x]$ with nonzero discriminant. Suppose the splitting field $\mathbb{Q}_g$ of g is contained in $\mathbb{Q}_f$ of f and $[\mathbb{Q}_f : \mathbb{Q}_g]$ is a prime power p^l. There is a $\mathrm{BPP}^{\mathrm{NP}}$ algorithm that computes $[\mathbb{Q}_f : \mathbb{Q}_g]$ exactly, assuming that $|Gal\,(\mathbb{Q}_g/\mathbb{Q})\,|$ is already computed.*

4 Computing the order of solvable Galois Groups

In this section we show that if the Galois group G of $f \in \mathbb{Z}[x]$ is *solvable* then $|G|$ can be computed exactly in $\mathrm{BPP}^{\mathrm{NP}}$, assuming GRH. In fact, we show that for solvable Galois groups, finding $|G|$ is polynomial-time reducible to approximating $|G|$.

To begin with we need a test for solvability by radicals. A naive application of Galois' theorem gives an exponential time algorithm (using Theorem. 1.5). An important breakthrough was achieved by Landau and Miller when they gave a deterministic polynomial time algorithm to check whether a polynomial

is solvable by radicals without actually computing the Galois group (see. [6]). We make use of results from [6]. We begin by recalling some definitions.

A group G is said to be *solvable* if there is a *composition series* of G, $G = G_0 \rhd G_1 \rhd \ldots \rhd G_t = 1$ such that G_i/G_{i+1} is a cyclic group of prime order. Throughout this section by composition series we mean such a composition series.

A Galois extension K/F is said to be *solvable* if $Gal\,(K/F)$ is a solvable group. Let $G = G_0 \rhd G_1 \rhd \ldots \rhd G_t = 1$ be a composition series of G. There is a corresponding tower of fields $F = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_t = K$ such that $Gal\,(K/E_i) = G_i$. Moreover if K/F is Galois then by the fundamental theorem of Galois, since $G_i \rhd G_{i+1}$, the extension E_{i+1}/E_i is Galois.

At this point we recall some permutation group theory (c.f. [15]): Let G be a subgroup of S_n acting on a set $\Omega = \{1, 2, \ldots, n\}$ of n elements. G is said to be *transitive* if for every pair of distinct elements $i, j \in \Omega$, there is a $\sigma \in G$ such that σ maps i to j, written as $i^\sigma = j$. A *block* is a subset $B \subseteq \Omega$ such that for every $\sigma \in G$ either $B^\sigma = B$ or $B^\sigma \cap B = \emptyset$. If G is transitive then under G-action blocks are mapped to blocks, so that starting with a block $B_1 \subseteq \Omega$ we get a *complete block system* $\{B_1, B_2, \ldots, B_s\}$ which is a partition of Ω. Notice that singleton sets and Ω are blocks for any permutation group. These are the *trivial* blocks. A transitive group G is *primitive* if it has only trivial blocks. Otherwise it is called *imprimitive*. A *minimal block* of an imprimitive group is a nontrivial block of least cardinality. The corresponding block system is a *minimal block system*.

The following result about solvable primitive permutation groups [10] has been used to show polynomial time bounds for several permutation group algorithms [9].

Theorem 4.1 (Pálfy's bound)**.** [10] *If $G < S_n$ is a solvable primitive group then $|G| \leq n^{3.25}$.*

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial and let G be the Galois group $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ which acts transitively on the set of roots $\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of f. Let $\{B_1, B_2, \ldots, B_s\}$ be the minimal block system of Ω under the action of G and H be the subgroup of G that setwise stabilizes all the blocks: i.e. elements of H map B_i to B_i for each i. Let $B_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, where $k = n/s$. Consider the polynomial $p(x) = \prod_{i=1}^{k}(x - \alpha_i) = \sum_{i=0}^{k} \delta_i x^i$.

In [6] it is shown that $p(x) \in \mathbb{Q}(\alpha_1)[x]$ and there is a polynomial time deterministic algorithm to find $p(x)$: the algorithm computes each coefficient δ_i as a polynomial $p_i(\alpha_1)$ with rational coefficients. In polynomial time we can compute a primitive element β_1 of $\mathbb{Q}(\delta_0, \delta_1, \ldots, \delta_k)$ [6] so that $\mathbb{Q}(\beta_1) = \mathbb{Q}(\delta_0, \delta_1, \ldots, \delta_k)$. Let $g(x) \in \mathbb{Z}[x]$ be the minimal polynomial of β_1. In the following theorem we recall some results from [6], suitably rephrased.

Theorem 4.2.

1. *The degree of $g(x)$ is s.*
2. *$H = Gal\,(\mathbb{Q}_f/\mathbb{Q}_g)$ and $Gal\,(\mathbb{Q}_g/\mathbb{Q}) = G/H$.*

3. *The Galois group* $Gal\,(\mathbb{Q}(B_1)/\mathbb{Q}(\beta_1))$ *acts primitively on* B_1.

Let $Gal\,(\mathbb{Q}(B_1)/\mathbb{Q}(\beta)) = G^{B_1} = G_0 \rhd G_1 \rhd \ldots \rhd G_t = 1$ be a composition series of the solvable group G^{B_1} and let $\mathbb{Q}(\beta_1) = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = \mathbb{Q}(B_1)$ be the corresponding tower of subfields of the extension $\mathbb{Q}(B_1)/\mathbb{Q}(\beta_1)$. Since K_{i+1}/K_i is an extension of prime degree for each i we have the following proposition.

Proposition 4.3. *For all* $0 \leq i < t$ *if* K' *be any field such that* $K_i \subseteq K' \subseteq K_{i+1}$ *then either* $K' = K_i$ *or* $K' = K_{i+1}$.

For each field K_j in the above tower, let θ_j be a primitive element, $0 \leq j \leq t$. I.e. $\mathbb{Q}(\theta_j) = K_j$ for each j. Let $h_j(x) \in K_{j-1}[x]$ be the minimal polynomial of θ_j over K_{j-1}. We can consider $h_j(x)$ as $h_j(x, \theta_{j-1})$, a polynomial over $\mathbb{Q}$ in the indeterminate x and the algebraic number θ_{j-1} as parameter. As before let $G = \cup_{i=1}^{s} H\sigma_i$. For each field K_j let K_{ij} be the conjugate field under the action of σ_i. More precisely, let $K_{ij} = K_j^{\sigma_i}$ and $\theta_{ij} = \theta_j^{\sigma_i}$. We have the following proposition which follows from the fact that σ_i is a field isomorphism which maps the extension $\mathbb{Q}(B_1)/\mathbb{Q}(\beta_1)$ to $\mathbb{Q}(B_i)/\mathbb{Q}(\beta_i)$, for each i.

Proposition 4.4.

1. $K_{i0} \subseteq K_{i1} \subseteq \ldots \subseteq K_{it}$ *forms a tower of fields of the extension* $\mathbb{Q}(B_i)/\mathbb{Q}(\beta_i)$ *corresponding to the composition series of* $Gal\,(\mathbb{Q}(B_i)/\mathbb{Q}(\beta_i))$.
2. $Gal\,(K_{it}/K_{ij}) = \sigma_i^{-1} G_j \sigma_i$.
3. $K_{ij} = \mathbb{Q}(\theta_{ij})$, *where* $\theta_{ij} = \theta_j^{\sigma_i}$.
4. *The minimal polynomial of* θ_{ij} *over the field* K_{ij-1} *is* $h_{ij}(x) = h_j(x, \theta_{ij-1})$.

For each i, let $\overline{h}_i(x)$ denote the minimal polynomial of θ_i over $\mathbb{Q}$ and let n_i be its degree. We have the following lemma:

Lemma 4.5. *Let* $n_i = deg(\overline{h}_i)$ *then* $n_0 = [\mathbb{Q}(\beta_1) : \mathbb{Q}]$ *and* $n_i = p_i n_{i-1}$, *where* $[K_i : K_{i-1}] = p_i$ *for each* i.

Let $E_i = \mathbb{Q}_{\overline{h}_i}$, $0 \leq i \leq t$. Notice that $\mathbb{Q}_f = E_t$ and $\mathbb{Q}_g = E_0$. We have the following theorem:

Theorem 4.6. *Let* p_i *be the order of* G_i/G_{i-1}. *For every* i *there is a* l_i *such that* $Gal\,(E_i/E_{i-1})$ *is an abelian group of order* $p_i^{l_i}$. *Furthermore* $Gal\,(E_i/E_{i-1})$ *is an elementary abelian* p_i*-group.*

Suppose we know $[\mathbb{Q}_g : \mathbb{Q}]$. Using Lemma 3.6 we can compute $[\mathbb{Q}_f : \mathbb{Q}]$ by finding $[E_i : \mathbb{Q}]$ for each $1 \leq i \leq t$ starting from $i = 1$. We will find $[\mathbb{Q}_g : \mathbb{Q}]$ recursively. It is also easy to generalize this algorithm for reducible polynomials $f(x) \in \mathbb{Q}[x]$. This gives the following theorem:

Theorem 4.7. *Assuming the GRH, there is a* $\mathrm{BPP}^{\mathrm{NP}}$ *procedure that takes as input a monic polynomial* $f \in \mathbb{Z}[x]$ *such that* $d(f) \neq 0$, *and computes* $|Gal\,(\mathbb{Q}_f/\mathbb{Q})|$ *exactly when* $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ *is solvable.*

5 Finding the Galois group of an abelian extension

Let f be a polynomial over $\mathbb{Z}[x]$ such that $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian. In this section we give a polynomial-time randomized algorithm that computes the Galois group (as a set of generators) with constant success probability.

Suppose $f \in \mathbb{Z}[x]$ is irreducible of degree n with Galois group G. Since G is a transitive subgroup of S_n, if G is abelian then $|G| = n$. Thus, given an irreducible $f \in \mathbb{Z}[x]$, the algorithm of Theorem 1.5 gives a $(\text{size}(f))^{O(1)}$ algorithm for testing if its Galois group is abelian, and if so, finding the group explicitly. On the other hand, when f is reducible with abelian Galois group, no polynomial time algorithm is known for computing the Galois group (c.f. Lenstra [8]). However, for any polynomial f testing if its Galois group is abelian can be done in polynomial time: we only need to test if the Galois group of each irreducible factors of f is abelian.

Let f be a polynomial over $\mathbb{Z}[x]$ such that $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian. Let $f = f_1 f_2 \ldots f_t$ be its factorization into irreducible factors f_i. Notice that if $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian then $Gal\,(\mathbb{Q}_{f_i}/\mathbb{Q})$ is abelian for each i. Consequently, each f_i is a primitive polynomial. Let $G = Gal\,(\mathbb{Q}_f/\mathbb{Q})$ and let $G_i = Gal\,(\mathbb{Q}_{f_i}/\mathbb{Q})$ for each i. Notice that $G \leq G_1 \times G_2 \times \ldots G_t$.

Let n_i be the degree of f_i. Since each f_i is a primitive polynomial, $|G_i| = n_i$. Let θ_i be any root of f_i, $1 \leq i \leq t$. Then, $\mathbb{Q}_{f_i} = \mathbb{Q}(\theta_i)$ for each i. Factorizing f_i in $\mathbb{Q}(\theta_i)$, we can express the other roots of f_i as $A_{ij}(\theta_i)$, where $A_{ij}(x)$ are all polynomials of degree at most n_i, $1 \leq j \leq n_i$. We can efficiently find these polynomials $A_{ij}(x)$ for $1 \leq i \leq t$, $1 \leq j \leq n_i$. Thus we can write $f_i(x) = \prod_{j=1}^{n_i}(x - A_{ij}(\theta_i))$, where θ_i is one of the roots of f_i. We have the following lemma:

Lemma 5.1. *Let θ be any root of f_i and let A_{ij} be polynomials of degree less than $\deg(f_i)$ such that $f_i(x) = \prod_{j=1}^{n_i}(x - A_{ij}(\theta))$. Then for $1 \leq j < deg(f_i)$, we have $A_{ij}(A_{ik}(\theta)) = A_{ik}(A_{ij}(\theta))$. Furthermore, for every $\sigma \in G_i$ there is an index $k, 1 \leq k \leq n_i$ such that for any root η of $f_i(x)$ we have $\sigma(\eta) = A_{ik}(\eta)$.*

From the above lemma it also follows that for each $i, 1 \leq i \leq t$, the polynomials A_{ij}, $1 \leq j \leq n_i$ are independent of the choice of the root θ of f_i because the Galois group is abelian.

Now, let σ_{ij} denote the unique automorphism of $\mathbb{Q}_{f_i}$ that maps θ to $A_{ij}(\theta)$ for every root θ of f_i. Since $G \leq G_1 \times G_2 \times \ldots \times G_t$, any element $\sigma \in G$ is a t-tuple $\sigma = \langle \sigma_{1j_1}, \sigma_{2j_2}, \ldots, \sigma_{tj_t} \rangle$, for indices $j_1, j_2, \ldots, j_t$. We will apply the Chebotarev density theorem to determine a generator set for G.

Let q be a prime such that $q \nmid d(f)$ and $\mathbb{F}_{q^m}$ be the extension of $\mathbb{F}_q$ where f splits. Observe that since G is abelian every conjugacy class of G is a singleton set. Let $\pi_g(x)$ denote the number of primes $p \leq x$ whose Frobenius corresponds to g. By Theorem 2.1 $\pi_g(x)$ converges to $\frac{x}{(\ln x)|G|}$. Furthermore using Theorem 2.2 we can show that for a random prime $p \leq x$, the probability that the Frobenius corresponding to p is g lies in the range $\left(\frac{1}{|G|} - \epsilon, \frac{1}{|G|} + \epsilon\right)$, $\epsilon = \frac{1}{x^{O(1)}}$.

Next, fix i and let $\{\alpha_1, \alpha_2, \ldots, \alpha_{n_i}\}$ be the roots of f_i. By Theorem 3.1, there is an ordering $\{\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_{n_i}\}$ of the roots of f_i in $\mathbb{F}_{q^m}$ such that the Frobenius automorphism $x \mapsto x^q$ maps $\overline{\alpha}_k$ to $\overline{\alpha}_l$ if and only if the element g (the unique Frobenius element corresponding to q) maps α_k to α_l. If the element $g = \langle \sigma_{1j_1}, \sigma_{2j_2}, \ldots, \sigma_{tj_t} \rangle$ we can determine σ_{ij_i} as follows: find the splitting field $\mathbb{F}_{q^k}$ of f_i. Since f_i is a primitive polynomial, $k \leq n_i$, thus $\mathbb{F}_{q^k}$ can be found efficiently.[1] Now, factorize f_i in $\mathbb{F}_{q^k}$. Pick any root $\overline{\theta} \in \mathbb{F}_{q^k}$ of f_i. Then $\overline{\theta}^q = A_{ij}(\overline{\theta})$ for exactly one polynomial A_{ij_i}, which can be found by trying all of them. This gives us σ_{ij_i}. Thus, we can determine g as a t-tuple in polynomial time, in a manner independent of the choice of the root $\overline{\theta}$ of f_i in $\mathbb{F}_{q^k}$.

We have the following almost uniform polynomial-time sampling algorithm from the Galois group G: Pick primes $p \nmid d(f)$ less that a suitably large x and recover corresponding Frobenius. It can be shown that if we choose $x \geq (n!)^{10}.\text{size}(f)^2$, the algorithm samples $g \in G$ with probability in the range $\left(\frac{1}{|G|} - \frac{1}{x^{1/4}}, \frac{1}{|G|} + \frac{1}{x^{1/4}}\right)$. We require the following lemma to complete the proof

Lemma 5.2. *Suppose we have a (almost) uniform sampling procedure $\mathcal{A}$ from a subgroup G of S_n. Then for every constant $c > 0$, there is a polynomial-time randomized algorithm with $\mathcal{A}$ as subroutine that outputs a generator set for G with error probability bounded by 2^{-n^c}.*

The above lemma implies the the following theorem.

Theorem 5.3. *There is a randomized polynomial time algorithm for computing a generator set for the Galois group of a polynomial $f \in \mathbb{Z}[x]$ if it is abelian.*

References

[1] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I & II.* ETACS monographs on theoretical computer science. Springer-Verlag, Berlin, 1988 and 1990.

[2] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1993.

[3] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields*, pages 409–464. Academic Press, London, 1977.

[4] E. Landau. Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques. *Bulletin de la Société de France*, 33:251–261, 1905.

[5] S. Landau. Polynomial time algorithms for galois groups. In J. Fitch, editor, *EUROSAM 84 Proceedings of International Symposium on Symbolic and Algebraic Computation*, volume 174 of *Lecture Notes in Computer Sciences*, pages 225–236. Springer, July 1984.

[1] In fact $k|n_i$ because k is the order of the corresponding Frobenius element which is in the Galois group of f_i, and the order of the Galois group is n_i.

[6] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *Journal of Computer and System Sciences*, 30:179–208, 1985.

[7] S. Lang. *Algebra*. Addison-Wesley Publishing Company, Inc, third edition, 1999.

[8] H. W. Lenstra Jr. Algorithms in algebraic number theory. *Bulletin of the American Mathematical Society*, 26(2):211–244, April 1992.

[9] E. M. Luks. Permutation groups and polynomial time computations. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 11:139–175, 1993.

[10] P. Pálfy. A polynomial bound for the orders of primitive solvable groups. *Journal of Algebra*, pages 127–137, July 1982.

[11] P. Ribenboim. *Classical theory of algebraic numbers*. Universitext. Springer, 1999.

[12] C. C. Sims. Computational methods in the study of permutation groups. *Computational problems in Abstract Algebra*, pages 169–183, 1970.

[13] L. Stockmeyer. On approximating algorithms for #P. *SIAM Journal of Computing*, 14:849–861, 1985.

[14] B. L. van der Waerden. *Algebra*, volume I. Springer-Verlag, seventh edition, 1991.

[15] H. Wielandt. *Finite Permutation Groups*. Academic Press, New York, 1964.