Solvability by Radicals is in Polynomial Time

(Preliminary Report)

Susan Landas*
Gary Lee Miller*

Mathematics Department
and
Laboratory for Computer Science
Massachusetts Institute of Technology

Every high school student knows how to express the roots of a quadratic equation in terms of radicals; what is less well-known is that this solution was found by the Babylonians a millennium and a half before Christ [Ne]. Three thousand years elapsed before European mathematicians determined how to express the roots of cubic and quartic equations in terms of radicals, and there they stopped, for their techniques did not extend. Lagrange published a treatise which discussed why the methods that worked for polynomials of degree less than five did not work for quintic polynomials [Lag], hoping to shed some light on the problem. Évariste Galois, the young mathematician who died in a duel at the age of twenty, solved it. In the notes he revised hastily the night before his death, he gave an algorithm which determines when a polynomial has roots expressible in terms of radicals. Yet of this algorithm, he wrote, "If now you give me an equation which you have chosen at your pleasure, and if you want to know if it is or is not solvable by radicals, I need do nothing more than to indicate to myself or anyone else the task of doing it. In a word, the calculations are impractical." [Ga].

They require double exponential time. Through the years other mathematicians developed alternate algorithms all of which, however, remained exponential. A major impasse was the problem of factoring polynomials, for until the recent

*This work partially supported by NSF grant MCS 800756-001 and ONR grant NOO14-80-C-022

breakthrough of Lenstra, Lenstra, and Lovász [L^2], all earlier algorithms had exponential running time. Their algorithm, which factors polynomials over the rationals in polynomial time, gave rise to a hope that some of the classical questions of Galois theory might have polynomial time solutions. We answer that the basic question of Galois theory — is a given polynomial, \( f(z) \), over the rationals solvable by radicals — has a polynomial time solution.

Galöis transformed the question of solvability by radicals from a problem concerning fields to a problem about groups. What we do is to change the inquiry into several problems concerning the solvability of certain primitive groups. Pályi has recently shown that the order of a primitive solvable group of degree \( n \) is bounded by \( 24^{-1/3} n^e \) for a constant \( e \approx 3.24399\ldots \) [Pa]. We attempt to construct the Galois group of specified polynomials in polynomial time. Each polynomial is constructed so that its Galois group acts primitively on its roots. If we succeed, we use an algorithm of Sims to determine if the groups in question are solvable. If any one of them is not, the Galois group of \( f(z) \) over \( Q \) is not solvable, and hence \( f(z) \) is not solvable by radicals. It may happen that we are unable to compute the groups within the time bound. Then we know that the group in question is not solvable, since it is primitive by construction, and primitive solvable groups are polynomially bounded in size.

We first observe that there is a polynomial time algorithm for factoring polynomials over algebraic number fields by using norms, a method due to Kronecker. We construct a tower of fields between \( Q \) and \( Q[z]/f(z) \), by determining elements \( \rho_i \), \( i = 0, \ldots, r + 1 \), such that \( Q = Q(\rho_0) \subseteq Q(\rho_1) \subseteq \ldots \)
\( Q(\rho_i) \subseteq Q(\rho_{i+1}) = Q[z]/f(z) \). The tower of fields we find is
rather special. If \( g_{r+1}(y) \) is the minimal polynomial for \( \alpha_{r+1} \) over \( Q(\alpha_i) \), then the Galois group of \( g_{r+1}(y) \) over \( Q(\alpha_i) \) acts primitively on the roots of \( g_{r+1}(y) \). The Galois group of \( f(x) \) over \( Q \) is solvable iff the Galois group of \( g_{r+1}(y) \) over \( Q(\alpha_i) \) is solvable for \( i = 0, \ldots, r \).

Using a simple bootstrapping technique, it is possible to construct the Galois group of \( g_{r+1}(y) \) over \( Q(\alpha_i) \) in time polynomial in the size of the group and the length of description of \( g_{r+1}(y) \). Since the \( \alpha_i \) are determined so that the Galois group of \( g_{r+1}(y) \) over \( Q(\alpha_i) \) acts primitively on the roots of \( g_{r+1}(y) \), if the group is solvable, it will be of small order. In that case, we can compute a group table and verify solvability in polynomial time. If it is not solvable, but it is of small order, we will discover that instead. Otherwise we will learn that the Galois group of \( g_{r+1}(y) \) over \( Q(\alpha_i) \) is too large to be solvable, and thus that \( f(x) \) is not solvable by radicals over \( Q \).

Our approach combines complexity and classical algebra. We introduce background algebraic number theory in Section 1. Section 2 begins the discussion of solvability. The algorithmic paradigm of divide-and-conquer finds a classical analogue in the group theoretic notion of primitivity. Galois established the connection between fields and groups; permutation group theory explains the connection between groups and blocks. Combining these ideas we present an algorithm to compute a polynomial whose roots form a minimal block of imprimitivity containing a root of \( f(x) \).

We use this procedure in section 3 to succinctly describe a tower of fields between \( Q \) and \( Q[x]/f(x) \). A simple divide-and-conquer observation allows us to convert the question of solvability of the Galois group into several questions of solvability of smaller groups. These are easy to answer, giving us a polynomial time algorithm for the question of solvability by radicals.

We discuss in section 4 a method for expressing the roots of a solvable polynomial in terms of radicals. We present a polynomial time solution to this problem using a suitable encoding. We conclude with a discussion of open questions.

1. Background

If \( f(x) = a_n x^n + \ldots + a_0 \) is a polynomial with coefficients in \( Z \), then Lenstra, Lenstra, and Lovász showed that:

Theorem 1.1: A polynomial \( f(x) \) in \( Z[x] \) of degree \( n \) can be factored in \( O(n^{1+e} + m^{1+e} \log^2 n (\sum a_i^2)) \).

As we are concerned with expressing roots as radicals, it is natural to ask if the above can be extended to finite extensions of the rationals. We recall some definitions. An element \( \alpha \) is algebraic over a field \( K \) iff \( \alpha \) satisfies a polynomial with coefficients in \( K \). An extension field \( L \) is algebraic over a field \( K \) iff every element in \( L \) is algebraic over \( K \). It is well known that every finite extension of a field is algebraic; the finite extensions of \( Q \) are called the algebraic number fields.

Every algebraic number field is expressible as \( Q(\alpha) \) for a suitable \( \alpha \). \( Q(\alpha) \) is isomorphic to \( Q[\beta]/g(t) \), where \( g(t) \) is the minimal (irreducible) polynomial for \( \alpha \). Let the degree of \( g(t) \) be \( m \). The conjugates of \( \alpha \) are the remaining roots of \( g(t); \alpha_1, \ldots, \alpha_m \). \( \alpha \) can be thought of as \( \alpha_1 \). By the minimality of \( g(t) \), these are all distinct. (Note that the fields \( Q(\alpha_i) \) are all isomorphic.) Every element \( \beta \) in \( Q(\alpha) \) can be uniquely expressed as \( \beta = a_0 + a_1 \alpha + \ldots + a_{m-1} \alpha^{m-1} \), with the \( a_i \)'s \( \in \) \( Q \), that is, \( Q(\alpha) \) is a vector space of dimension \( m \) over \( Q \). This provides a third way to describe an algebraic number field.

A number \( \alpha \) is an algebraic integer iff it is a root of a monic polynomial over \( Z \). The set of algebraic integers of \( K = Q(\alpha) \) form a ring, frequently written \( O_K \). If we factor \( f(x) \), a polynomial in a number ring, the factors of \( f(x) \) also lie in the number ring. The ring of algebraic integers of \( Q(\alpha) \) is contained in \( (1/d)Z[\alpha] \), where

\[
d \mid \text{disc}(g(t)) = \prod_{i < j} (a_i - a_j)^2.
\]

We consider the question of length in greater detail. If \( g(t) = t^n + a_{m-1} t^{m-1} + \ldots + a_0 \), \( a_i \in Z \), then we define the size of \( g(t) \), \( \| g(t) \| = 1 + \max_i |a_i| \). If \( f(x) = \beta_n x^n + \ldots + \beta_0 \), \( \beta_i = \sum_{j=0}^{m-1} b_j \alpha^j \), then the size of \( f(x) \), \( \| f(x) \| = (1 + \max_i |b_j|)(1 + \max_i |a_i|)^m \). Note that the size of \( f(x) \) in \( Q[x] \) includes the size of \( \alpha \) as a factor. Following Weinberger and Rothschild, we define the size of \( \beta, \| \beta \| \), to be the maximum of the absolute values of the conjugates of \( \beta \).

A classical technique to reduce questions in number fields to questions in the rationals is the norm. If the conjugates of \( \alpha \) over \( K \) are \( (\alpha =) a_1, \ldots, a_m \), then if \( \beta = a_0 + a_1 \alpha + \ldots + a_{m-1} \alpha^{m-1} \alpha_0(\alpha) \) is an element of \( K(\alpha) \), the Norm \( \text{Norm}_{K(\alpha)/K}(\beta) = N_\alpha(\beta) = \prod_i (a_0 + a_1 a_i + \ldots + a_{m-1} a_i^{m-1}) \). By extending...
the definition of norms to polynomials over algebraic number fields we have:

**Theorem 1.2**: Let \( g(t) \) be a monic irreducible polynomial of degree \( m \) over \( Z \), with discriminant \( d \), and let \( f(x) \) be in \( Z(\alpha)[x] \) of degree \( n \). Then \( f(x) \) can be factored into irreducible polynomials over \( (1/d)Z(\alpha)[x] \) in 
\[O(m^{1+\epsilon} + m^{2+\epsilon} \log^2 m \log^3 (\|f(x)\|_p) |g(t)|)\]
steps.

Let \( K \) be an algebraic number field, and let \( f(x) \) be a polynomial with coefficients in \( K \), with roots \( \alpha_1, \ldots, \alpha_m \). Then \( K(\alpha_i) \simeq K[x]/f(x) \simeq K(\alpha_j) \), but in general, \( K(\alpha_i) \neq K(\alpha_j) \) for \( i \neq j \). The field \( K(\alpha_1, \ldots, \alpha_m) \) is called the splitting field of \( f(x) \) over \( K \). We consider the set of automorphisms of \( K(\alpha_1, \ldots, \alpha_m) \) which leave \( K \) fixed. These form a group, called the Galois group of \( K(\alpha_1, \ldots, \alpha_m) \) over \( K \). As we can think of these automorphisms as permutations on the \( \alpha_i \), this group is sometimes referred to as the Galois group of \( f(x) \) over \( K \). The Galois group is transitive on \( \{ \alpha_1, \ldots, \alpha_m \} \), that is, for each pair \( \alpha_i \) and \( \alpha_j \) there is an element \( \sigma \) in \( G \), with \( \sigma(\alpha_i) = \alpha_j \). Galois’ deep insight was to discover the relationship between the subgroups of the Galois group \( G \), and the subfields of \( K(\alpha_1, \ldots, \alpha_m) \).

Let \( H \) be a subgroup of \( G \). We denote by \( K(\alpha_1, \ldots, \alpha_m)^H \) the set of elements of \( K(\alpha_1, \ldots, \alpha_m) \) which are fixed by \( H \). This set forms a field. Furthermore \( H \) fixes \( K \) so that we have
\[ K \subseteq K(\alpha_1, \ldots, \alpha_m)^H \subseteq K(\alpha_1, \ldots, \alpha_m) \]

Conversely suppose that \( K(\gamma) \) is a field such that \( K \subset K(\gamma) \subset K(\alpha_1, \ldots, \alpha_m) \). Then \( \gamma \) can be written as a polynomial in \( \alpha_1, \ldots, \alpha_m \), and \( H \), the subgroup of \( G \) which fixes \( K(\gamma) \), consists of those elements of \( G \) which fix \( \gamma \). The relationship between the fields and the groups can be more formally stated as:

**Fundamental Theorem of Galois Theory**: Let \( K \) be a field, and let \( f(x) \) with roots \( \alpha_1, \ldots, \alpha_m \), be irreducible over \( K[x] \). Then:

1. Every intermediate field \( K(\beta) \), \( K \subset K(\beta) \subset K(\alpha_1, \ldots, \alpha_m) \) defines a subgroup \( H \) of the Galois group \( G \), namely the set of automorphisms of \( K \) which leave \( K(\beta) \) fixed.

2. \( K(\beta) \) is uniquely determined by \( H \), for \( K(\beta) \) is the set of elements of \( K(\alpha_1, \ldots, \alpha_m) \) which are invariant under the action of \( H \).

---

(3) \( H \) is normal iff \( K(\alpha_1, \ldots, \alpha_m) \) over \( K(\beta) \) is a Galois extension, that is, if the minimal polynomial for \( \beta \) over \( K \) splits into linear factors over \( K(\alpha_1, \ldots, \alpha_m) \). In that case, the Galois group of \( K(\beta) \) over \( K \) is \( G/H \).

| \(| G | = [K(\alpha_1, \ldots, \alpha_m) : K] \), and \(| H | = [K(\alpha_1, \ldots, \alpha_m) : K(\beta)] \) |

Once the Galois group is known, the Fundamental Theorem allows us to determine all intermediate fields:

**Theorem A**: Let the hypothesis be as in the Fundamental Theorem, and let
\[ K \subseteq L_1, L_2 \subseteq K(\alpha_1, \ldots, \alpha_m) \]
with \( G \) the group which fixes \( L_1, G_2 \), the group which fixes \( L_2 \). Then \( G_1 \subset G_2 \iff L_2 \subset L_1 \).

**Theorem B**: Let the hypothesis be as in the Fundamental Theorem. Then:

1. Let \( L_1 \) and \( L_2 \) be two subfields of \( K(\alpha_1, \ldots, \alpha_m) \) which contain \( K \). Suppose \( H_1 \) and \( H_2 \) are the subgroups of \( G \) which correspond to \( L_1 \) and \( L_2 \) respectively. Then \( H_1 \cap H_2 \) is the subgroup of \( G \) corresponding to \( L_1 \cup L_2 \).

2. The field corresponding to \( H_1 \cap H_2 \) is \( L_1 \cap L_2 \).

We want to know the answer to the following question:

What irreducible equations have the property that their roots can be expressed in terms of the elements of the base field \( K \) by means of rational operations and taking radicals. Let us be more precise. In general \( \sqrt[n]{a} \) is a many valued function, as in, for example \( \sqrt{1} \). We will require that all solutions to the equation in question be represented by expressions of the form:

\[ \sqrt[n]{p} + \sqrt[n]{q} + \cdots \]

(4)

(or similar ones), and that these expressions are to represent solutions of the equation for any choice of the radicals appearing. (If a radical appears more than once, it is assigned the same value each time.)

Since roots of unity can always be expressed in terms of radicals, consider determining expressibility of a root in radicals over \( Q(\zeta_m) \), where \( \zeta_m \) is a primitive \( m \)th root of unity.

This simplifies the situation. (We will discuss the question of expressing roots of unity in terms of radicals in Section 4.) Suppose a root \( \zeta \) is expressible in radicals, and the expression is an \( m \)th root. If \( m \) is not prime, \( m = m_1 m_2 \). Then taking an
and we call \( G \) regular if \( G \) is transitive and \( G_\alpha = 1 \) for all \( \alpha \).

A fundamental way the action of a permutation group on a set breaks up is into blocks: a subset \( B \) is a block iff for every \( \sigma \) in \( G \), \( \sigma(B) \cap B = B \) or \( \emptyset \). It is not hard to see that if \( B \) is a block, \( eB \) is also. Every group has trivial blocks: \( \{ e \} \) or \( \Omega \). The nontrivial blocks are called blocks of imprimitivity, and a group with only trivial blocks is called a primitive group.

The set of all blocks conjugate to \( B : B, a_1B, \ldots, a_kB \), form a complete block system. The idea is to construct minimal blocks of imprimitivity, and to consider actions on the blocks. We first present several well-known theorems about permutation groups.

**Theorem 2.1:** Let \( \alpha \in \Omega \), \( |\Omega| \neq 1 \). Then the transitive group \( G \) on \( \Omega \) is primitive iff \( G_\alpha \) is maximal.

**Proposition 2.2:** The lattice of groups between \( G_\alpha \) and \( G \) is isomorphic to the lattice of blocks containing \( \alpha \).

Let \( \alpha \) be a root of \( f(x) \). If \( f(x) \) is a normal polynomial, i.e., \( f(x) \) factors completely in \( Q(\alpha)[x] \), the Galois group can be computed easily. Suppose \( f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_m) \) in \( Q(\alpha)[x] \), then the \( \alpha_i \)'s will be expressed as polynomials in \( \alpha, \alpha_i = r_i(\alpha) \). Since the Galois group is a permutation group of order \( n \) on \( n \) elements, for each \( \alpha_i \) there is a unique \( \sigma_i \) in \( G \) with \( \sigma_i(\alpha) = \alpha_i = r_i(\alpha) \). Then \( \sigma_i(\alpha) = r_i(\alpha) \) implies that \( \sigma_i(r_j(\alpha)) = r_j(\sigma_i(\alpha)) = p_j(\sigma_i(\alpha)) \), and the action of \( \sigma \) on \( \Omega \) is easily determined. We can construct a group table for \( G \) and identify a set of minimal blocks in polynomial time.

Of course, it is rare that \( f(x) \) is normal. But the general case is not much more difficult. Theorem 2.1 gives a characterisation of primitive groups. We offer as an alternate characterization one that will allow us to compute blocks of imprimitivity.

**Theorem 2.3:** Let \( \alpha \) be an element of \( \Omega \), \( |\Omega| \neq 1 \). Then the transitive group \( G \) on \( \Omega \) is primitive iff \( \forall \alpha \neq \beta, \ G_\alpha G_\beta = G \), or \( G \) is regular of prime order.

**Proposition 2.4:** Suppose \( G \) acts transitively on \( \Omega \), and \( G_\alpha \) has no fixed points except \( \alpha \). Let \( A \) be a minimal nontrivial block containing \( \alpha \). Then for all \( \gamma \) in \( A \), \( \gamma \neq \alpha \), \( A = \{ \sigma(\alpha) \mid \sigma \in G_\alpha G_\gamma \} \).

**Proposition 2.4** provides the backbone of our algorithm. The orbit structure of \( G_\alpha \) can be determined from a factorisation of \( f(x) \) in \( Q(\alpha)[x] \), since the roots of the irreducible factors.
of \( f(z) \) form the orbits of \( G_\alpha \). We can likewise deduce the orbit structure of \( G_\beta \) from a factorization of \( f(z) \) in \( \mathbb{Q}(\beta)[z] \). By considering a factorization of \( f(z) \) in \( \mathbb{Q}(\alpha, \beta)[z] \) it is possible to tie together the orbit structures of \( G_\alpha \) and \( G_\beta \) in such a way as to determine if \( G_\alpha G_\beta = G \). Since \( G \) is transitive, \( \alpha \) may be fixed, and only \( \beta \) need vary.

Let \( f(z) \) be an irreducible polynomial over \( \mathbb{Q} \), with roots \( \alpha_1, \ldots, \alpha_s \). Suppose

\[
f(z) = (z - \alpha_1)g_1(z) \ldots g_r(z) \text{ in } \mathbb{Q}(\alpha_1)[z],
\]

and

\[
f(z) = (z - \alpha_s)h_1(z) \ldots h_r(z) \text{ in } \mathbb{Q}(\alpha_s)[z],
\]

with \( g_i(z) = z - \alpha_1 \), and \( h_i(z) = z - \alpha_s \). We consider \( G \), the Galois group of \( f(z) \) over \( \mathbb{Q} \), acting on the roots of \( f(z) \). We propose to determine a minimal nontrivial block of imprimitivity containing \( \alpha \), if it exists. Observe that the factorization of \( f(z) \) over \( \mathbb{Q}(\alpha_i)[z] \) is the same as the factorization of \( f(z) \) over \( \mathbb{Q}(\alpha_i)[z] \), with \( \alpha_i \)’s substituted in for \( \alpha \)’s.

Suppose \( z - p_0(\alpha_1) \) is a linear factor of \( f(z) \) in \( \mathbb{Q}(\alpha_1)[z] \); then \( p_0(z) = z - \alpha_i \) is fixed by \( G_\alpha \). The linear factors of \( f(z) \) form a block. Suppose the block \( \Lambda \) consists of the roots \( \alpha_1, \ldots, \alpha_k \). Let us consider the induced action of \( G_\Lambda \) on \( \Lambda \). Since \( G \) is transitive on \( \alpha_1, \ldots, \alpha_s \), \( G_\Lambda \) must be transitive on \( \alpha_1, \ldots, \alpha_k \). The action of \( G_\Lambda \) on \( \Lambda \) can be determined, since for \( i = 1, \ldots, k \), \( \alpha_i = p_i(\alpha_1) \). Let \( \sigma \) be in \( G_\Lambda \) and let \( \overline{\sigma} \) be the induced action of \( \sigma \) on \( \alpha_1, \ldots, \alpha_k \). Then if \( \overline{\sigma}(\alpha_1) = \alpha_j = p_j(\alpha_1) \), we have \( \sigma(\alpha_1) = \sigma(p_1(\alpha_1)) = p_j(\sigma(p_1(\alpha_1))) \).

We determine the group table of the induced action of \( G_\Lambda \) on \( \Lambda \), and find a minimal block \( \Gamma \) of \( G_\Lambda \) which contains \( \alpha_1 \) in polynomial time.

Finally we observe that \( \Gamma \) is a block of \( G \). For suppose \( \Gamma \cap \gamma \Gamma \neq \emptyset \) for some \( \gamma \in G \). Since \( \Lambda \) is a block of \( G_\Lambda \), and \( \Gamma \subseteq \Lambda \), it must be the case that \( \gamma \Gamma \subseteq \Lambda \). But \( \Gamma \) is a block of \( G_\Lambda \), thus \( \Gamma \cap \gamma \Gamma = \Gamma \).

Next suppose \( f(z) \) has no linear factors in \( \mathbb{Q}(\alpha_1)[z] \) except \( z - \alpha_1 \). Let us consider a factorization of \( f(z) \) over \( \mathbb{Q}(\alpha_1, \alpha_s)[z] \) for \( \alpha_s \neq \alpha_1 \). This will tie together the factorizations of \( f(z) \) over \( \mathbb{Q}(\alpha_1)[z] \) and \( \mathbb{Q}(\alpha_s)[z] \). In particular, this will enable us to compute the block fixed by \( G_\alpha G_\alpha \).

Define a set of graphs \( \Gamma_s, s = 1, \ldots, r \) with vertices \( V \), and edges \( E \) by:

\[
V = \{ g_i(z), i = 1, \ldots, r \} \cup \{ h_j(z), j = 1, \ldots, r \}
\]

\[
E = \{ (g_i(z), h_j(z)) \mid \gcd(g_i(z), h_j(z)) \neq 1 \text{ over } \mathbb{Q}(\alpha_1, \alpha_s) \}
\]

Then we compute the set of vertices connected to \( g_0(z) \). Let

\[
g(z) = \prod_{g_0(z) \text{ connected to } g(z)} g(z),
\]

and let \( \Lambda = \{ \alpha_1 \mid \alpha_1 \text{ is a root of } g(z) \} \). We claim \( \Lambda = \{ \sigma(\alpha_1) \mid \sigma \in G_\alpha G_\alpha \} \). To prove this we observe the following:

**Lemma 2.5:** Let \( \alpha_i \) be a root of \( g_i(z) \) in \( \mathbb{Q}(\alpha_1)[z] \). Then the roots of \( g_i(z) \) are precisely \( G_\alpha(\alpha_i) \).

It follows immediately that \( \gcd(g_i(z), h_j(z)) \neq 1 \) iff \( G_\alpha(\alpha_i) \cap G_\alpha(\alpha_j) \neq \emptyset \), where \( \alpha_i \) is a root of \( g_i(z) \) and \( \alpha_j \) is a root of \( h_j(z) \). This implies:

**Lemma 2.6:** Let \( \alpha_i \) be a root of \( g_i(z) \), a factor of \( f(z) \) in \( \mathbb{Q}(\alpha_1)[z] \). Then

\[
\alpha_i \in \Lambda = \{ \sigma(\alpha_1) \mid \sigma \in G_\alpha G_\alpha \}
\]

iff \( g_i(z) \) is connected to \( g_0(z) \).

If we compute \( \Gamma_s \) for \( s = 1, \ldots, r \), we are cycling over all \( \alpha_s \neq \alpha_1 \) which are roots of \( f(z) \) and computing \( G_\alpha G_\alpha \). By Proposition 2.4, this will give us a minimal nontrivial block containing \( \alpha_1 \), if one exists. Algorithm 2.1, which appears in the Appendix, determines minimal blocks of imprimitivity.

**Theorem 2.7:** If \( f(z) \in \mathbb{Z}[z] \) of degree \( n \) is irreducible, Algorithm 2.1 computes \( H(z) \) a polynomial in \( \mathbb{Z}[z] \) whose roots \( \alpha_1, \ldots, \alpha_k \), are elements of a minimal block of imprimitivity containing \( \alpha \). It does so in the time required to factor \( f(z) \) over \( \mathbb{Q}[z]/f(z) \) and to calculate \( n^3 \) gcd’s of polynomials of degree less than \( \deg[f(z)] \) and with coefficient length less than \( n^3 \log \| f(z) \| \) over a field containing two roots of \( f(z) \).

The Fundamental Theorem established the correspondence between fields and groups, and we know now that the lattice of groups between \( G_\alpha \) and \( G \) is isomorphic to the lattice of blocks of \( G \) which contain \( \alpha \). In the next section we use the minimal blocks of imprimitivity to obtain a tower of fields between \( Q \) and \( Q(\alpha) \). Having this tower of fields will enable us to check solvability of the Galois group in polynomial time.

Zassenhaus [Za] suggests a method for computing Galois groups which also uses blocks of imprimitivity. His method prima facie is exponential; although using our techniques it a running time can be improved.
A generalisation of Algorithm 2.1 gives a method to compute the intersection of $Q(\alpha_1)$ and $Q(\alpha_2)$. Since $G_\alpha$ is the subgroup of $G$ belonging to the subfield $Q(\alpha_1)$, and $G_{\alpha_2}$ is the subgroup of $G$ corresponding to $Q(\alpha_2)$, the subgroup of $G$ belonging to $Q(\alpha_1) \cap Q(\alpha_2)$ [Theorem B]. We can compute $Q(\alpha) \cap Q(\beta)$ even when $\alpha$ and $\beta$ are not conjugate over $Q$. Since the minimal polynomial for $\beta$ over $Q$ may factor over $Q(\alpha)$ (in which case the problem is ambiguous), we must have a description of a field containing $\alpha$ and $\beta$. The description $Q(\{x, y \mid (f(x), h(y))\}$, where $\alpha$ satisfies the irreducible polynomial $f(x)$ over $Q$, and $\beta$ satisfies the irreducible polynomial $h(y)$ over $Q$, is sufficient.

Suppose $[Q(\alpha) : Q] = m$, and let $\alpha_1, \ldots, \alpha_m$ be the conjugates of $\alpha = \alpha_1$ over $Q$. Suppose also that $\beta$ satisfies $h(z)$, an irreducible polynomial over $Q(\alpha)$, and assume that the conjugates of $\beta$ over $Q(\alpha)$ are $\beta_1, \ldots, \beta_m$ with $\beta = \beta_1$. We know there exists a $z \leq mn$ such that whenever $H(z) = N_{\alpha_i}(h(z - \alpha))$ is squarefree, then $H(z)$ is irreducible. If $\gamma = \beta + \alpha_i$, then $Q(\gamma) = Q(\alpha, \beta)$. Furthermore, since the degree of $H(z)$ is $mn$, and

$$H(z) = \prod_{i=1}^m (z - (\beta_i + \alpha_i)),$$

the roots of $H(z)$ are precisely $\{\beta_i + \alpha_i \mid i = 1, \ldots, m\}$.

To compute the intersection of $Q(\alpha)$ with $Q(\beta)$, we factor $H(z)$ over $Q(\alpha)$ and $Q(\beta)$, and compute a connected component in the same way as we did in Algorithm 2.1. This yields the algorithm INTERSECTION, which runs in polynomial time.

3. Determining Solvability

We consider a tower of fields, $F_i$, between $Q$ and $Q(\alpha)$, where $\alpha$ is a root of $f(x)$ and has conjugates $\alpha_1, \ldots, \alpha_m$, with $\alpha = \alpha_1$. The subgroup of $G$ determined by $Q(\alpha)$ is $G_\alpha$. Each subfield between $Q$ and $Q(\alpha)$ corresponds to a subgroup of $G$ which contains $G_\alpha$. Finally, each subgroup corresponds to a block of imprimitivity containing $\alpha$. This statement can be made more precise.

Lemma 3.1: Let $K$ be a field, and let $f(x)$ with roots $\alpha_1, \ldots, \alpha_m$ be an irreducible polynomial over $K[x]$. Let $B = \{\alpha_1, \ldots, \alpha_m\}$ be a block of the roots. Then $K(\alpha_1, \ldots, \alpha_m)^{G_B} = K(\text{symmetric functions in } \{\alpha_1, \ldots, \alpha_k\})$.

This means that all the fields $F_i, Q = F_k \subset F_{k-1} \subset \cdots \subset F_1 \subset F_0 = Q(\alpha)$ can be described as $Q(\text{symmetric functions in elements of } B)$, where $B$ is a block of roots containing $\alpha$. We have already observed that if $B$ is a minimal block, and if $G_1$ is the Galois group for $f(x)$ over $Q(\text{symmetric functions in elements of } B)$, then $G_1$ acts primitively on $B$. We would like to find a set of elements $\rho_i, i = 1, \ldots, k$, such that if $g_i(y)$ is the minimal polynomial for $\rho_i$ over $Q(\alpha_{i-1})$, then the Galois group $G_i$ of $g_i(y)$ over $Q(\alpha_{i-1})$ acts primitively on the roots of $g_i(y)$. These elements $\rho_i$ will be primitive elements for $F_i$ over $Q$, i.e., $F_i = Q(\rho_i)$. We already have a description of the $F_i$ from Lemma 3.1; what we seek is a succinct description. We would like a set of $\rho_i$'s whose minimal polynomials over $Q$ have polynomial length coefficients. (Since $Q(\rho_i) \subset Q(\alpha)$ for each $i$, we know that the degree of $\rho_i(y)$ is less than $n$.) We will describe the $\rho_i$'s in terms of their minimal polynomials, $h_i(x)$, over $Q$. There is an inherent ambiguity as to which root of $h_i(x)$ we are referring, but this difficulty is resolved by linking the fields $Q(\alpha)$ and $Q(\alpha_{i+1})$ through the polynomial $g_i(y)$. Fortunately, there is a simple way to do this.

Lemma 3.2: Let $f(x) \in Q[x]$ be irreducible with roots $\alpha = \alpha_1, \ldots, \alpha_m$, and Galois group $G$. Let $Q(\alpha), Q(\gamma)$ be subfields of $Q(\alpha)$, with $Q(\gamma) \subset Q(\rho)$, and let $h_1(x)$ be an irreducible factor of $f(x)$ in $Q(\rho)[x]$. Then the roots of $h_1(x)$, $\alpha_1, \ldots, \alpha_m$, form a block $B_1$. The set of roots of $N_{Q(\rho)/Q(\alpha)}(h_1(x))$ form a block of $\alpha_1, \ldots, \alpha_m$ which contains $B_1$. Let $g(x)$ be the minimal polynomial for $\rho$ over $Q(\gamma)$. If the Galois group of $g(x)$ over $Q(\gamma)$ acts primitively on the roots of $g(x)$, the roots of $N_{Q(\rho)/Q(\alpha)}(h_1(x))$ form a minimal block containing $B_1$.

This lemma allows us to compute the blocks of $\alpha_1, \ldots, \alpha_m$ directly. As the coefficients of $B(\gamma), \beta_{k-1}, \ldots, \beta_0$ are elements of $Q(\rho)/h_1(y) = Q(\rho)$, and $Q(\beta_{k-1}, \ldots, \beta_0) = Q(\gamma)$ is a subfield of $Q(\rho)$, if $\gamma_0, \ldots, \gamma_{k-1}$ are the symmetric functions in $\alpha_1, \ldots, \alpha_{k-1}$, we can determine

$$\rho_2 = \gamma_0 + c_{1} \gamma_1 + \ldots + c_{k-1} \gamma_{k-1},$$

where $Q(\rho) = Q(\gamma_0, \ldots, \gamma_{k-1}, c_i)$, and the $c_i$'s are integers less than $\gamma_i$. We let $h_2(x)$ be the minimal polynomial for $\rho_2$ over $Q$. 

145
We have found fields $F_1 = Q(\alpha_1) = Q[\alpha]/h_1(\alpha) = Q[x,y]/h_2(x)g_1(y)$ and $F_2 = Q(\alpha_2) = Q[\alpha]/h_2(\alpha)$ such that

1) the Galois group of $f(x)$ over $Q(\alpha_1)$ acts primitively on the roots of $f(x)$,

2) the Galois group of $h_1(x)$ over $Q(\alpha_1)$ acts primitively on the roots of $h_1(x)$.

We may now repeat this process with $h_2(x)$ playing the same role as $h_1(x)$ did, and determine a minimal block of roots of $h_2(x)$. Iterating this process until $\text{BLOCKS}(h_n(x))$ returns a polynomial in $Q[x]$, determines a set of fields $F_i = Q(\alpha_i)$, $i = 1, \ldots, k$, such that if $g_i(y)$ is the minimal polynomial for $\alpha_i$ over $Q(\alpha_{i+1})$, and $G_i$ is the Galois group of $g_i(y)$ over $Q(\alpha_{i+1})$, then $G_i$ acts primitively on the roots of $g_i(y)$. Furthermore $F_0 = Q(\alpha)$, and $F_k = Q$.

It is not hard to show that the $h_n(x)$ have succinct descriptions. This is because the roots of $h_n(x)$ are sums of symmetric functions of the roots of $f(x)$. We claim:

3) $|h_n(x)| \leq |f(x)|^{2^{n-1}}$ for $i = 1, 2, \ldots, k$.

4) $|g_1(y)| \leq m!|f(x)|^m$.

but omit the proof.

Generalizing this procedure yields an algorithm for determining $h_n(x)$ and $g_i(y)$, $i = 1, \ldots, r$ which satisfy:

1) $Q[x,y,h_1(x)g_0(y)] = Q(x,f(x))$,

2) $h_1(x) \subseteq Q[\alpha]$, and $g_i(y) \subseteq Q[x,y,h_1(x)]$, for $i = 1, \ldots, r$.

3) The Galois group of $g_{i-1}(y)$ over $Q[x,y]/h_1(x)$ acts primitively on the roots of $g_{i-1}(y)$.

4) The Galois group of $h_1(x)$ over $Q$ acts primitively on the roots of $h_1(x)$.

The algorithm appears in the appendix.

Theorem 3.3: Let $f(x) \subseteq Z(x)$ of degree $m$ be irreducible. Algorithm 3.1 computes $\{h_i, g_{i-1} \mid i = 1, \ldots, r\}$ which satisfy conditions 1, 2, 3, and 4 above. Let $\text{BLOCKS}(g(x))$ be the running time for $\text{BLOCKS}$ on input $g(x)$. Then the running time for $\text{FIELDS}$ is $O(m^{2} \log m \cdot \text{BLOCKS}(g(x)))$, where $\deg g(x) \leq m$, and the coefficients of $g(x)$ are less than $m^2 \log(m^{2} \log m)$.

We can now determine all the fields between $Q$ and $Q(\alpha)$. This enables us to check solvability by a simple divide-and-conquer observation. Let $Q(\beta)$ be a field such that $Q \subseteq Q(\beta) \subseteq Q(\alpha)$. Every element in $Q(\alpha)$ can be written in radicals if every element of $Q(\beta)$ can be written in radicals over $Q(\alpha)$, and every element of $Q(\beta)$ can be written in radicals over $Q(\beta)$. The divide-and-conquer terminates when no more fields can be included in the chain between $Q(\beta)$ and $Q(\alpha)$, that is, when the Galois group of the normal closure of $Q(\beta_{i-1})$ over $Q(\beta_i)$ acts primitively on the roots of the minimal polynomial of $\beta_{i-1}$ over $Q(\beta_i)$.

![Figure 3.1: The Primitive Extensions Between Q and Q(α)](image)

We consider what this means group-theoretically. Suppose $\{\beta_i \mid i = 1, \ldots, r + 1\}$ are such that $g_i(y)$ is the minimal polynomial for $\beta_i$ over $Q(\beta_{i-1})$, then the Galois group of $g_i(y)$ over $Q(\beta_{i-1})$ acts primitively on the roots of $g_i(y)$. If the set $\gamma_i \mid i = 1, \ldots, r + 1$ is chosen so that $Q(\gamma_i)$ is the splitting field for $Q(\beta_i)$ over $Q(\beta_{i-1})$, then $Q(\beta_i)$ is the block of imprimitivity associated with $Q(\beta_i)$, and let $\{\alpha_{i-1,0}, \alpha_{i-1,1}, \ldots, \alpha_{i-1,m}\}$ be the conjugate blocks. Then, if $Q(\gamma_2), \ldots, Q(\gamma_t)$ are the fields associated with the conjugate blocks, we know that $Q(\gamma_i) \subseteq Q(\gamma_{i-1})$, for $i = 1, \ldots, r$. This means that the Galois group $H_1$ of $Q(\alpha_{1}, \ldots, \alpha_{m})$ over $Q(\gamma_1)$ fixes each of the $(Q(\gamma_i))$. Assume $L_1$ is the subgroup of the Galois group which fixes $Q(\beta_1)$. Clearly $H_1 \subseteq L_1$, furthermore, $H_1 \subseteq (\text{induced action of } L_1 \text{ on } \alpha_{1}, \ldots, \alpha_{m})^2$.

If $K_1$ is the Galois group of $Q(\alpha_1, \ldots, \alpha_m)$ over $Q(\beta_1)$, then $H_1 \subseteq K_1^2$, and $H_1$ is solvable if $K_1$ is. The question of whether a particular polynomial is solvable by radicals can be transformed into $\log m$ questions of solvability of particular primitive groups. If $G_i$ is the Galois group of $Q(\beta_{i-1})$ over $Q(\beta_i)$, then $f(x)$ is solvable by radicals iff $G_i$ is solvable for $i = 1, \ldots, r$. This is surprisingly easy to answer, for primitive solvable groups are highly structured, which limits their size.
Theorem 3.4 [Fályy]: If $G$ is a primitive solvable group which acts transitively on $n$ elements, then $|G| \leq 24^{-1/3}n^2$, for a constant $c = 3.24399$.

This result is sufficient for us to obtain a polynomial time algorithm for checking solvability by radicals. Although no algorithms which compute the Galois group in time polynomial in the size of the input are known, a straightforward bootstrapping method yields an algorithm whose running time is polynomial in the size of the group. We factor $f(x)$ in $Q(y)/f(y)$. If $f(x)$ does not factor completely we adjoin a root of $f(x)$, different from $y$, to $Q(y)/f(y)$, compute a primitive element, and factor $f(x)$ over the new field. We continue this process until a splitting field for $f(x)$ is reached. (The algorithm, GALOIS, is a generalisation of Corollary 6 [L], and we do not repeat it here.)

Theorem 3.5: Let $f(x)$, a polynomial in $O_K[x]$, be monic and irreducible of degree $m$, where $K = Q(\theta)$, $\theta$ is an algebraic integer of degree 1 over $Q$, and $O_K$ is the ring of integers of $K$. Algorithm 3.2, FIELDS, returns $g(y)$ and $\{n_i\}$, where $K(y)/g(y)$ is the splitting field for $f(x)$ over $K$, and the $\{n_i\}$ form the Galois group of $f(x)$ over $K$. It does so in $O((|G|)^{2}+(|G|\log|G|\log[f(x)])+f^2\log[G])^{2}$ steps.

Let $f(x) \in Z[x]$ be monic and irreducible, with roots $\alpha_1, \ldots, \alpha_m$. We have shown how to compute field extensions $Q(\beta_i)$, $i = 1, \ldots, m+1$, such that $Q(\beta_i) = Q(\alpha_i)$, and for $j = 1, \ldots, m$, the Galois group of $Q(\beta_j)$ over $Q(\beta_{j+1})$ acts primitively on the conjugates of $\beta_j$ over $Q(\beta_{j+1})$ [Algorithm 3.1]. We have shown that if $f(x)$ is a monic, irreducible polynomial in $O_K[x]$, where $K = Q(\theta)$ is an algebraic number field, then we can compute the Galois group of $f(x)$ over $K[x]$ in time polynomial in the size of the Galois group, $[f(x)]$ and $[\theta]$. We know that primitive solvable groups are small.

It fits together quite simply. We call FIELDS on $f(x)$ to determine a tower of fields each one of which has the Galois group acting primitively on the roots of the polynomial which generates it from the field below. For each one of these extensions, we call GALOIS with a clock. Let $g(y)$ be the polynomial described in FIELDS, and suppose the degree of $g(y)$ is $n_e$. By construction the extension $Q[y]/h_{n-1}(y)$ over $Q[x]/h_n(x)$ has Galois group which acts primitively on the roots of $h_{n-1}(y)$. By Theorem 3.4, if this group is solvable, then its order must be less than $24^{-1/3}n_e^{2.25}$. For each $i, i = 1, \ldots, r$, we call GALOIS on input $g_{i-1}(y), Q[x]/h_{i}(x)$. We allow this procedure to run while the extension is of degree less than $24^{-1/3}n_e^{2.25}$. If the procedure fails to return a Galois group in that amount of time, we know that the Galois group of $g_{i-1}(y)$ over $Q[x]/h_i(x)$ is not solvable, and hence neither is $f(x)$ solvable over $Q$. If a group is returned, we call any of the standard algorithms for testing solvability of a group [Sims, FHL]. Since the order of the group is polynomial size in $n_e$, these algorithms can check solvability of the group in polynomial time. Let SOLVABLECP be the reader's favorite algorithm for testing if a given group is solvable. We assume that the input to SOLVABLECP is a set $\{n_i\}$ which forms the Galois group for $g_{i-1}(y)$ over $Q[x]/h_i(x)$. Then SOLVABLECP returns "yes" if the group is solvable, and "no" otherwise.

Algorithm 3.2 SOLVABILITY
input: $f(x) \in Z[x]$, monic irreducible of degree $m$

Step 1: Call BLOCKS(f(x))

Step 2: For $i = 1, \ldots, r$, do:

For $(\text{degree}(g_{i-1}(y)))^{h_i}$ steps, do:

Step 3: Call GALOIS($g_{i-1}(y), Q[x]/h_{i}(x)$)

If no return, return $f(x)$ "IS NOT SOLVABLE BY RADICALS"

Else call SOLVABLECP($\{n_i\}$)

If SOLVABLECP($\{n_i\}$) = "no", return $f(x)$ "IS NOT SOLVABLE BY RADICALS"

Step 4: return $f(x)$ "IS SOLVABLE BY RADICALS"

Theorem 3.6: Let $f(x) \in Z[x]$ be monic and irreducible of degree $m$ over $Q$. Then Algorithm 3.2 determines whether the roots of $f(x)$ are expressible in radicals in time polynomial in $m$ and $\log|f(x)|$.

4. Expressibility

If $f(x)$ is an irreducible solvable polynomial over the rationals, it would be most pleasing to find an expression in radicals for the roots of $f(x)$. In this section we outline a method for obtaining a polynomial time straight line program to express the roots of $f(x)$ in radicals. We begin with the classical:
Theorem 4.1: Every cyclic field of $n^{th}$ degree over an algebraic number field can be generated by an adjunction of an $n^{th}$ root provided that the $n^{th}$ roots of unity lie in the base field.

The method we use to express $\alpha$ as radicals over $Q$ relies on the effective proof of Theorem 4.1. Clearly roots of unity play a special role in the question of expressibility; it is well-known that:

Lemma 4.2: The $p^{th}$ roots of unity, $p$ a prime, are expressible as "irreducible radicals" over $K$.

We assume $f(x)$ is an irreducible solvable polynomial of degree $m$ over the rationals, and we let $\alpha$ be a root of $f(x)$.

In §3 we presented an algorithm which found a tower of fields $Q(\beta_i), i = 1, \ldots, r$, where $Q \subseteq Q(\beta_1) \subseteq \ldots \subseteq Q(\beta_i) \subseteq Q(\alpha)$, and the Galois group of $Q(\beta_i)$ over $Q(\beta_{i-1})$ acts primitively on the roots of the minimal polynomial of $\beta_i$ over $Q(\beta_{i-1})$. We also described a polynomial time algorithm to find the fields $Q(\gamma_i), i = 1, \ldots, r$, where $Q(\gamma_i)$ is the splitting field for $Q(\beta_i)$ over $Q(\beta_{i-1})$. In light of Theorem 4.1, we first adjoin to $Q$ the $t^{th}$ roots of unity, where $t = [Q(\alpha) : Q]$. We claim that there is a straight line program which expresses $\alpha$, a primitive $p^{th}$ root of unity, in radicals in polynomial time. Since the proof is similar to that for expressing $\beta_i$ as radicals in polynomial time, we begin by showing a bound for the $\beta_i$'s. We find elements $\tilde{\beta}_i$ such that $Q(\tilde{\beta}_i) = Q(\gamma_i, \beta_i)$. To write straight line code to express $\alpha$ as radicals over $Q$, it suffices to present straight line code for expressing $\tilde{\beta}_i$ as radicals over $Q(\tilde{\beta}_{i-1})$. If we can solve the latter problem in time polynomial in $m$ and $\log |f(x)|$, the former can also be solved in polynomial time, because there are at most $\log m$ fields between $Q$ and $Q(\alpha)$. (The bounds we present are not best possible, but are simplified for the sake of readability.)

Lemma 4.3: If $\tilde{\beta}_i(x)$ is the minimal polynomial for $\tilde{\beta}_i$ over $Q$, then $|\tilde{\beta}_i(x)| \leq O(|f(x)|^{o(m^2})$. If $\tilde{\beta}_i(x)$ is the minimal polynomial for $\tilde{\beta}_i$ over $Q(\tilde{\beta}_{i-1})$, then $|\tilde{\beta}_i(x)| \leq O(|f(x)|^{o(m^3})$.

Lemma 4.4: If $\tilde{\beta}_i(x)$ is the minimal polynomial for $\gamma_i$ over $Q(\tilde{\beta}_{i-1})$, then $|\tilde{\beta}_i(x)| \leq O(|f(x)|^{o(m^2})$.

Suppose that $H$ is the Galois group for $Q(\gamma_i)$ over $Q(\beta_{i-1})$, and that $H$ is solvable. In polynomial time we can find a set of subgroups of $H$ which satisfy $H_0 \subseteq H_1 \subseteq \ldots \subseteq H_r = H$, where $H_k$ is normal in $H_{k+1}$, and $H_{k+1}/H_k$ is of prime order $[Sims]$, [PFI]. We let

$$
\tilde{j}_k(x) = \prod_{\gamma \in H_k} \sigma(x - \gamma);
$$

then $Q(\tilde{\beta}_{i-1})[x]/\tilde{j}_k(x)$ is the subfield of $Q(\gamma_i)$ corresponding to $H_k$. Since we can compute the $H_k$'s in polynomial time, we can also compute polynomials $\tilde{j}_k(x)$ in polynomial time. We can find a primitive element $\theta_k$ for the field $Q(\tilde{\beta}_{i-1})[x]/\tilde{j}_k(x)$ in polynomial time.

We conclude:

Lemma 4.5: Let $\tilde{\beta}_i(x)$ be the minimal polynomial for $\theta_k$ over $Q$. Then $\tilde{\beta}_i(x) \leq O(|f(x)|^{o(m^3)})$. If $i_k(x)$ is the minimal polynomial for $\theta_k$ over $Q(\tilde{\beta}_{i-1})$, then $|i_k(x)| \leq O(|f(x)|^{o(m^3)})$.

We have determined primitive elements $\theta_i$ such that $Q(\gamma_i)$ is a cyclic extension of $Q(\beta_{i-1})$, $Q(\beta_{i+1})$ is a cyclic extension of $Q(\beta_i)$, and $Q(\beta_i)$ is a cyclic extension of $Q(\tilde{\beta}_{i-1})$. (For the sake of simplicity, let $\theta_0 = \tilde{\beta}_{i-1}$.) Denote $[Q(\theta_i) : Q(\theta_{i-1})] = d_i$.

We inductively express $\eta_1, \ldots, \eta_{r+1}$ such that $Q(\theta_j, \eta_j) = Q(\theta_{j+1})$, and $\eta_j = \sqrt[p_j]{\sigma_j(\theta_j)}$, where $p_j(x) \in Q[x]$. Since $\eta_1$ is small in absolute value, its minimal polynomial over $Q$ has polynomial size coefficients. This polynomial factors over $Q(\theta_0)$. Since $x - \eta_1 = x - p_1(\theta)_0$ is a factor, we conclude by Weinberger and Retheschild [Theorem 1.3] that $p_1(x)$ has polynomial size coefficients.

Theorem 4.6: There exists a polynomial time straight line program to express $\alpha$, a root of a solvable irreducible polynomial over $Q$, in terms of radicals.

We have not yet shown how to express the $t^{th}$ roots of unity as radicals over $Q$, but Lemma 4.2 is effective. We observe that in order to express the $t^{th}$ roots of unity as radicals over $Q$, we need to have the $p^t$th roots of unity expressed as radicals, where $p_t$ is a prime divisor of $p(t)$. Of course, this requires that $p^t$ roots of unity are expressed as radicals, where $p_t$ is a prime divisor of $p_t - 1$. This inductive construction requires no more that $\log t$ steps. Therefore we conclude that
3) Is there a polynomial time algorithm to determine
   a) the order of the Galois group
   b) a set of generators for the Galois group,
   in the case of a solvable Galois group? 

   Actually determining the group. For example, the Galois group
   of an irreducible polynomial \( f(x) \) of degree \( n \) over
   the rationals is contained in \( A_n \), the alternating group
   of order \( n \), iff \( \text{disc}(f(x)) \) is a square in \( \mathbb{Q} \). 
   This means that the Galois group of an irreducible polynomial
   of degree 3 over \( \mathbb{Q} \) may be found by simply calculating
   the discriminant. Various tricks and
   methods have been used to determine the Galois group of polynomials
   over \( \mathbb{Q} \) of degree less than 10 [Mc,St, Za], but until
   the recent results concerning polynomial factorisation there
   was no feasible way to compute the Galois group of a general
   polynomial of large degree. It would be most exciting if a
   polynomial time algorithm were found for computing the Galois
   group. We offer no further insights on this problem, but we
   hope for, and would be delighted by, its solution.

   Appendix

   The algorithm we present computes a minimal block of
   imprimitivity. It can be easily modified to compute a tower
   of blocks at once.

   Algorithm 2.1 blocks

   Input: \( f(x) \in \mathbb{Z}[x], f(x) \) irreducible of degree \( n \) over \( \mathbb{Z} \)

   Step 1: Find \( c \neq 0 \) such that \( N(q(x)/f(x))/\mathbb{Q}(f(x - cx)) \)
   is squarefree and factor \( N(q(x)/f(x))/\mathbb{Q}(f(x - cx)) \)
   over \( \mathbb{Q} \),
   \[ N(q(x)/f(x))/\mathbb{Q}(f(x - cx)) = \prod_{i=1}^{n^3} G_i(z - cx) \]
   [At most \( n^3 \) \( c \)'s in \( \mathbb{Q} \) do not satisfy this condition.]

   Step 2: For \( i = 1 \ldots d \) do: \( g_i(x) = \text{gcd}(f(x), G_i(z)) \) over \( \mathbb{Q}[x]/f(x) \).
   [Thus \( f(x) = \prod g_i(x) \) is a complete factorization
   of \( f(x) \) over \( \mathbb{Q}[x]/f(x) \).]

   \*The second author claims to have shown that polynomial size representa-
   tion of roots of radicals is possible given symbols \( \gamma \), for roots of
   unity.
Step 3: If \( f(x) \) has more than one linear factor, compute the induced action of Galois group and Cayley table, and find maximal block by inspection. Then
\[
B^*(x) = \prod_{a_i} \text{block}(x - a_i),
\]
and return \( B^*(x) \).

[In this case, the fixed points form a block, and the induced action of the full group on the block can be determined by substitutions.]

Step 4: For each \( G_j(x - cz) \) a factor of \( N_G(\alpha_j)/f(\alpha_j)/Q(f(x)-cz) \) do steps 5-9:

Step 5: \( g_j(t) \leftarrow \text{constant term of } \gcd(g_j(x), f(t - cz)) \) over \( Q[t, x]/G_j(t) \)
\[
p_j(t) \leftarrow t - c g_j(t)
\]
[This computes \( y \) and \( z \) in terms of a primitive element for the field \( Q[y,z]/(y^2 g_j^2(\alpha_j)) \)
\[
= Q[t]/G_j(t)\]
]

Step 6: For \( i = 1 \ldots i, \) do:
\[
g_i(t) \leftarrow g_i^p(t)
\]
\[
g_i(t) \leftarrow g_i^{q_i(t)}
\]
[This rewrites the factorisations of \( f(x) \) over \( Q[x]/f(x) \) and \( Q[y]/f(y) \) as factorisations over \( Q[x]/G_j(t) \).]

Step 7: Compute the graph \( G_j = (V_j, E_j) \), with vertices, \( V_j \), and edges, \( E_j \), given by:
\[
V_j = \{ g_i^2(x) \} \cup \{ x \}
\]
\[
E_j = \{ (g_i^2(x), g_j^2(x)) \mid \gcd(g_i^2(x), g_j^2(x)) \neq 1 \}
\]

Step 8: Compute \( Y_j = \{ i \mid g_i^2(x) \text{ is connected to } g_j^2(x) = x - p_j(t) \} \)

Step 9: \( B_j(x) \leftarrow \prod_{i \in Y_j} g_j^2(x) \)

Step 10: \( B(x) \leftarrow B_j(x) \), of minimal degree

return \( B(x) \in Q[x, z]/f(x) \), a polynomial whose roots form a minimal block of imprimitivity containing \( z \).

Algorithm 3.1 FIELDS

input: \( f(x) \in Z[x] \), a monic, irreducible polynomial

Step 1: \( i \leftarrow 1 \)
\[
h_0(z) \leftarrow f(z)
\]
\[
C^*(t) \leftarrow \text{BLOCKS}(f(z))
\]
\[
g_0(t) \leftarrow t + c_0(z) z^{e_0-1} + \ldots + a_0(z) - C^*(t)
\]
[\( C^*(t) \) will be the polynomial whose norm we compute in order to determine the chain of fields.]

Step 2: While \( C^*(t) \notin Q[t], \) do steps 3-17
Else go to return

Step 3: \( t^k + a_{k-1}(z)t^{k-1} + \ldots + a_0(z) \leftarrow C^*(t) \)

Step 4: \( \beta(z) \leftarrow a_{k-1}(z) \)

Step 5: For \( j = 1 \ldots k-1, \) do:
While \( a_j(z) \notin \{ 1, \beta(z), \ldots, \beta^{m-1}(z) \} \), do:
\[
\beta(z) \leftarrow \beta(z) + a_j(z)
\]
[This computes an element \( \beta(z) \) such that \( Q[a_{k-1}(z), \ldots, a_0(z)]/f(x) \simeq Q[\beta(z)]/f(x) \).]

Step 6: \( l \leftarrow l + 1 \)

Step 7: While \( \{ 1, \beta(z), \ldots, \beta^l(z) \} \) is a linearly independent set over \( Q \), do:
\( l \leftarrow l + 1 \)

Step 8: Else if \( \beta^l(z) + d_{l-1} \beta^{l-1}(z) + \ldots + d_0 = 0, \)
\[
h_i(z) \leftarrow z^i + d_{l-1} z^{i-1} + \ldots + d_0
\]
[This determines the minimal polynomial for \( \beta(z) \) over \( Q \); we have \( Q[\beta(z)]/f(x) = Q[z]/h_i(z) \).]

Step 9: For \( j = 0 \ldots l-1, \) do:
Find \( p_j(x) \) such that \( p_j(\beta(z)) = c_j(z) \)

Step 10: \( g_{i-1}(y) \leftarrow y^i + p_{i-1}(z) y^{i-1} + \ldots + p_0(z) \)
[Then \( Q[y]/h_{i-1}(t) \approx Q[z]/h_i(z) g_{i-1}(y) \).]

Step 11: For \( j = 0 \ldots k-1, \) do:
Find \( q_j(z) \) such that \( q_j(\beta(z)) = a_j(z) \).

Step 12: \( C^*(t) \leftarrow t^k + g_{k-1}(z) t^{k-1} + \ldots + q_0(z) \)
[This expresses \( C^*(t) \), a polynomial in \( Q[\beta(z)]/f(x) \simeq Q[z]/h_i(z) \) in terms of the element \( z \).]

Step 13: \( B^*(t) \leftarrow \text{ BLOCKS}(h_i(z)); \)
\[
t^k + b_{k-1}(z) t^{k-1} + \ldots + b_0(z) \leftarrow B^*(t) \)
Step 14: For $j = 0, \ldots, t - 1$, do:
   
   $c_j(z) \leftarrow b_j(B(z))$

   [This will allow us to express $B^*(t)$ as a polynomial
   with coefficients which are polynomials in $z$ and
   which has root $z_j$.]

Step 15: $B^*(z) \leftarrow z^t + c_{t-1}(z)z^{t-1} + \ldots + c_0(z)$

Step 16: $C^*(t) \leftarrow \text{Res}_z(B^*(z), C^*(t))$

Step 17: $i \leftarrow i + 1$

return: \{ $h_i(x), g_i(y) \mid i = 1, \ldots, r$ \}

1. $Q[x, y] / h_1(x)g_1(y) \cong Q[x] / f(x)$
2. $h_i(z) \in Q[x]$, and
   
   $g_{i-1}(y) \in Q[y] / h_i(x)$, for $i = 1, \ldots, r$
3. The Galois group of $g_{i-1}(y)$ over $Q[x, y] / h_i(x)$
   acts primitively on the roots of $g_{i-1}(y)$
4. The Galois group of $h_i(x)$ over $Q$ acts primitively
   on the roots of $h_i(x)$.

Acknowledgements: Warm thanks to Eric Landers who
originally suggested the approach of primitive groups. Thanks
also to Mike Artin and Rich Zippel.