Solvability by Radicals is in Polynomial Time

(Preliminary Report)

Susan Landau*

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 millenia 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 breakthrough of Lenstra, Lenstra, and Lovász [L^3], 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, $f(x)$, over the rationals solvable by radicals* – has a polynomial time solution.

Galois 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. Pálfy has recently shown that the order of a primitive solvable group of degree n is bounded by $24^{-1/3}n^c$ for a constant $c = 3.24399\ldots$ [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 $f(x)$ over Q is not solvable, and hence $f(x)$ 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 $Q[x]/f(x)$, by determining elements ρ_i, $i = 0, \ldots, r+1$, such that $Q = Q(\rho_0) \subseteq Q(\rho_1) \subseteq \ldots Q(\rho_r) \subseteq Q(\rho_{r+1}) = Q[x]/f(x)$. The tower of fields we find is

*This work partially supported by NSF grant MCS 800756-A01 and ONR grant NOO14-80-C-622

rather special. If $g_{i+1}(y)$ is the minimal polynomial for ρ_{i+1} over $Q(\rho_i)$, then the Galois group of $g_{i+1}(y)$ over $Q(\rho_i)$ acts primitively on the roots of $g_{i+1}(y)$. The Galois group of $f(x)$ over Q is solvable iff the Galois group of $g_{i+1}(y)$ over $Q(\rho_i)$ is solvable for $i = 0, \ldots, r$.

Using a simple bootstrapping technique, it is possible to construct the Galois group of $g_{i+1}(y)$ over $Q(\rho_i)$ in time polynomial in the size of the group and the length of description of $g_{i+1}(y)$. Since the ρ_i are determined so that the Galois group of $g_{i+1}(y)$ over $Q(\rho_i)$ acts primitively on the roots of $g_{i+1}(y)$, 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 $g_{i+1}(y)$ over $Q(\rho_i)$ 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 $O(n^{9+\epsilon} + m^{7+\epsilon} \log^{2+\epsilon}(\sum a_i^2))$.

As we are concerned with expressing roots as radicals, it is natural to ask is if the above can be extended to finite extensions of the rationals. We recall some definitions. An element α is *algebraic over a field* K iff α 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 α. $Q(\alpha)$ is isomorphic to $Q[t]/g(t)$, where $g(t)$ is the minimal (irreducible) polynomial for α. Let the degree of $g(t)$ be m. The conjugates of α are the remaining roots of $g(t)$: $\alpha_2 \ldots \alpha_m$, α can be thought of as α_1. By the minimality of $g(t)$, these are all distinct. (Note that the fields $Q(\alpha_i)$ are all isomorphic.) Every element β 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 α 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

$$d \mid \text{disc}(g(t)) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

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

A classical technique to reduce questions in number fields to questions in the rationals is the *norm* . If the conjugates of α over K are $(\alpha =)\alpha_1, \ldots, \alpha_m$, then if $\beta = a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}$ is an element of $K(\alpha)$, the $Norm_{K(\alpha)/K}(\beta) = N_\alpha(\beta) = \prod_i (a_0 + a_1\alpha_i + \ldots + a_{m-1}\alpha_i^{m-1})$. 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 $Z(\alpha)[x]$ be of degree n. Then $f(x)$ can be factored into irreducible polynomials over $(1/d)Z(\alpha)[x]$ in $O(m^{9+\epsilon}n^{9+\epsilon}\log^{2+\epsilon}(m^2n^2\|f(x)\||g(t)|))$ 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 α_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 α_i and α_j there is an element σ 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 γ 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 γ. 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, iff the minimal polynomial for β 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.

(4) $|G| = [K(\alpha_1, \ldots, \alpha_m) : K]$, 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

$$K \subset L_1, L_2 \subset K(\alpha_1, \ldots, \alpha_m)$$

with G_1 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_1L_2.

(2) The field corresponding to H_1H_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 $\sqrt[m]{a}$ is a many valued function, as in, for example $\sqrt[4]{1}$. We will require that all solutions to the equation in question be represented by expressions of the form:

$$\sqrt[a]{\sqrt[b]{p\ldots} + \sqrt[c]{\ldots}} \qquad (*)$$

(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 ζ_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 α is expressible in radicals, and the expression is an m^{th} root. If m is not prime, $m = m_1m_2$. Then taking an

m^{th} root could be broken into two steps, first taking an m_1^{th} root, then an m_2^{nd} root, By further decomposition, one need only take roots of prime degree. This would give rise to a series of field extensions, $Q(\varsigma_m) = F_k \subset F_{k-1} \subset ... \subset F_0$, where F_{i-1} is an extension of F_i which arises by taking a p_i^{th} root of an element in F_{i-1}. Each F_{i-1} is a Galois extension of F_i. The accompanying lattice of groups, $G_0 \subset G_1 \subset ... \subset G_k = G$, where G_i is the subgroup of G which fixes F_{k-i} satisfies the following two important conditions: G_{i-1} is *normal* in G_i, and G_i/G_{i-1} is of prime order. A group which satisfies these two conditions is called *solvable*. Galois showed that $f(x)$ is solvable in radicals iff the Galois group of $f(x)$ over Q is solvable.

Fundamental Theorem on Equations Solvable by Radicals:

(1) If one root of an irreducible equation $f(x)$ over K can be represented by an expression of the form (*), then the Galois group of $f(x)$ over K is solvable.

(2) Conversely, if the Galois group of $f(x)$ over K is solvable, then all roots can be represented by expressions (*) in such a way that the successive extensions F_{i-1} over F_i are extensions of prime degree, with $F_{i-1} = F_i(\sqrt[p]{a_i})$, with $a_i \in F_i$, and $x^p - a_i$ irreducible over F_i.

The problem of checking solvability by radicals can be converted to a problem of determining if a group is solvable. Yet on first glance, it is not obvious that this reduction is useful. How does one check solvability of a group? Various algorithms exist [Sims], [FHL] which do so in polynomial time given generators of the group. We do not use this approach since there is at present no polynomial time algorithm for determining the generators of the Galois group. Instead, solvability provides a natural way to use divide-and-conquer. If H is a normal subgroup of G, then G is solvable iff H and G/H are. Finding the right set of H's is the key to solving this problem, and is the subject of the next section.

2. Finding Blocks of Imprimitivity

The Galois group, G, is a transitive permutation group on the set of roots,

$$\{\alpha_1, \ldots, \alpha_m\} = \Omega$$

We define:

$$G_\alpha = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$$

and we call G *regular* if G is transitive and $G_\alpha = 1$ for all α. 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 σ in G, $\sigma(B) \cap B = B$ or $\emptyset$. It is not hard to see that if B is a block, σB is also. Every group has trivial blocks: $\{\alpha\}$ or Ω. 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: $B, \sigma_2 B \ldots \sigma_k B$, 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 Ω is primitive iff G_α is maximal.

Proposition 2.2: The lattice of groups between G_α and G is isomorphic to the lattice of blocks containing α.

Let α 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 $f(x) = (x-\alpha)(x-\alpha_2)\ldots(x-\alpha_m)$ in $Q(\alpha)[x]$, then the α_i's will be expressed as polynomials in α, $\alpha_i = p_i(\alpha)$. Since the Galois group is a permutation group of order n on n elements, for each α_i there is a unique σ_i in G with $\sigma_i(\alpha) = \alpha_i = p(\alpha)$. Then $\sigma_i(\alpha) = p_i(\alpha)$ implies that $\sigma_i(\alpha_j) = \sigma_i(p_j(\alpha)) = p_j(\sigma_i(\alpha)) = p_j(p_i(\alpha))$, and the action of σ_i on Ω 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 characterization of primitive groups. We offer as an alternate characterization one that will allow us to compute blocks of imprimitivity.

Theorem 2.3: Let α be an element of Ω, $|\Omega| \neq 1$. Then the transitive group G on Ω 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 Ω, and G_α has no fixed points except α. Let Λ be a minimal nontrivial block containing α. Then for all γ in Λ, $\gamma \neq \alpha$, $\Lambda = \{\sigma(\alpha) \mid \sigma \in G_\alpha G_\gamma\}$.

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

Let $f(x)$ be an irreducible polynomial over Q, with roots $\alpha_1,\ldots,\alpha_n$. Suppose

$$f(x) = (x-\alpha_1)g_2(x)\ldots g_r(x) \text{ in } Q(\alpha_1)[x], \text{ and}$$
$$f(x) = (x-\alpha_s)h_2(x)\ldots h_r(x) \text{ in } Q(\alpha_s)[x],$$

with $g_1(x) = x-\alpha_1$, and $h_1(x) = x-\alpha_s$. We consider G, the Galois group of $f(x)$ over Q, acting on the roots of $f(x)$. We propose to determine a minimal nontrivial block of imprimitivity containing α, if it exists. Observe that the factorization of $f(x)$ over $Q(\alpha_s)[x]$ is the same as the factorization of $f(x)$ over $Q(\alpha_1)[x]$, with α_s's substituted in for α_1's.

Suppose $(x-p_i(\alpha_1))$ is a linear factor of $f(x)$ in $Q(\alpha_1)[x]$; then $p_i(x) = (x-\alpha_i)$ is fixed by G_{α_1}. The linear factors of $f(x)$ form a block. Suppose the block Λ consists of the roots $\alpha_1,\ldots,\alpha_k$. Let us consider the induced action of G_Λ on Λ. Since G is transitive on $\alpha_1,\ldots,\alpha_n$, G_Λ must be transitive on $\alpha_1,\ldots,\alpha_k$. The action of G_Λ on Λ can be determined, since for $i=1,\ldots,k$, $\alpha_i = p_i(\alpha_1)$. Let σ be in G_Λ and let $\bar\sigma$ be the induced action of σ on $\alpha_1,\ldots,\alpha_k$. Then if $\bar\sigma(\alpha_1) = \alpha_j = p_j(\alpha_1)$, we have $\bar\sigma(\alpha_l) = \bar\sigma(p_l(\alpha_1)) = p_j(p_l(\alpha_1))$. We determine the group table of the induced action of G_Λ on Λ, and find a minimal block Γ of G_Λ which contains α_1 in polynomial time [At.]

Finally we observe that Γ is a block of G. For suppose $\Gamma\cap\tau\Gamma \neq \phi$ for some $\tau\in G$. Since Λ is a block of G, and $\Gamma\subset\Lambda$, it must be the case that $\tau\Gamma\subset\Lambda$. But Γ is a block of G_Λ, thus $\Gamma\cap\tau\Gamma = \Gamma$.

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

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

$V = \{\, g_i(x), i=1,\ldots,r\,\} \cup \{\, h_i(x), 1 = 1,\ldots,r\,\}$
$E = \{\, \langle g_i(x), h_j(x)\rangle \mid \gcd(g_i(x),h_j(x)) \neq 1 \text{ over } Q(\alpha_1,\alpha_s)\,\}$

Then we compute the set of vertices connected to $g_0(x)$. Let

$$g(x) = \prod_{\substack{g_i(x)\text{ is}\\ \text{connected to } g_0(x)}} g_i(x) \quad ,$$

and let $\Lambda_s = \{\,\alpha_i \mid \alpha_i \text{ is a root of } g(x)\,\}$. We claim $\Lambda_s = \{\,\sigma(\alpha_1) \mid \sigma\in G_{\alpha_1}G_{\alpha_s}\,\}$. To prove this we observe the following:

Lemma 2.5: Let α_i be a root of $g_i(x)$ in $Q(\alpha_1)[x]$. Then the roots of $g_i(x)$ are precisely $G_{\alpha_1}(\alpha_i)$.

It follows immediately that $\gcd(g_i(x),h_j(x)) \neq 1$ iff $G_{\alpha_1}(\alpha_i)\cap G_{\alpha_s}(\alpha_j) \neq \emptyset$, where α_i is a root of $g_i(x)$ and α_j is a root of $h_j(x)$. This implies:

Lemma 2.6: Let α_j be a root of $g_j(x)$, a factor of $f(x)$ in $Q(\alpha_1)[x]$. Then

$$\alpha_j \in \Lambda_s = \{\,\sigma(\alpha_1) \mid \sigma\in G_{\alpha_1}G_{\alpha_s}\,\}$$

iff $\quad g_j(x)$ is connected to $g_0(x)$.

If we compute Γ_s for $s=1,\ldots,r$, we are cycling over all $\alpha_i \neq \alpha_1$ which are roots of $f(x)$ and computing $G_{\alpha_1}G_{\alpha_s}$. By Proposition 2.4, this will give us a minimal nontrivial block containing α_1, if one exists. Algorithm 2.1, which appears in the Appendix, determines minimal blocks of imprimitivity.

Theorem 2.7: If $f(x)\in Z[x]$ of degree n is irreducible, Algorithm 2.1 computes $B(x)$ a polynomial in $Z(\alpha)[x]$ whose roots $\alpha_1\ldots\alpha_k$, are elements of a minimal block of imprimitivity containing α. It does so in the time required to factor $f(x)$ over $Q[z]/f(z)$ and to calculate n^3 gcd's of polynomials of degree less than $\deg(f(x))$ and with coefficient length less than $n^2\log[\![f(x)]\!]$ 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_α and G is isomorphic to the lattice of blocks of G which contain α. 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 s running time can be improved.

A generalization of Algorithm 2.1 gives a method to compute the intersection of $Q(\alpha_1)$ and $Q(\alpha_s)$. Since G_{α_1} is the subgroup of G belonging to the subfield $Q(\alpha_1)$, and G_{α_s} is the subgroup of G belonging to $Q(\alpha_s)$, $G_{\alpha_1}G_{\alpha_s}$ is the subgroup of G belonging to $Q(\alpha_1) \cap Q(\alpha_s)$ [Theorem B.] We can compute $Q(\alpha) \cap Q(\beta)$ even when α and β are not conjugate over Q. Since the minimal polynomial for β over Q may factor over $Q(\alpha)$ (in which case the problem is ambiguous), we must have a description of a field containing α and β. The description $Q[x,y]/(f(x),h(y))$, where α satisfies the irreducible polynomial $f(x)$ over Q, and β satisfies the irreducible polynomial $h(y)$ over $Q[x]/f(x)$ suffices.

Suppose $[Q(\alpha):Q] = m$, and let $\alpha_2, \ldots, \alpha_m$ be the conjugates of $\alpha = \alpha_1$ over Q. Suppose also that β satisfies $h(x)$, an irreducible polynomial over $Q(\alpha)$, and assume that the conjugates of β over $Q(\alpha)$ are $\beta_1, \ldots, \beta_n$, with $\beta = \beta_1$. We know there exists a c less than mn such that whenever $H(x) = N_\alpha(h(x - c\alpha))$ is squarefree, then $H(x)$ is irreducible. If $\gamma = \beta + c\alpha$, then $Q(\gamma) = Q(\alpha, \beta)$. Furthermore, since the degree of $H(x)$ is mn, and

$$H(x) = \prod_i \prod_j (x - (\beta_j + c\alpha_i)),$$

the roots of $H(x)$ are precisely $\{ \beta_j + c\alpha_i \mid j = 1, \ldots, n; \quad i = 1, \ldots, m \}$.

To compute the intersection of $Q(\alpha)$ with $Q(\beta)$, we factor $H(x)$ 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 α is a root of $f(x)$ and has conjugates $\alpha_2, \ldots, \alpha_m$, with $\alpha = \alpha_1$. The subgroup of G determined by $Q(\alpha)$ is G_α. Each subfield between Q and $Q(\alpha)$ corresponds to a subgroup of G which contains G_α. Finally, each subgroup corresponds to a block of imprimitivity containing α. 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 $B = \{\alpha_1, \ldots, \alpha_k\}$ 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, $Q = F_k \subseteq F_{k-1} \subseteq \ldots \subseteq F_1 \subseteq F_0 = Q(\alpha)$ can be described as Q(symmetric functions in elements of B), where B is a block of roots containing α. We have already observed that if B is a minimal block, and if G_1 is the Galois group for $f(x)$ over Q(symmetric functions in elements of B), then G_1 acts primitively on B. We would like to find a set of elements ρ_i, $i = 1, \ldots, k$, such that if $g_i(y)$ is the minimal polynomial for ρ_i over $Q(\rho_{i+1})$, then the Galois group G_i of $g_i(y)$ over $Q(\rho_{i+1})$ acts primitively on the roots of $g_i(y)$. These elements ρ_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 ρ_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 $g_i(y)$ is less than n.) We will describe the ρ_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 $Q(\rho_i)$ and $Q(\rho_{i+1})$ 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 $Q(\rho), Q(\tau)$ be subfields of $Q(\alpha)$, with $Q(\tau) \subset Q(\rho)$, and let $h_1(x)$ be an irreducible factor of $f(x)$ in $Q(\rho)[x]$. Then the roots of $h_1(x)$, $\alpha_1, \ldots, \alpha_{k_1}$, form a block B_1. The set of roots of $N_{Q(\rho)/Q(\tau)}(h_1(x))$ form a block of $\alpha_1, \ldots, \alpha_m$ which contains B_1. Let $g(x)$ be the minimal polynomial for ρ over $Q(\tau)$. If the Galois group of $g(x)$ over $Q(\tau)$ acts primitively on the roots of $g(x)$, the roots of $N_{Q(\rho)/Q(\tau)}(h_1(x))$ 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 $B(x)$, $\beta_{k_2-1}, \ldots, \beta_0$ are elements of $Q[y]/h_1(y) = Q(\rho)$, and $Q(\beta_{k_2-1}, \ldots, \beta_0) = Q(\tau)$ is a subfield of $Q(\rho)$, if $\gamma_0, \ldots, \gamma_{jk-1}$ are the symmetric functions in $\alpha_1, \ldots, \alpha_{k_1k_2}$, we can determine

$$\rho_2 = \gamma_0 + c_1\gamma_1 + \ldots + c_{k_1k_2}\gamma_{k_1k_2},$$

where $Q(\rho_2) = Q(\gamma_0, \ldots, \gamma_{k_1k_2})$, and the c_i's are integers less than n^4. We let $h_2(x)$ be the minimal polynomial for ρ_2 over Q.

We have found fields $F_1 = Q(\rho_1) = Q[x]/h_1(x) = Q[x,y]/h_2(x)g_1(y)$ and $F_2 = Q(\rho_2) = Q[x]/h_2(x)$ such that

1) the Galois group of $f(x)$ over $Q(\rho_1)$ acts primitively on the roots of $f(x)$,

2) the Galois group of $h_1(x)$ over $Q(\rho_2)$ 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 BLOCKS $(h_i(x))$ returns a polynomial in $Q[x]$, determines a set of fields $F_i = Q(\rho_i)$, $i = 1, \ldots, k$, such that if $g_i(y)$ is the minimal polynomial for ρ_i over $Q(\rho_{i+1})$, and G_i is the Galois group of $g_i(y)$ over $Q(\rho_{i+1})$, 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 $h_i(x)$ have succinct descriptions. This is because the roots of $h_i(x)$ are sums of symmetric functions of the roots of $f(x)$. We claim:

3) $|h_i(x)| \leq |f(x)|^{2m^2}$ for $i = 1, 2$, and

4) $[\![g_1(x)]\!] \leq m![\![f(x)]\!]^{m^4}$.

but omit the proof.

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

1) $Q[x,y]/h_1(x)g_0(y) \simeq Q[z]/f(z)$

2) $h_i(x) \in Q[x]$, and

$g_{i-1}(y) \in Q[x,y]/h_i(x)$, 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 $h_r(x)$ over Q acts primitively on the roots of $h_r(x)$.

The algorithm appears in the appendix.

Theorem 3.3: Let $f(z) \in Z(z)$ 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 $BLOCKS(g(x))$ be the running time for BLOCKS on input $g(x)$. Then the running time for FIELDS is $O(\log m BLOCKS(g(x)))$, where degree$(g(x)) \leq m$, and the coefficients of $g(x)$ are less than $m^2 \log(m![\![f(x)]\!])$.

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 iff every element of $Q(\beta)$ can be written in radicals over Q, *and* every element of $Q(\alpha)$ 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 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 β_{i-1} over $Q(\beta_i)$.

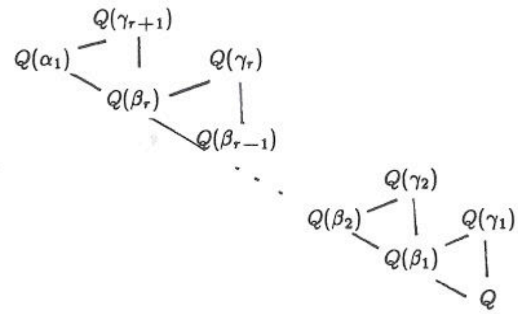

Figure 3.1: The Primitive Extensions Between Q and $Q(\alpha)$

We consider what this means group-theoretically. Suppose $\{ \beta_i \mid i = 1, \ldots, r+1 \}$ are such that if $g_i(y)$ is the minimal polynomial for β_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 $Q(\beta_{i-1})$, let $\{ \alpha_1, \ldots, \alpha_k \}$ be the block of imprimitivity associated with $Q(\beta_1)$, and let $\{ \alpha_{k+1}, \ldots, \alpha_{2k} \}, \ldots, \{ \alpha_{(t-1)k+1}, \ldots, \alpha_m \}$, be the conjugate blocks. Then, if $Q(\theta_2), \ldots, Q(\theta_t)$ are the fields associated with the conjugate blocks, we know that $Q(\theta_i) \subseteq Q(\gamma_1)$, for $i = 1, \ldots, t$. This means that the Galois group H_1 of $Q(\alpha_1, \ldots, \alpha_m)$ over $Q(\gamma_1)$ fixes each of the $Q(\theta_i)$. Assume L_1 is the subgroup of the Galois group which fixes $Q(\beta_1)$. Clearly $H_1 \subseteq L_1$; furthermore, $H_1 \subseteq$ (induced action of L_1 on $\alpha_1, \ldots, \alpha_k)^t$. If K_1 is the Galois group of $Q(\alpha_1, \ldots, \alpha_k)$ over $Q(\beta_1)$, then $H_1 \subseteq K_1^t$, 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 suprisingly easy to answer, for primitive solvable groups are highly structured, which limits their size.

Theorem 3.4 [Pálfy]: If G is a primitive solvable group which acts transitively on n elements, then $|G| \leq 24^{-1/3}n^c$, for a constant $c = 3.24399\ldots$.

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 generalization of Corollary 6 [La] , 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 $K = Q(\theta)$, θ is an algebraic integer of degree l over Q, and O_K is the ring of integers of K. Algorithm 3.2, FIELDS, returns $g(y)$ and $\{\tau_i\}$, where $K[y]/g(y)$ is the splitting field for $f(x)$ over K, and the $\{\tau_i \mid i = 1,\ldots,n\}$, form the Galois group of $f(x)$ over K. It does so in $O((|G|l)^{9+\epsilon}(|G|\log|G|[\![f(x)]\!] + l^3\log[\![\theta]\!])^{2+\epsilon})$ 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 $Q(\beta_i)$, $i = 1,\ldots,r+1$, such that $Q(\beta_{r+1}) = Q$, and $Q(\beta_1) = Q(\alpha)$, and for $j = 1,\ldots,r$, the Galois group of $Q(\beta_j)$ over $Q(\beta_{j+1})$ acts primitively on the conjugates of β_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 $g_i(y)$ be the polynomial described in FIELDS, and suppose the degree of $g_i(y)$ is n_i. By construction the extension $Q[x]/h_{i-1}(x)$ over $Q[x]/h_i(x)$ has Galois group which acts primitively on the roots of $g_{i-1}(y)$. By Theorem 3.4, if this group is solvable, then its order must be less than $24^{-1/3}n_{i-1}^{3.25}$. 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 $24^{-1/3}n_{i-1}^{3.25}$. 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_{i-1}, these algorithms can check solvability of the group in polynomial time. Let SOLVABLEGP be the reader's favorite algorithm for testing if a given group is solvable. We assume that the input to SOLVABLEGP is a set $\{\tau_i \mid i = 1,\ldots,n\}$ which forms the Galois group for $g_{i-1}(y)$ over $Q[x]/h_i(x)$. Then SOLVABLEGP 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 $(degree(g_{i-1}(y)))^{k_i}$ 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 SOLVABLEGP$\{\tau_i\}$
If SOLVABLEGP$\{\tau_i\}$ = "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 α 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 α 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 $Q \subseteq Q(\beta_r) \subseteq \ldots \subseteq Q(\beta_1) \subseteq Q(\alpha)$, and the Galois group of $Q(\beta_i)$ over $Q(\beta_{i+1})$ acts primitively on the roots of the minimal polynomial of β_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 l^{th} roots of unity, where $l = [Q(\gamma_r) : Q]$. We claim that there is a straight line program which expresses ζ_l, a primitive l^{th} root of unity, in radicals in polynomial time. Since the proof is similar to that for expressing β_i as radicals in polynomial time, we begin by showing a bound for the β_i's. We find elements $\tilde{\beta}_i$ such that $Q(\tilde{\beta}_i) = Q(\zeta_l, \beta_i)$. To write straight line code to express α as radicals over $\tilde{Q}$, 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 $\tilde{Q}$ and $\tilde{Q}(\alpha)$. (The bounds we present are not best possible, but are simplified for the sake of readability.)

Lemma 4.3: If $\tilde{h}_i(x)$ is the minimal polynomial for $\tilde{\beta}_i$ over Q, then $|\tilde{h}_i(x)| \leq O(|f(x)|^{m^6})$. If $\tilde{g}_i(x)$ is the minimal polynomial for $\tilde{\beta}_i$ over $Q(\tilde{\beta}_{i+1})$, then $[\![\tilde{g}_i(x)]\!] \leq O(|f(x)|^{m^{12}})$.

Lemma 4.4: If $\tilde{k}_i(x)$ is the minimal polynomial for γ_i over $Q(\tilde{\beta}_{i+1})$, then $[\![\tilde{k}_i(x)]\!] \leq O(|f(x)|^{m^9})$.

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 $\{e\} = H_0 \subsetneq H_1 \subsetneq \ldots \subsetneq H_r = H$, where H_k is normal in H_{k+1}, and H_{k+1}/H_k is of prime order [Sims],[FHL]. We let

$$j_r(x) = \prod_{\sigma_s \in H_k} \sigma_s(x - \gamma_i);$$

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

We conclude:

Lemma 4.5: Let $\tilde{j}_k(x)$ be the minimal polynomial for θ_k over Q. Then $|\tilde{j}_k(x)| \leq O(|f(x)|^{m^{14}})$. If $i_k(x)$ is the minimal polynomial for θ_k over $Q(\tilde{\beta}_{k-1})$, then $[\![\tilde{i}_k(x)]\!] < O(|f(x)|^{m^{21}})$.

We have determined primitive elements θ_i such that $Q(\tilde{\gamma}_i)$ is a cyclic extension of $Q(\theta_r)$, $Q(\theta_{j+1})$ is a cyclic extension of $Q(\theta_j)$, and $Q(\theta_1)$ is a cyclic extension of $Q(\tilde{\beta}_{i+1})$. (For the sake of simplicity, let $\theta_0 = \tilde{\beta}_{i+1}$.) Denote $[Q(\theta_i) : Q(\theta_{i-1})]$ by d_i.

We inductively express $\eta_1, \ldots, \eta_{r+1}$ such that $Q(\theta_j, \eta_j) = Q(\theta_{j+1})$, and $\eta_j = \sqrt[d_j]{p_j(\theta_j)}$, where $p_j(x) \in Q[x]$. Since η_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 Rothschild [Theorem 1.3] that $p_1(x)$ has polynomial size coefficients.

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

We have not yet shown how to express the l^{th} roots of unity as radicals over Q, but Lemma 4.2 is effective. We observe that in order to express the l^{th} roots of unity as radicals over Q, we need to have the p_i^{th} roots of unity expressed as radicals, where p_i is a prime divisor of $\varphi(l)$. Of course, this requires that q_j^{th} roots of unity are expressed as radicals, where q_j is a prime divisor of $p_i - 1$. This inductive construction requires no more that $\log l$ steps. Therefore we conclude that

α can be expressed as radicals over Q in a field of degree no greater than $l^{\log l}$ over Q.

It would be much more pleasing to express α in polynomial time in the form:

$$\sqrt[17]{\frac{1+\sqrt{5}}{2}+\sqrt[1729]{65537}}$$

rather than what we have proposed here. However, certain examples the field which contains α expressed in radicals in the usual way will be of degree $l^{\log l}$ over Q. This indicates that Theorem 4.6 may be the best we can do.*

5. Open Questions

If now you give us a polynomial which you have chosen at your pleasure, and if you want to know if it is or is not solvable by radicals, we have the techniques to answer that question in polynomial time. We have transformed Galois' exponential time methods into a polynomial time algorithm. Furthermore, if the polynomial is solvable by radicals, we can express the roots in radicals using a suitable encoding. Although we have provided a polynomial time algorithm for the motivating problem of Galois Theory, we leave unresolved many interesting questions. In light of the running times presented in Section 3, we hesitate to claim practicality for our polynomial time algorithm. This suggests the following set of questions:

1) All of our running times are based on the time needed by the L^3 algorithm for factoring polynomials over the integers. Can the present time bound be improved?

2) In Section 2 we presented an algorithm which determines a minimal block of imprimitivity of the Galois group of the irreducible polynomial $f(x)$ over the field K. Is there a faster algorithm than Algorithm 2.1 for determining the minimal blocks of imprimitivity? We conjecture that any algorithm that determines minimal blocks of imprimitivity must factor $f(x)$ over $K[x]/f(x)$; we would like to see a proof of this.

The divide-and-conquer technique used to determine solvability answers the question without actually determining the order of the group. We ask:

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?

tually 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 $\mathrm{disc}(f(x))$ is a square in Q. This means that the Galois group of an irreducible polynomial of degree 3 over Q may be found by simply calculating the discriminant. Various tricks and methods have been used to determine the Galois group of polynomials over Q of degree less than 10 [Mc],[St], [Za], but until the recent results concerning polynomial factorization 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: $f(x) \in Z[x]$, $f(x)$ irreducible of degree n over Z

Step 1: Find $c \neq 0$ such that $N_{(Q[z]/f(z))/Q}(f(x-cz))$ is squarefree and factor $N_{(Q[z]/f(z))/Q}(f(x-cz))$ over Q,

$$N_{(Q[z]/f(z))/Q}(f(x-cz)) = \prod_{i=1}^{l} G_i(x-cz)$$

[At most n^3 c's in Z do not satisfy this condition.]

Step 2: For $i = 1 \ldots l$ do: $g_i^z(x) \leftarrow \gcd(f(x), G_i(x))$ over $Q[z]/f(z)$.

[Thus $f(x) = \prod g_i(x)$ is a complete factorization of $f(x)$ over $Q[z]/f(z)$.]

*The second author claims to have shown that polynomial size representation of roots of radicals is possible given symbols ζ_i 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

$B^z(x) \leftarrow \prod_{\alpha_i \in \text{block}}(x - \alpha_i)$, and

return $B^z(x)$

[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 $N_{(Q[z]/f(z))/Q}(f(x-cz))$ do steps 5-9:

Step 5: $q_j(t) \leftarrow$ constant term of $\gcd(g_j(x), f(t-cx))$ over $Q[t,x]/G_j(t)$

$p_j(t) \leftarrow t - cq_j(t)$

[This computes y and z in terms of a primitive element for the field $Q[y,z]/(g(y)g_i^z(z)) = Q[t]/G_i(t)$.]

Step 6: For $i = 1 \ldots l$, do:

$g_i^z(x) \leftarrow g_i^{p_j(t)}(x)$

$g_i^y(x) \leftarrow g_i^{q_j(t)}(x)$

[This rewrites the factorizations of $f(x)$ over $Q[z]/f(x)$ and $Q[y]/f(y)$ as factorizations over $Q[t]/G_j(t)$.]

Step 7: Compute the graph $\Gamma_j = \langle V_j, E_j \rangle$, with vertices, V_j, and edges, E_j given by:

$V_j = \{ g_i^y(x) \} \cup \{ g_k^z(x) \}$

$E_j = \{ \langle g_i^y(x), g_k^z(x) \rangle \mid \gcd(g_i^y(x), g_k^z(x)) \neq 1 \}$

Step 8: Compute $Y_j = \{ i \mid g_i^z(x)$ is connected to $g_1^z(x) = x - p_j(t)$ in $\Gamma_j \}$

Step 9: $B_j(x) \leftarrow \prod_{i \in Y} g_i^z(x)$

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

return $B^z(x) \in Q[x,z]/f(z)$, 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: $i \leftarrow 1$

$h_0(x) \leftarrow f(x)$

$C^z(t) \leftarrow$ BLOCKS$(f(z))$

$g_0(t) \leftarrow t^l + c_{l-1}(z)t^{l-1} + \ldots + c_0(z) \leftarrow C^z(t)$

[$C^z(t)$ will be the polynomial whose norm we compute in order to determine the chain of fields.]

Step 2: While $C^z(t) \notin Q[t]$, do steps 3-17

Else go to **return**

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

Step 4: $\beta(z) \leftarrow a_0(z)$

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 $Q[a_{k-1}(z), \ldots, a_0(z)]/f(z) \simeq Q[\beta(z)]/f(z)$.]

Step 6: $l \leftarrow 1$

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 $\beta^l(z) + d_{l-1}\beta^{l-1}(z) + \ldots + d_0 = 0$,

$h_i(x) \leftarrow x^l + d_{l-1}x^{l-1} + \ldots + d_0$

[This determines the minimal polynomial for $\beta(z)$ over Q; we have $Q[\beta(z)]/f(z) = Q[x]/h_i(x)$.]

Step 9: For $j = 0, \ldots, l-1$, do:

Find $p_j(x)$ such that $p_j(\beta(z)) = c_j(z)$

Step 10: $g_{i-1}(y) \leftarrow y^l + p_{l-1}(x)y^{l-1} + \ldots + p_0(x)$

[Then $Q[t]/h_{i-1}(t) \simeq Q[x,y]/h_i(x)g_{i-1}(y)$.]

Step 11: For $j = 0, \ldots, k-1$, do:

Find $q_j(x)$ such that $q_j(\beta(z)) = a_j(z)$.

Step 12: $C^z(t) \leftarrow t^k + q_{k-1}(x)t^{k-1} + \ldots + q_0(x)$

[This expresses $C^z(t)$, a polynomial in $Q[\beta(z)]/f(z) \simeq Q[x]/h_i(x)$ in terms of the element x.]

Step 13: $B^z(t) \leftarrow$ BLOCKS$(h_i(x))$;

$t^l + b_{l-1}(x)t^{l-1} + \ldots + b_0(x) \leftarrow B^z(t)$

Step 14: For $j = 0, \ldots, l-1$, do:

$c_j(z) \leftarrow b_j(\beta(z))$

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

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

Step 16: $C^z(t) \leftarrow Res_x(B^z(x), C^z(t))$

Step 17: $i \leftarrow i + 1$

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

1) $Q[x,y]/h_1(x)g_0(y) \simeq Q[z]/f(z)$

2) $h_i(x) \in Q[x]$, and

$g_{i-1}(y) \in Q[x,y]/h_i(x)$, 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 $h_r(x)$ over Q acts primitively on the roots of $h_r(x)$.

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

References

[Ar] E. Artin, *Galois Theory,* University of Notre Dame Press, Notre Dame, 1971.

[At] M. Atkinson, "An Algorithm for Finding the Blocks of a Permutation Group," *Mathematics of Computation,* July, 1975, pp. 911-13.

[Cam] P.J.Cameron, "Finite Permutation Groups and Finite Simple Groups," *Bulletin of the London Mathematical Society, Vol.13,* 1981, pp.1-22.

[Edm] J. Edmonds, "Systems of Distinct Representations and Linear Algebra," *Journal of the National Bureau of Standards, Series B, Vol. 71B, No. 4,* Oct-Dec 1967, pp. 241-5.

[Ed] H. Edwards, *Galois Theory,* Springer-Verlag, New York, to appear.

[FHL] M. Furst, J. Hopcroft, and E. Luks, "Polynomial Time Algorithms for Permutation Groups," *Proc. Twenty-first Annual IEEE Symposium on the Foundations of Computer Science,* 1980, pp. 36-41.

[Ga] Évariste Galois, *Oeuvres Mathematiques,* publieés sous les auspices de la societé mathematique de France, Gauthier-Villars, 1897.

[Lag] J.L. Lagrange, *Reflexions sur la Resolution Algebrique des Equations,* Prussian Academy, 1770.

[La] S. Landau, "Factoring Polynomials over Algebraic Number Fields," to appear.

[Lang] S. Lang, *Algebra,* Addison-Wesley, Reading, Mass., 1971.

[L³] A.K. Lenstra, H.W. Lenstra, and L. Lovasz, "Factoring Polynomials with Rational Coeffients," Tech. Report 82-05, Department of Mathematics, University of Amsterdam.

[Lpc] H.W. Lenstra, private communication.

[Mc] J.McKay, "Some Remarks on Computing Galois Groups," *SIAM Journal of Computing, Vol. 8, No. 3,* August 1979, pp. 344-7.

[Ne] O. Neugebaur, *Mathematical Cuniform Texts,* American Oriental Society, 1945.

[Pa] Palfy, "A Polynomial Bound for the Orders of Primitive Solvable Groups," *Journal of Algebra,* July, 1982, pp. 127-137.

[Sh] H. Shapiro, "An Arithmetical Function Arising from the φ Function," *American Mathematical Monthly, Vol. 50,* 1943, pp.18-30.

[Sims] C. Sims, "Computational Methods in the Study of Permutation Groups," in *Computational Problems in Abstract Algebra,* Pergamon Press, 1970.

[St] R.P.Staduhar, "The Determination of Galois groups," *Mathematics of Computation, Vol. 27,* 1973, pp.981-996.

[Tr] B. Trager, "Algebraic Factoring and Rational Function Integration," *Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation,* pp. 219-226.

[vdW] B.L. van der Waerden, *Modern Algebra,* Frederick Ungar, New York, 1941.

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

[Za] H. Zassenhaus, "On the Group of an Equation," *Computers in Algebra and Number Theory,* G.Birkhoff and M.Hall, eds., SIAM and AMS Proceedings, 1971, pp.69-88.