Reprinted from JOURNAL OF COMPUTER AND SYSTEM SCIENCES
All Rights Reserved by Academic Press, New York and London

Vol. 30, No. 2, April 1985
Printed in Belgium

Solvability by Radicals Is in Polynomial Time*

SUSAN LANDAU† AND GARY LEE MILLER‡

Mathematics Department and Laboratory for Computer Science,
Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Received June 19, 1983; revised September 15, 1984; accepted December 21, 1984

A polynomial time algorithm is presented for the founding question of Galois theory: determining solvability by radicals of a monic irreducible polynomial over the integers. Also a polynomial time algorithm which expresses a root in radicals in terms of a straightline program is given. Polynomial time algorithms are demonstrated for computing blocks of imprimitivity of roots of the polynomial under the action of the Galois group, and for computing intersections of algebraic number fields. In all of the algorithms it is assumed that the number field is given by a primitive element which generates it over the rationals, that the polynomial in question is monic, and that its coefficients are in the integers.

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 millenium and a half before Christ [15]. 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 generalize. Lagrange published a treatise which discussed why the methods that worked for polynomials of degree less than five did not extend to quintic polynomials [8], hoping to shed some light on the problem. Evariste 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." [7].

They require 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-A01 and ONR Grant NOO14-80-C-622.
† Author's present address: Math. Dept., Wesleyan University, Middletown, CT 06457.
‡ Author's present address: Dept. of Computer Science, USC, Los Angeles, CA 90089.

0022-0000/85 $3.00

breakthrough of Lenstra, Lenstra, and Lovasz [12], 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. We transform the inquiry into several problems concerning the solvability of certain primitive groups. We construct a series of polynomials such that the original polynomial is solvable by radicals iff each of the new polynomials is solvable by radicals. Each polynomial is constructed so that its Galois group acts primitively on its roots. Palfy has recently shown that the order of a primitive solvable group of degree n is bounded by $24^{-1/2}n^c$ for a constant $c = 3.24399\ldots$ [16]. We attempt to construct the Galois group of these specified polynomials in polynomial time. 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 $f(x)$ ovr 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 $\mathrm{Q} = Q(\rho_{r+1}) \subset Q(\rho_r) \subset \cdots \subset Q(\rho_1) \subset Q(\rho_0) = Q[x]/f(x)$. The tower of fields we find is rather special. If $g_i(y)$ is the minimal polynomial for ρ_i over $Q(\rho_{i+1})$, then the Galois group of $g_i(y)$ over $Q(\rho_{i+1})$ acts primitively on the roots of $g_i(y)$. The Galois group of $f(x)$ over Q is solvable iff the Galois group of $g_i(y)$ over $Q(\rho_{i+1})$ is solvable for $i = 0,\ldots, r$.

Using a simple bootstrapping technique, it is possible to construct the Galois group of $g_i(y)$ over $Q(\rho_{i+1})$ in time polynomial in the size of the group and the length of description of $g_i(y)$. Since the ρ_i are determined so that the Galois group of $g_i(y)$ over $Q(\rho_{i+1})$ acts primitively on the roots of $g_i(y)$, 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 $g_i(y)$ over $Q(\rho_{i+1})$ 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 and Galois 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 expression 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 $f(x) = a_n x^n + \cdots + a$, is a polynomial with coefficients in Z, then, Lenstra, Lenstra, and Lovasz [12] showed that

THEOREM 1.1. *A polynomial $f(x)$ in $Z[x]$ of degree n can be factored in $O(n^{9+\varepsilon} + n^{7+\varepsilon} \log^{2+\varepsilon}(\sum a_i^2))$.*

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 a is ***algebraic over a field K*** iff a satisfies a polynomial with coefficients in K. An extension field L is ***algebraic ouer 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 a. The field $Q(\alpha)$ is isomorphic to $Q[t]/g(t)$, where $g(t)$ is the minimal (irreducible) polynomial for a. Let the degree of $g(t)$ be m. The conjugates of a are the remaining roots of $g(t)$: $\alpha_2 \cdots \alpha_m$, a 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 $\beta = a_0 + a_1 + \cdots + a_{m-1}\alpha^{m-1}$, 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 a 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 $(1/d)\,Z[\alpha]$, for some d for which

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

We consider the question of length in greater detail. If $g(t)=t^m+a_{m-1}t^{m-1}+\cdots+a_0$, a_i in Z, then we define the *size* of $g(t)$, $|g(t)|=(\sum_{i=0}^{m-1}a_i^2)^{1/2}$. Following Weinberger and Rothschild [22], we define the *size* of β, $[\beta]$, to be the maximum of the absolute values of the conjugates of β. 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 $f(x)$, $[f(x)]=\max_i(\sum_{j=0}^{m-1}b_{ij}^2)^{1/2}$.

Weinberger and Rothschild showed that the factors of polynomials in algebraic number fields are polynomially bounded in size:

THEOREM 1.2. *Let β be a root of $Z[\alpha][x]$, notation as above. Then $[\beta]\leqslant[f(x)]$. Assume that $f(x)$ is monic, and let*

$$h(x)=h_r x^r+h_{r-1}x^{r-1}+\cdots+h_0$$

be a factor of $f(x)$ in $(1/d)Z[\alpha][x]$ which is primitive. If $h_i=(1/d)(c_{im-1}\alpha^{m-1}+\ldots+c_{i0})$, then $|c_{ij}|<m![f(x)]^n|g(t)|^{m^2}$

A detailed proof appears in [9].

A classical technique to reduce questions in number fields to questions in the rationals is the *norm*. If the conjugates of $a=a_1$ over K are $\alpha_2,\ldots,\alpha_n$ then if $\beta=a_0+a_1\alpha+\cdots+a_{m-1}\alpha^{m-1}$ is an element of $K(\alpha)$, the $\mathrm{Norm}_{K(\alpha)/K}(\beta)=N_\alpha(\beta)=\prod_i(a_0+a_1\alpha_i+\cdots+a_{m-1}\alpha_i^{m-1})$. We can think of a polynomial $f(x)$ in $Q(\alpha)[x]$ as a polynomial in two variables, x and a, and denote it by $f_\alpha(x)$. It is quite natural to extend the definition of norm to polynomials in $Q(\alpha)[x]$ by

$$N(f(x))=\prod_i f_{\alpha_i}(x).$$

If $f(x)$ is in $Q(\alpha[x])$, then $N(f(x))$ is in $Q[x]$. Under appropriate hypothesis, a polynomial in $Q(\alpha)[x]$ can be factored by taking the norm of the polynomial, factoring the norm over the rationals and raising that to a factorization of the polynomial over the number field. It was shown in [9] that these techniques lead to a polynomial time algorithm for factoring polynomials over algebraic number fields:

THEOREM 1.3. *Let a satisfy $g(t)$, 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 $Q(\alpha)[x]$ in $O(m^{9+\varepsilon}n^{7+\varepsilon}\log^{2+\varepsilon}([f(x)](m|g(t)|)^n(mn)^n))$ steps.*

We note that in factoring $f(x)$ over $Q(\alpha)$ we obtain a primitive element for the field $Q(\alpha,\beta)$, where β is a root of $f(x)$ different from α. This will prove useful in Algorithm 2.1.

We conclude with a brief review of Galois theory; for a more complete treatment the reader may consult either Artin [1] or Lang [11].

Let K be an algebraic number field, and let $f(x)$ be a polynomial with coefficients in K, with roots $a_1,\ldots,a_n$. Then $K(\alpha_i)\sim K[x]/f(x)\sim K(\alpha_j)$, but in general

$K(\alpha_i) \neq K(\alpha_j)$ for $i \neq j$. The field $K(\alpha_1,..., a_n)$ is called the *splittingfield of* $f(x)$ *over* K. We consider the set of automorphisms of $K(\alpha_1,..., a_n)$ which leave K fixed. These form a group, called the *Galois group of* $K(\alpha_1,..., a_n)$ *over* K. *As* we can think of these automorphisms as permutations on the a_i, this group is sometimes referred to as the *Galois group of* $f(x)$ *over* K. The Galois group is *transitive* on $\{\alpha_1,..., a_n\}$, that is, for each pair of elements α_i, 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 $K(\alpha_1,..., a_n)$.

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

$$K \subseteq K(\alpha_1,..., a_n)^H \subseteq K(\alpha_1,..., a_n).$$

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

FUNDAMENTAL THEOREM OF GALOIS THEORY. *Let* K *be afield, and let* $f(x)$ *with roots* $\alpha_1,..., a_n$ *be irreducible over* $K[x]$. *Then*

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

(2) *The field* $K(\beta)$ *is uniquely determined by* H, *for* $K(\beta)$ *is the set of elements of* $K(\alpha_1,..., a_n)$ *which are invariant under action of* H.

(3) *The subgroup* H *is normal iff* $K(\alpha_1,..., a_n)$ *over* $K(\beta)$ *is a Galois extension, that is, iff the minimal polynomial for* β *over* K *splits into linear factors over* K. *In that case the Galois group of* $K(\beta)$ *over* K *is* G/H.

(4) $|G| = [(K(\alpha_1,..., a_n): K]$, *and* $|H| = [K(\alpha_1,..., a_n): K(\beta)]$.

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. If*

$$K \subset L_1 \subset L_2 \subset K(\alpha_1,..., a_n),$$

then the group G_2 *corresponding to* L_2 *is a subgroup of the group* G_1 *corresponding to* L_1, *and vice versa.*

THEOREM B. *Let the hypothesis be as in the fundamental theorem. Then*

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

(2) The field corresponding to H, 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 $\sqrt[m]{a}$ is a many valued function, as in, for example $\sqrt[17]{1}$. We will require that all solutions to the equation in question be represented by expressions of the form

$$\sqrt[y]{\sqrt[h]{p+\cdots}+\sqrt[s]{\cdots}} \tag{1}$$

(or similar ones), and that these expressions are to represent solutions of the equation for *any* evaluation 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 (see [20]), let us consider for a moment determining expressibility of a root in radicals over $Q(\zeta_m)$, where ζ_m is a primitive mth root of unity. This will simplify the situation. Suppose a root α_i is expressible in terms of radicals, and the expression is an mth root. If m is not prime, $m = m_1 m_2$. Then taking an mth root could be broken up into two steps, first taking m_1st root, then an m_2nd root. By further decomposition, one need only take roots of prime degree. This would give rise to a series of field extensions, $Q(\zeta_m) = F_0 \subset F, \subset \cdots \subset F_k$, where F_i is an extension of F_{i-1} which is obtained by taking a p_ith root of some element in F_{i-1}. Each extension is Galois. The accompanying tower of groups $G_k \subset G_{k-1} \subset \cdots \subset G_0$, where G_i is the subgroup of G which fixes F_{k-i} satisfies the following two important conditions: G_i is *normal* in G_{i-1}, and G_{i-1}/G_i 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* (1), *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* (1) *in such a way that the successive extensions F_i over F_{i-1} are extensions of prime degree, with $F_i = F_{i-1}(\sqrt[p]{a_i})$, with $a_i \in F_{i-1}$, and $x^p - a_i$ irreducible over F_{i-} ,.*

Galois transformed the problem of checking solvability by radicals to a problem of determining if the Galois 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 [17, 6] 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

Let a be a root of $f(x)$. If $f(x)$ is a normal polynomial, i.e., if $f(x)$ factors completely in $Q(\alpha)[x]$, the Galois group can be computed easily. Suppose $f(x)=(x-\alpha)(x-a_2)\cdots(x-a_n)$ in $Q(\alpha)[x]$, then the α_i's will be expressed as polynomials in a, with $\alpha_i=p_i(\alpha)$. Since the Galois group is a permutation group of order m on m elements, for each a, 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 can be determined.

Thus in the case that $f(x)$ is normal, we can construct a group table for G and check solvability in polynomial time [17, 6]. Of course, it is rare that $f(x)$ is normal. We now develop some group theory to handle the nonnormal situation.

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

$$\{\alpha_1,\ldots,\alpha_n\}=\Omega.$$

We define

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

and we call G *regular* if G_a is transitive and $G_a=1$ for all a. 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 $\varnothing$. It is not hard to see that if B is a block, σB is also. We will let G_Δ be the subgroup of G which fixes the block Δ setwise.

Every group has trivial blocks: $\{a\}$ or Ω. The nontrivial blocks are called *blocks of imprimitiuity,* and a group with only trivial blocks is called a *primitive* group. The set of all blocks conjugate to B: B, $\sigma_2 B\cdots\sigma_t B$, 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; proofs and further details may be found in Wielandt [21].

THEOREM 2.1. *Let $a\in\Omega$, $|\Omega|\neq 1$. Then the transitive group G on Ω is primitive iff G_a is maximal.*

PROPOSITION *2.2. The lattice of groups between G_a and G is isomorphic to the lattice of blocks containing a.*

THEOREM 2.3. *Let $\Lambda \subset \Omega$, and $\alpha \in \Omega$. Then*

$$\Lambda = \bigcap_{\alpha \in \sigma(\Lambda)} \sigma(\Lambda)$$

is a block of the transitive group G.

COROLLARY 2.4. *Let*

$$\Lambda = \{\beta \mid \sigma(\beta) = \beta \ (\forall \sigma \in G_\alpha)\}.$$

Then Λ is a block of G.

Proof. We let $\Lambda = \{\beta \mid \sigma(\beta) = \beta(\forall \sigma \in G_\alpha)\}$. Let β be fixed by G_α, that is, $\beta \in \Lambda$. Then $\sigma \in G_\alpha$ implies that $\sigma \in G_\beta$. But $|G_\beta| = |G_\alpha|$ means that $G_\alpha = G_\beta$.

Now suppose that $\beta \in \sigma\Lambda \cap \Lambda$. Then $\beta = \sigma(\gamma)$, where $\tau(\beta) = \beta$ and $\tau(\gamma) = \gamma$ for all $\tau \in G_\Lambda$. Furthermore $\sigma^{-1}(\beta) = \gamma$ implies that $\sigma\tau\sigma^{-1}(\beta) = \sigma\tau(\gamma) = \sigma(\gamma) = \beta$. Therefore $\sigma\tau\sigma^{-1}$ is an element of $G_\beta = G_\alpha$. Thus $\sigma\tau\sigma^{-1}(\alpha) = \alpha$.

Let ρ be an element of Λ. Then $\sigma\tau\sigma^{-1}(\rho) = \rho$, and $\tau\sigma^{-1}(\rho) = \sigma^{-1}(\rho)$ for all τ in G_α. Then $\sigma^{-1}(\rho)$ is in Λ. Therefore $\sigma^{-1}\Lambda = \Lambda$ or $\Lambda = \sigma\Lambda$, which was to have been shown. ∎

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}. By Corollary 2.4, the linear factors of $f(x)$ form a block. Suppose the block Λ described in Corollary 2.4 consists of the roots $\alpha_1, \ldots, \alpha_k$. Consider the induced action of G_Λ on A. Since G is transitive on $\alpha_1, \ldots, \alpha_m$, G_Λ must be transitive on $\alpha_1, \ldots, \alpha_k$. The action of G_Λ on Λ can be determined, since for $l = 1, \ldots, k$, $\alpha_l = p_l(\alpha_1)$. Let σ be in G_Λ, and let $\bar{\sigma}$ be the induced action of σ on $\alpha_1, \ldots, \alpha_k$. Then if $\overline{\sigma_j}(\alpha_1) = \alpha_j = p_j(\alpha_1)$, we have $\bar{\sigma}(\alpha_l) = \bar{p}_j(\alpha_l) = p_j(p_l(\alpha_1))$. In polynomial time we can determine the group table of the induced action of G_Λ on Λ. Then we can find a minimal block Γ of G_Λ which contains α_1 in polynomial time by Atkinson [2].

Finally we observe that Γ is a block of G. For suppose that $\Gamma \cap \tau\Gamma \neq \varnothing$ 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 if $\Gamma \cap \tau(\Gamma) \neq \varnothing$ it must be the case that $\Gamma \cap \tau\Gamma = \Gamma$.

Note that this algorithm is just a generalization of the case in which $f(x)$ is normal. We now develop some group theory to handle the case in which $f(x)$ has only one linear factor in $Q(\alpha)[x]$.

THEOREM 2.5. *Suppose that G is not regular of prime degree. Let α be an element of Ω, $|\Omega| \neq 1$. Then the transitive group G on Ω is primitive iff $\forall \alpha \neq \beta$, $\langle (G_\alpha, G_\beta) \rangle = G$.*

Proof. Let Λ be a nontrivial block of imprimitivity, with α, β elements of Λ, with $\alpha \neq \beta$. Then $G_\alpha, G_\beta \subset G_\Lambda$ implies $\langle G_\alpha, G_\beta \rangle \subset G_\Lambda$. Since Λ is a nontrivial block of imprimitivity, $G_\Lambda \subsetneq G$, and we conclude $\langle G_\alpha, G_\beta \rangle \subsetneq G$.

Next we assume $\langle G_\alpha, G_\beta \rangle \neq G$ for some $\beta \neq \alpha$. Let

$$\Lambda = \{\sigma(\alpha) \mid \sigma \in \langle G_\alpha, G_\beta \rangle\}.$$

We claim A is a block. For suppose γ is contained in $A \cap \tau\Delta$, τ an element of G. Then $\gamma = \sigma_1(\alpha) = \tau\sigma_2(\alpha)$, for some σ_1, σ_2 in $\langle G_\alpha, G_1 \rangle$. But $a = \sigma_1^{-1}\tau\sigma_2(\alpha)$ implies that $\sigma_1^{-1}\tau\sigma_2$ is in G_1. Since σ_1, σ_2 are both in $\langle G_\alpha, G_1 \rangle$, we have τ is an element of $\langle G_1, G_\beta \rangle$; therefore $A = \tau\Delta$, and A is a block. If A is nontrivial we are done.

Suppose $A = \{a\}$. Then $G_1 = G_1$, and we let

$$\Delta = \{\gamma \mid \sigma(\gamma) = \gamma \ \forall \sigma \in G_\alpha\}.$$

We know a, β are in Δ, so Δ is nontrivial. Furthermore G is transitive, so $\Delta \neq \Omega$. By Corollary 2.4, Δ is a block.

Our final case occurs when $\Delta = \Omega$. Let τ be an element of G, and suppose $\tau(\alpha) = \gamma$. Then there is a σ in $\langle G_\alpha, G_1 \rangle$, with $\sigma(\alpha) = \gamma$. Thus $\tau^{-1}\sigma(\alpha) = \alpha$, and $\tau^{-1}\sigma$ belongs to G_1. But this would mean that τ is in $\langle G_1, G_1 \rangle$, and that $\langle G_1, G_1 \rangle = G$, contrary to assumption. We are done. ∎

PROPOSITION 2.6. Suppose G acts transitively on Ω, and G_1 has no *fixed* points except a. Let A be a minimal nontrivial block containing a. Then *for all* γ in A, $\gamma \neq a$, $\Delta = \{\sigma(\alpha) \mid \sigma \in \langle G_\alpha, G_\gamma \rangle\}$.

Proof. Let γ be in Δ, $\gamma \neq \alpha$. Then we let $\Delta = \{\sigma(\alpha) \mid \sigma \in \langle G_\alpha, G_\gamma \rangle\}$. Since $\langle G_\alpha, G_\gamma \rangle \subset G_\Delta$, we have $\Delta \subset \Delta$.

Next, suppose β is an element in $\Delta \cap \tau\Delta$ for some τ in G. Then $\beta = \sigma_1(\alpha)$ and $\beta = \tau\sigma_2(\alpha)$, with σ_1, σ_2 elements in $\langle G_\alpha, G_1 \rangle$. But $a = \sigma_1^{-1}\tau\sigma_2(\alpha)$ means that $\sigma_1^{-1}\tau\sigma_2$ is an element of G_1. Then τ belongs to $\langle G_1, G_1 \rangle$, and $\tau\Delta = \Delta$. Therefore Δ is a block. But A is a minimal nontrivial block containing a; therefore $\Delta = \Delta$. ∎

Proposition **2.6** provides a way to compute a minimal block of imprimitivity. Since the roots of the irreducible factors of $f(x)$ in $Q(\alpha)[x]$ form the orbits of G_1, the orbit structure of G, can be determined from a factorization of $f(x)$ in $Q(\alpha)[x]$. We can likewise deduce the orbit structure of G_1 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_1 and G_1 so as to determine whether $\langle G_\alpha, G_1 \rangle = G$. Observe that since G is a transitive group, a may be fixed, and only β need vary.

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

$$f(x) = (x - \alpha_1)\, g_2(x) \cdots g_r(x) \qquad \text{in} \quad Q(\alpha_1)[x],$$

and

$$f(x) = (x - \alpha_j)\, h_2(x) \cdots h_r(x) \qquad \text{in} \quad Q(\alpha_j)[x],$$

with $g_1(x) = x - a$, and $h_1(x) = x - a$. (The factorization of $f(x)$ over $Q(\alpha_j)[x]$ is the same as the factorization of $f(x)$ over $Q(\alpha_1)[x]$, with α_j's substituted in for α_1'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 a_1 if it exists. Let us consider a factorization of $f(x)$ over $Q(\alpha_1, \alpha_j)[x]$ for $\alpha_j \neq a_1$. By tying the factorization of $f(x)$ over $Q(\alpha_1)[x]$ to its factorization over $Q(\alpha_j)[x]$, we are able to compute the block fixed by $\langle G_{\alpha_1}, G_{\alpha_j} \rangle$.

Define a set of graphs Γ_j, $j = 2,..., r$ with vertices V, and edges E by

$$V = \{g_i(x), i = 1,..., r\} \cup \{h_i(x), 1 = 1,..., r\}$$

$$E = \{\langle g_i(x), h_k(x) \rangle \mid \gcd(g_i(x), h_k(x)) \neq 1 \text{ over } Q(\alpha_1, \alpha_j)\}.$$

Now there is an edge between $g_i(x)$ and $h_k(x)$ iff $\gcd(g_i(x), h_k(x)) \neq 1$; identically, there is an edge between $g_i(x)$ and $h_k(x)$ iff they have a common root. We compute the set of vertices connected to $g_1(x)$. Let

$$g(x) = \prod_{\substack{g_i(x) \text{ is} \\ \text{connected to } g_1(x)}} g_i(x),$$

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

LEMMA 2.7. *Let a_i be a root of $g_i(x)$ in $Q(\alpha_1)[x]$. Then the roots of $g_i(x)$ are precisely $G_{\alpha_1}(a_i)$.*

Suppose $h_k(x)$ is connected to $g_1(x)$. Then α_1 is a root of $h_k(x)$, and if $\beta_1,..., \beta_k$ are also roots of $h_k(x)$, then $G_{\alpha_j}(\alpha_1) \subset \{\beta_1,..., \beta_k\}$. Suppose the $h_k(x)$ is also connected to $g_i(x)$, with roots $a_{i_1},..., a_{i_r}$. Then $\{\alpha_1, \alpha_{i_1},..., \alpha_{i_r}\} \subset (G_{,,}, G_{\alpha_j})(\alpha_1)$. It follows that the $\gcd(g_i(x), h_k(x)) \neq 1$ iff $G_{\alpha_1}(\alpha_i) \cap G_{\alpha_j}(\alpha_k) \neq \emptyset$, where α_i is a root of $g_i(x)$ and α_k is a root of $h_k(x)$. This implies

LEMMA 2.8. *Let α_l be a root of $g_l(x)$, a factor of $f(x)$ in $Q(\alpha_1)[x]$. Then*

$$\alpha_j \in \Lambda_j = \{\sigma(\alpha_1) \mid \sigma \in \langle G_{\alpha_1}, G_{\alpha_j} \rangle\}$$

iff $g_j(x)$ is connected to $g_1(x)$.

If we compute Γ_j for $j = 2,..., r$, we are cycling over all $a_i \neq \alpha_1$ which are roots of $f(x)$, and computing $(G_{,,}, G_{\alpha_j})(\alpha_1)$. By Proposition 2.6, this will give us a minimal nontrivial block containing α_1, if one exists.

We now briefly describe our algorithm, details of which appear in the Appendix. Algorithm 2.1 determines minimal blocks of imprimitivity.

Let $f(x)$ be an irreducible polynomial of degree m over Q. We factor $f(x)$ over $Q[z]/f(z)$. If $f(x)$ has more than one linear factor, we compute the induced action of the Galois group on those roots which are elements of $Q[z]/f(z)$. This gives us a group table, from which we can determine a minimal block using Atkinson's algorithm.

Otherwise suppose that $f(x)=g_1^z(x)\,g_2^z(x)\cdots g_r^z(x)$ in $Q[z]/f(z)$, where $g_1^z(x)=(x-z)$. For each $g_j^z(x)$ different from $g_1^z(x)$, we factor $f(x)$ over $Q[z, y]/(f(z), g_j^z(y))$. Let $g_i^y(x)$ be identical to $g_i^z(x)$, with z replaced by y. Then for $j=2,\ldots, r$, we compute the gcd of all pairs of polynomials $g_i^z(x)$ and $g_k^y(x)$ $(i,k=1,\ldots, r)$, over $Q[z, y]/(f(z), g_j^z(y))$. Let Γ_j be the graph with vertices $g_i^z(x)$ and $g_k^y(x)$, and edges defined by $E(g_i^z(x), g_k^z(x))$ iff $\gcd(g_i^z(x), g_k^y(x))$ over $Q[z, y]/(f(z), g_j^z(y))$ is nontrivial. We compute Y_j, which is the set of polynomials $g_i^z(x)$ connected to $g_1^z(x)=x-z$, and let B_j be the product of those polynomials. The algorithm returns the $B_j(x)$ of minimal degree. This is a polynomial whose roots form a minimal block containing z.

At this juncture, we observe that it is unnecessary to actually factor $f(x)$ over $Q[z, y]/f(z), g_j^z(y))$, since we can determine a primitive element for $Q[z, y]/(f(z), g_j^z(y))$ by factoring $f(x)$ over $Q[z]/f(z)$. By computing gcd's of the factors of $f(x)$ over $Q[z]/f(z)$ and $Q[y]/f(y)$, we avoid a factorization of $f(x)$ over $Q[z, y]/(f(z), g_j^z(y))$.

THEOREM **2.9.** *If $f(x)\in Z[x]$ of degree m is irreducible, Algorithm* **2.1** *computes $B(x)$ a polynomial in $Z(\alpha)[x]$ whose roots $\alpha_1\cdots\alpha_k$, are elements of a minimal block of imprimitivity containing a. It does so in the time required to factor $f(x)$ over $Q[z]/f(z)$ and to calculate m^3 gcd's of polynomials of degree less than $\deg(f(x))$ and with coefficient length less than $m^2\log[f(x)]$ over a field containing two roots of $f(z)$.*

We note that Zassenhaus [23] suggests a method for computing Galois groups which also uses blocks of imprimitivity. His method is prima facie exponential, although using our techniques its running time can be improved.

The fundamental theorem of Galois theory establishes the correspondence between field and groups, and we know now that the lattice of groups between G, and G is isomorphic to the lattice of blocks of G which contain a. 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.

A generalization of Algorithm **2.1** gives a method to compute the intersection of $Q(\alpha_1)$ and $Q(\alpha_j)$. Since G_{α_1} is the subgroup of G belonging to the subfield $Q(\alpha_1)$, and G_{α_j} is the subgroup of G belonging to $Q(\alpha_j)$, $\langle G_{\alpha_1}, G_{\alpha_j}\rangle$ is the subgroup of G belonging to $Q(\alpha_1)\cap Q(\alpha_j)$ [Theorem B]. We can compute $Q(\alpha)\cap Q(\beta)$ even when a 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 a and β. The description $Q[x, y]/(f(x), h(y))$, where a 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 $a=\alpha_1$ 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 $\{\beta_j + c\alpha_i \mid j = 1,..., n;\ i = 1,..., m\}$.

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. It appears in the Appendix.

3. Determining Solvability

Let $f(x)$ be a monic irreducible polynomial over Z with roots $\alpha_1,..., \alpha_m$, and Galois group G. Suppose $B_1 = \{\alpha_1,..., \alpha_{k_1}\}$ is a minimal block of imprimitivity containing α_1, and let

$$h_1(x) = \prod_{i=1}^{k_1} (x - \alpha_i) = x^{k_1} + \beta_{k_1 - 1} x^{k_1 - 1} + \cdots + \beta_0.$$

We define $F_1 = Q(\beta_0, \beta_1,..., \beta_{k_1 - 1})$. The minimal polynomial for $\alpha = \alpha_1$ over F_1 is $h_1(x)$. This is easy to see, for

(1) $[Q(\alpha): F_1] = [Q(\alpha_1,..., \alpha_m): Q(\alpha_1)] = |G_{B_1}|/|G_\alpha| = k_1$,

(2) α_1 satisfies $h_1(x)$, a polynomial over F_1.

We observe that since B_1 was chosen as a minimal block containing α_1, the Galois group of $Q(\alpha_1)$ over Q((elementary) symmetric functions in $\{\alpha_1,..., \alpha_{k_1}\}$) acts primitively on the set of roots of $h_1(x)$. Next we consider a tower of fields, F_i, between Q and $Q(\alpha)$, where α is a root of $f(x)$ and has conjugates $\alpha_2,..., \alpha_m$, 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 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 $\alpha_1,..., \alpha_m$ be an irreducible polynomial over $K[x]$. Let $B = \{\alpha_1,..., \alpha_k\}$ be a block of the roots. Then $K(\alpha_1,..., \alpha_m)^{G_B} = K$((elementary) symmetric functions in $\{\alpha_1,..., \alpha_k\}$).*

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((elementary) 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((elementary) symmetric functions in elements of B), then G, acts primitively on B. We would like to find a set of elements ρ_i, $i = 1,..., r$, such that if $g_i(y)$ is the minimal polynomial for ρ_i over $Q(\rho_{i+1})$, then the Galois group G, 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 each $g_i(y)$ will be less than m.) 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 can be resolved by linking the fields $Q(\rho_i)$ and $Q(\rho_{i+1})$ through the polynomial $g_i(y)$.

Of course one way we could determine F_1 would be by calling BLOCKS on $f(x)$. Then if

$$h_1(x) = x^{k_1} + \beta_{k_1-1}x^{k_1-1} + \cdots + \beta_0$$

is the polynomial described earlier, $F_1 = Q(\beta_0,..., \beta_{k_1-1})$, and ρ_1 equals one of the β_i, since F_1 is a field obtained by adjoining (elementary) symmetric functions in a minimal block of imprimitivity.

Let $\sigma_1 B_1,..., \sigma_j B_1$, where σ_1 is the identity, form a complete block system for G acting on the roots of $F(x)$, and suppose that $g_1(x)$ is the minimal polynomial for ρ_1 over Q. Then $g_1(x)$ is of degree $m/k_1 = j$. We know that $\sigma(h_1(x)) = h_1(x)$ for σ in G_1. If $\theta_i = \sigma_i(\rho_1)$ for $i = 1,..., j$, then $\sigma_i(h_1(\rho_1)) = 0$ implies that $\sigma_i(\rho_1) = 0_i$ is a root of $h_1(x)$. Applying BLOCKS to $g_1(x)$ returns a polynomial

$$B(x) = x^{k_2} + \beta_{k_2-1}x^{k_2-1} + \cdots + \beta_0,$$

whose roots $\rho_1,..., \sigma_{k_2}\rho_1$ form a minimal block containing ρ_1. Then

$$\begin{aligned} F_2 &= Q(\beta_{k_2-1},..., \beta_0) \\ &= Q(\text{symmetric functions in } \{\theta_1,..., \theta_j\}) \\ &= Q(\text{symmetric functions in } \{\text{symmetric functions in } (a_1,..., \alpha_{k_1}\},..., \\ &\qquad \text{symmetric functions in } \sigma_j\{a_1,..., \alpha_{k_1}\}\}). \end{aligned}$$

But $Q(\beta_{k_2-1},..., \beta_0)$ is a cumbersome way to name F_2; we would like to name F_2 in terms of the original roots of $f(x)$, $a_1,..., a_n$. Fortunately, there is a simple way to do this.

LEMMA 3.2. *Let $f(x) \in Q[x]$ be irreducible with roots $\alpha = \alpha_1,..., a_n$ 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 $h_1(x)$, $\alpha_1,..., \alpha_{k_1}$, 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 minial block containing B_1.

Proof. Because the fields $Q(\tau), Q(\rho)$ are subfields of $Q(\alpha)$, we know that $Q(\rho)=Q$((elementary) symmetric functions of B), $Q(\tau)=Q$((elementary) symmetric functions in elements of B_2), where B, B_2 are blocks of $\{\alpha_1,\ldots,\alpha_m\}$. However, $h_1(x)$ is irreducible over $Q(\rho)[x]$ with roots $\alpha_1,\ldots,\alpha_{k_1}$, so it must be the case that $B=B_1$. Furthermore, $Q(\tau)\subset Q(\rho)$ implies that $B_1\subset B_2$. We consider the induced action of G on B_2, and let $\sigma_1 B_1,\ldots,\sigma_{k_2-1}B_1$ be a complete block system for B_1 in B_2, with σ_1 equal to the identity, and the σ_i's in G. Then if $g(x)$ is the minimal polynomial for ρ over $Q(\tau)$,

$$g(x)=\prod_{i=1}^{k_2}\sigma_i(x-\rho).$$

In particular,

$$\begin{aligned}N_{Q(\rho)/Q(\tau)}(h_1(x)) &= \prod_{i=1}^{k_2}\sigma_i(h_1(x))\\ &= \prod_j \sigma_j\Bigg(\prod_{\substack{\alpha_i\in\text{minimal}\\ \text{block } ctg\,\alpha=\alpha_1}}(x-\alpha_i)\Bigg)\\ &= \prod_j \prod_{\substack{\alpha_i\in\text{minimal}\\ \text{block } ctg\,\alpha=\alpha_1}}\sigma_j(x-\alpha_i)\\ &= \prod_{i=1}^{k_1k_2}(x-\alpha_i)\end{aligned}$$

will give a polynomial whose roots $\alpha_1,\ldots,\alpha_{k_1k_2}$ are a block of $\alpha_1,\ldots,\alpha_m$ which contain $\alpha_1,\ldots,\alpha_{k_1}$. If the Galois group of $g(x)$ over $Q(\tau)$ acts primitively on the roots of $g(x)$, then B_1 is a minimal block of B_2. ∎

This lemma allows us to compute the blocks of $\alpha_1,\ldots,a$, 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 $\gamma_1,\ldots,\gamma_{k_1k_2}$ are the elementary symmetric functions in $\alpha_1,\ldots,\alpha_{k_1k_2}$, we can determine

$$\rho_2=\gamma_1+c_2\gamma_2+\cdots+c_{k_1k_2}\gamma_{k_1k_2},$$

where $Q(\rho_2)=Q(\gamma_1,\ldots,\gamma_{k_1k_2})$, and the c_i's are integers less than n^4. We let $h_2(x)$ be the minimal polynomial for ρ_2 over $\mathbf{Q}$.

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 tis 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 $F_i = Q(\rho_i)$, $i = 1,..., k$, such that if $g_i(y)$ is the minimal polynomial for ρ_i over $Q(\rho_{i+1})$, and G, is the Galois group of $g_i(y)$ over $Q(\rho_{i+1})$, then G, 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 [10]. This is because the roots of $h_i(x)$ are sums of elementary symmetric functions of the roots of $f(x)$. Then

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

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

Generalizing this procedure yields an algorithm for determining $h_i(x)$ and $g_i(y)$, $i = 1,..., r$ 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

(3) $g_{i-1}(y) \in Q[x, y]/h_i(x)$, for $i = 1,..., r$.

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

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

THEOREM 3.3. *Let $f(z) \in Z(z)$ of degree m be irreducible. Algorithm* **3.1** *computes $\{h_i, g_{i-1} | i = 1,..., r\}$ 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 $(g(x)) \leqslant m$, and the coefficients of $g(x)$ are less than $m^2 \log(m! [f(x)])$.*

The algorithm, a proof of correctness, and an analysis of running time appear in the Appendix.

We can now determine a tower of 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 $Q \subset Q(\beta) \subset Q(\alpha)$. Every element in $Q(\alpha)$ can be written in radicals over Q iff every element of $Q(\alpha)$ can be written in radicals over $Q(\beta)$, *and* every element of $Q(\beta)$ can be written in radicals over Q. Suppose we continued until there were a maximal number of fields between Q and $Q(\alpha)$, with $Q \subset Q(\beta_r) \subset \cdots \subset Q(\beta_1) \subset Q(\alpha)$. We denote a by β_0. The divide-and-conquer terminates 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 $Q(\beta_i)$, for each i from 1 to $r + 1$ (with $Q(\beta_{r+1}) = Q$).

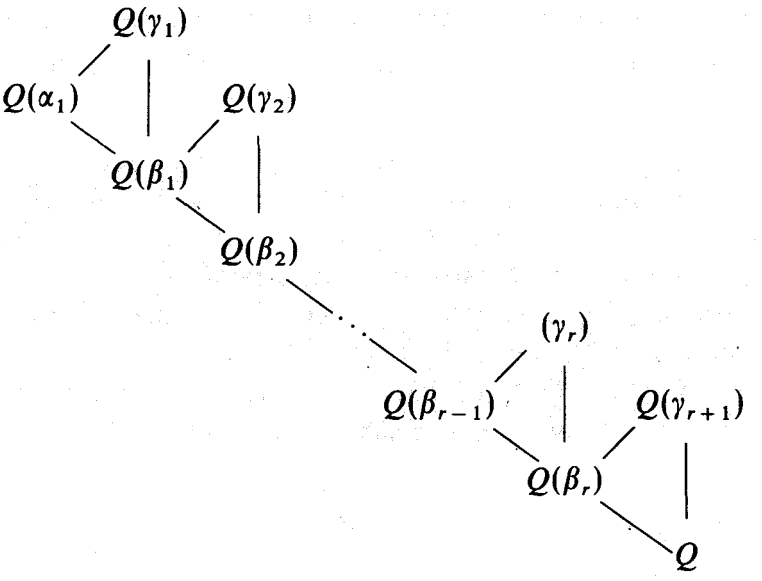

FIG. 3.1. **The primitive extensions between Q and $Q(\alpha)$.**

We consider what this means group-theoretically. Suppose $\{\beta_i | i = 1,..., r+1\}$ 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 $\{\gamma_i | i = 1,..., r+1\}$ is chosen so that $Q(\gamma_i)$ is the splitting field for $Q(\beta_i)$ over $Q(\beta_{i+1})$, let $\{\alpha_1,..., \alpha_k\}$ be the block of imprimitivity associated with $Q(\beta_r)$, and let $\{\alpha_{k+1},..., \alpha_{2k}\},..., \{\alpha_{(t-1)k+1},..., a_{,,,}\}$, be the conjugate blocks. Then, if $Q(\theta_2),..., Q(\theta_t)$ are the fields associated with the conjugate blocks, we know that $Q(\theta_i) \subset Q(\gamma_r)$, for $i = 1,..., t$. This means that the Galois group H_1 of $Q(\alpha_1,..., a_{,,,})$ over $Q(\gamma_r)$ fixes each of the $Q(\theta_i)$. Assume L_1 is the subgroup of the Galois group which fixes $Q(\beta_r)$. Clearly $H_1 \subset$ L, ; furthermore, $H, \subset$ (induced action of L_1 on $\alpha_1,..., \alpha_k)'$. If K_1 is the Galois group of $Q(\alpha_1,..., \alpha_k)$ over $Q(\beta_1)$, then $H, \subset K_1'$, 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, is the Galois group of the normal closure of $Q(\beta_{i-1})$ over $Q(\beta_i)$, then $f(x)$ is solvable by radicals iff G_i is solvable for $i = 1,..., r+1$. This is surprisingly 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* $c = 3.243999....$

This result is sufficient for us to obtain a polynomial time algorithm for checking solvability by radicals. Let $f(x) \in Z[x]$ be monic and irreducible, with roots $\alpha_1,..., a_{,,,}$. We have shown how to compute field extensions $Q(\beta_i)$, $i = 1,..., r+1$, such that $Q(\beta_{r+1}) =$ Q, and $Q(\beta_0) = Q(\alpha)$, and for $j = 1,..., r+1$, the Galois group of the normal closure of $Q(\beta_{j-1})$ over $Q(\beta_j)$ acts primitively on the conjugates of β_i over

$Q(\beta_{j-1})$ [Algorithm 3.11. 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 straightforward generalization of Corollary 6 [9], and we do not repeat a proof of correctness 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 G, where $K[y]/g(y)$ is the splitting field for $f(x)$ over* K, *and G is the Galois group of $f(x)$ over* K *(given as a Cayley table). It does so in $O((|G|\, l)^{9+\varepsilon}(|G| \log |G|[f(x)] + l^3 \log[\theta])^{2+\varepsilon})$ steps.*

We know that primitive solvable groups are small. 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, $i = 1,..., r+1$, 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 $n_{i-1}^{3.25}$. 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 one of the standard algorithms for testing solvability of a group [17, 6]. 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 Cayley table for G, 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 **FIELDS**$(f(x))$

Step 2. For $i = 1,..., r+1$, *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**(G)
If **SOLVABLEGP**(G) = "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*** $off(x)$ ***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 a definition.

Let K be an algebraic number field which contains the nth roots of unity. Then $K(\sqrt[n]{a})$ is a Galois extension of K, and the map $\sqrt[n]{a} \mapsto \zeta_m \sqrt[n]{a}$, where ζ_m is a primitive nth root of unity, generates the Galois group of $K(\sqrt[n]{a})$ over K, which is cyclic of order n. If $K(\alpha)$ is a Galois extension of K with cyclic Galois group, we say $K(\alpha)$ is a ***cyclic extension of K.*** If $K(\alpha)$ is cyclic of order n, we claim that $K(\alpha) = K(\sqrt[n]{a})$ for some a in K. Let σ be a generator of the Galois group of $K(\alpha)$ over K, and let ζ be a primitive nth root of unity. For each element y in $K(\alpha)$ we can form the ***Lagrange resolvent:***

$$(\zeta, \gamma) = \gamma + \zeta\sigma(\gamma) + \zeta^2\sigma^2(\gamma) \cdots + \zeta^{n-1}\sigma^{n-1}(\gamma).$$

The Lagrange resolvent is a K-linear map form $K(\alpha)$ onto itself, and can be thought of as a matrix. Then $(\zeta, y) = 0$ iff γ is in the nul space of this matrix. Then we need

THEOREM **4.1** [Artin]. ***The elements of the Galois group of*** $K(\alpha)$ ***over K are linearly independent over K.***

Now let $y \in K(\alpha)$ be such that $(\zeta, y) \neq 0$, and consider

$$\begin{aligned}\sigma(\zeta, \gamma) &= \sigma(\gamma) + \zeta\sigma^2(\gamma) + \cdots + \zeta^{n-1}(\gamma) \\ &= \zeta^{-1}(\zeta\sigma(\gamma) + \zeta^2\sigma^2(\gamma) + \cdots + \gamma) \\ &= \zeta^{-1}(\zeta, \gamma). \qquad (2)\end{aligned}$$

This means that $(\zeta, \gamma)^n$ is fixed by σ, and thus that $(\zeta, \gamma)^n$ is in K. But we also know from (2) that $\sigma^k(\zeta, \gamma) = \zeta^{-k}(\zeta, \gamma)$, which means that the only element of the Galois group which fixes (ζ, γ) is the identity. If we let $a = (\zeta, \gamma)^n$, we conclude that $K(\alpha) = K(\sqrt[n]{a})$. We have shown

THEOREM 4.2. *Every cyclic field of nth degree over an algebraic number field can be generated by an adjunction of an nth root provided that the nth roots of unity lie in the base field.*

The method we use to express a as radicals over Q relies on the effective proof of Theorem **4.2,** which appears in [20]. Roots of unity play a special role in the question of expressibility; it is well known that

LEMMA 4.3. *The* pth *roots of unity, p a prime, are expressible as "irreducible radicals" over K.*

As always $f(x)$ is an irreducible solvable polynomial of degree m over the rationals, and we let a be a root of $f(x)$. In Section **3** we presented an algorithm which found a tower of fields $Q(\beta_i)$, $i = 1, \ldots, r+1$, where $Q = Q(\beta_{r+1}) \subset Q(\beta_r) \subset \cdots \subset Q(\beta_1) \subset Q(\alpha)$, 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 $Q(\gamma_i)$, $i = 1, \ldots, r+1$, where $Q(\gamma_i)$ is the splitting field for $Q(\beta_i)$ over $Q(\beta_{i+1})$. In light of Theorem **4.2,** we first adjoin to Q the lth roots of unity, where $l = [Q(\gamma_r): Q]$. We claim that there is a straight line program which expresses ζ_l, a primitive lth 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 will instead begin by showing a bound for the β_i's.

Actually we find elements $\tilde{\beta}_i$ such that $Q(\tilde{\beta}_i) = Q(\zeta_l, \beta_i)$. *To* write straight line code to express a as radicals over $\tilde{Q}$, it suffices to present straight line code for expressing $\tilde{\beta}_i$ as radicals over $Q(\tilde{\beta}_{i+1})$. Since there are at most $\log m$ fields between $\tilde{Q}$ and $\tilde{Q}(\alpha)$, 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. (The bounds we present are not best possible, but are simplified for the sake of readability.)

LEMMA 4.4. *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 $[\tilde{g}_i(x)] \leq O(|f(x)|^{m^{12}})$.*

Proof. Because the Galois group of $f(x)$ is solvable, each extension $[Q(\gamma_i): Q(\beta_{i+1})] \leq m_i^{3.25}$, where $[Q(\beta_i): Q(\beta_{i+1})] = m_i$. Since $[Q(\alpha): Q] = \prod m_i = m$, we have $l = [Q(\gamma_r): Q] \leq m^{3.25}$. Now $Q(\beta_{i+1}) = Q[x]/h_{i+1}(x)$ implies that $Q(\tilde{\beta}_{i+1}) = Q[x, y]/(h_{i+1}(x), z(y))$, where $z(y)$ is an irreducible factor of the cyclotomic polynomial $x^l + x^{l-1} + \cdots + 1$ over $Q[x]/h_{i+1}(x)$. By Theorem **1.2** $[z(y)] \leq m_i! \, |h_{i+1}(x)|^{m_i^2}$.

The roots of $h_{i+1}(x)$ are symmetric functions in a block of roots of $f(x)$, which means that $|h_{i+1}(x)| \leqslant |f(x)|^m$. Thus $[z(y)] \leqslant m_i! \, |f(x)|^{mm_i^2}$. We can now use a linear combination of y and x to obtain a primitive element $\tilde{\beta}_{i+1}$ over Q. If $\tilde{h}_{i+1}(x)$ is the minimal polynomial for $\tilde{\beta}_{i+1}$ over Q, then

$$\begin{aligned} |\tilde{h}_{i+1}(x)| &\leqslant (m_i l m_i! \, |f(x)|^{mm_i^2} |f(x)|^m)^{m_i l} \\ &< (m_i!)^2 \, |f(x)|^{m^6}. \end{aligned}$$

Now $\tilde{g}_i(y)$ will be factor of $g_i(y)$, the polynomial described in Algorithm 3.2. Since $g_i(y)$ is an irreducible factor of $h_i(y)$, we have

$$\begin{aligned} [g_i(y)] &\leqslant m! \, [\tilde{h}_i(y)]^m \, |\tilde{h}_{i+1}(x)|^{m^2} \\ &\leqslant m! \, |f(x)|^{m^7} \, (|f(x)|^{m^6})^{m^2} \\ &< m! \, |f(x)|^{m^9}. \end{aligned}$$

This implies that

$$\begin{aligned} [\tilde{g}_{i+1}(y)] &\leqslant m! \, (|f(x)|^{m9})^{m^2} \, |h_{i+1}(x)|^{m^2} \\ &\leqslant m! \, |f(x)|^{m^{11}} \, |f(x)|^{m^8} \\ &< m! \, |f(x)|^{12}. \end{aligned}$$

(We remind the reader that the bounds are not best possible.) ∎

LEMMA 4.5. *If $\tilde{k}_i(x)$ is the minimal polynomial for γ_i over $Q(\tilde{\beta}_{i+1})$, then* $[\tilde{k}_i(x)] \leqslant O(|f(x)|^{m^9})$.

Proof. If $k_i(x)$ is the minimal polynomial for γ_i over $Q(\beta_{i+1})$, then the roots of $k_i(x)$ are the conjugates of

$$\beta_i + c_2\theta_2 + \cdots + c_t\theta_t$$

over $Q(\beta_{i+1})$, whre $\theta_2, \ldots, \theta_t$ are the conjugates of β_i over $Q(\beta_{i+1})$, and the c_i's are integers less than m^3. Then by Theorem 1.2,

$$\begin{aligned} [k_i(x)] &\leqslant (m^7 \, |f(x)|^{m^6})^m \, |f(x)|^{m^5} \\ &< m^{7m} \, |f(x)|^{m^7}. \end{aligned}$$

Since $\tilde{k}_i(x)$ is an irreducible factor of $k_i(x)$ over $Q(\beta_{i+1})$, we obtain

$$\begin{aligned} [\tilde{k}_i(x)] &\leqslant m! \, [k_i(x)]^m \, |h_{i+1} \, d(x)|^{m^2} \\ &\leqslant m! \, |f(x)|^{m^2} \, (|f(x)|^{m^2})^{m^2} \\ &< m! \, |f(x)|^{m^9}. \quad \blacksquare \end{aligned}$$

In order to write straight line code to express a 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 $\log|f(x)|$, then the former can also be solved in polynomial time, since there are at most logm fields between $\tilde{Q}$ and $\tilde{Q}(\alpha)$.

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 $(e\} = H_0 \subset H_1 \subset \cdots \subset H_s$, where H_k is normal in H_{k+1}, and H_{k+1}/H_k is of prime order [17, 6]. 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 $Q(\gamma_i)$ corresponding to H_k. Since we can compute the H_k's in polynomial time, we can also compute polynomial $j_k(x)$ in polynomial time. We can also find a primitive element θ_k for the field $Q(\tilde{\beta}_{i+1})[x]/j_k(x)$ in polynomial time. We do this in the usual way. If $j_k(x) = x^l + b_{l-1}x^{l-1} + \ldots + b_0$, the b_i's are symmetric functions in conjugates of $\tilde{\gamma}_i$, and $[b_j] \leqslant [\tilde{\gamma}_i]^{m^3} < (|f(x)|^{m^7})^{m^3} = |f(x)|^{m^{10}}$. We let $\theta_k = b_0 + c_1 b_1 + \cdots + c_{l-1} b_{l-1}$, picking the c_i from Z so as to ensure that θ_k is primitive. Then $[\theta_k] < (m^7 |f(x)|^{m^{10}})$, and if $\tilde{j}_k(x)$ is the minimal polynomial for θ_k over Q,

$$\begin{aligned}[\tilde{j}_k] &\leqslant (m^7 |f(x)|^{m^{10}})^{m^3} \\ &< m^{7m^3} |f(x)|^{m^{14}}.\end{aligned}$$

If we let $i_k(x)$ be the minimal polynomial for $\tilde{\theta}_k$ over $Q(\theta_{k-1})$, then since $i_k(x)$ is a factor of $j_k(x)$, we have

$$\begin{aligned}[i_k(x)] &\leqslant (m^3)([\tilde{j}_k(x)])^{m^{3.25}} ([\tilde{j}_k(x)])^{m^{6.5}} \\ &< m^3 |f(x)|^{m^{21}}.\end{aligned}$$

We conclude

LEMMA 4.6. *Let* $\tilde{j}_k(x)$ *be the* minimal polynomial *for* θ_k *over* Q. *Then* $|\tilde{j}_k(x)| \leqslant O(|f(x)|^{m^{14}})$. *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.

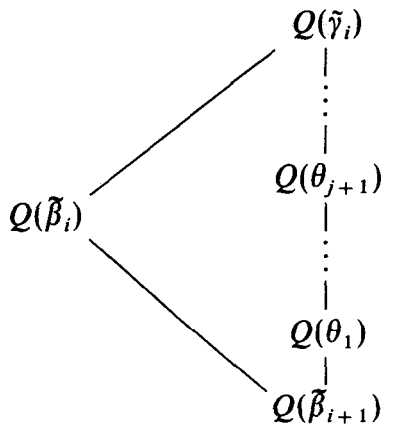

FIG. 4.1. The cyclic extensions between $Q(\tilde{\beta}_{i+1})$ and $Q(\tilde{\gamma}_i)$.

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 $p_j(x)\in Q[x]$. To do this it is also necessary to construct $q_j(x,y)\in Q[x,y]$, $j=0,\ldots,$ s, where $\theta_{j+1}=q_j(\sqrt[d_j]{p_j(\theta_j)},0,)$. Once we have shown how to construct $p_j(x)$ and $q_j(x,y)$ in size polynomial in m and $\log|f(x)|$, we will be done showing how to express α over $Q(\zeta_l)$ in a straight line program in polynomial time. Finally ζ_l will be expressed in a similar way.

We proceed with induction, beginning with η_1. Consider the Lagrange resolvent of $Q(\theta_1)$ over $Q(\tilde{\beta}_{i+1})$ m and let κ_1 be in $Q(\theta_1)$—*the null* space *of* $Q(\tilde{\beta}_{i+1})$. (Observe that κ_1 can be found in polynomial time.) If $\kappa_1=r_1(\theta_1)$ then

$$[r_1(x)]\leqslant((d_1[\theta_1])^{d_1})^{d_1^3}=(d_1[\theta_1])^{d_1^4}$$

[4]. Let $\eta_1=(\zeta,\kappa_1)^{d_1}$. By the proof of Theorem 5.2, $\eta_1\in Q(\beta_{i+1})=Q(\theta_0)$, and $Q(\theta_1)=Q(\theta_0,\sqrt[d_1]{\eta_1})$. Let $p_1(x)\in Q[x]$ be such that $p_1(\theta_0)=\eta_1$. We want to show that $p_1(x)$ has polynomial size coefficients.

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 (22, Theorem 1.2) that $p_1(x)$ has polynomial size coefficients. We repeat this with actual, though not best possible, bounds.

We chose $\eta_1=(\zeta,\kappa_1)^{d_1}$. This means that

$$\begin{aligned}[\eta_1]&=[(\zeta,\kappa_1)]^{d_1}\\&\leqslant(d_1[\kappa_1])^{d_1}\\&\leqslant(d_1^2[\theta_1]^{d_1^4})^{d_1}\\&<[\theta_1]^{d_1^6}.\end{aligned}$$

By Lemma **4.6,** $|\tilde{f}_0(x)|<|f(x)|^{14}$ and $[\theta_1]<|f(x)|^{m^{14}}$. By a rough approximation using Weinberger and Rothschild, we find

$$|p_1(x)|\leqslant|f(x)|^{m^{26}d_1^6}.$$

Next we determine and bound $q_1(x, y)$. Our argument is that the minimal polynomial for 8, over Q is of bounded size (Lemma **4.6**), and thus its factors over $Q(\theta_0)$ are also bounded. We find an integer c_1 such that $v_1 = \theta_0 + c_1 \sqrt[d_j]{\eta_1}$ is a primitive element for $Q(\theta_1)$ over Q. Then v_1 has a minimal polynomial over Q which is of bounded size. This means that the polynomial $t_1(x) \in Q[x]$ such that $\theta_1 = t_1(v_1)$ has polynomial size Coefficients. Furthermore the polynomial $q_1(x, y) \in Q[x, y]$ such that $8_1 = q_1(\sqrt[d_j]{\eta_1}, \theta_1) = t_1(y + c_1 x)$ also has polynomial size coefficients.

For the inductive step it remains to replace 0 by i, and 1 by $i + 1$, because all of our bounds are a priori established by Lemmas **4.4-4.6.** The crucial fact to observe is that each of the polynomials $p_i(x)$ and $q_i(x, y)$ are determined in sequence from the θ_i's, whose length of description is polynomially bounded.

One step remains. We must show that if $\tilde{\beta}_i = l_i(\tilde{\gamma}_i)$, with $l_i(x)$ a polynomial in $Q[x]$, then the coefficients of $l_i(x)$ are polynomial in size. This folows immediately since the minimal polynomials for $\tilde{\beta}_i$ and $\tilde{\gamma}_i$ over $Q(\tilde{\beta}_{i+1})$ are polynomial in size. We have shown

THEOREM 4.7. ***There exists a polynomial time straight line program to express a, a root of a solvable irreducible polynomial over Q, in terms of radicals.***

We have not yet shown how to express the Ith roots of unity as radicals over Q, but Lemma **4.3** is effective. We observe that in order to express the lth roots of unity as radicals over Q, we need to have the p_ith roots of unity expressed as radicals, where p_i is a prime divisor of $\varphi(l)$. Of course, this requires that q_jth 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 log1 steps. Therefore we conclude that ζ_l 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 a in polynomial time in the form

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

rather than what we have proposed here. However, for small examples, the field which contains ζ_l expressed in radicals in the usual way is of degree $l^{\log l}$ over Q. This indicates that Theorem 4.7 may be the best we can do.[1]

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 presented techniques to answer that question in polymonial time. We have transformed Galois'

[1] **The second author has shown that polynomial size representation of roots in radicals is possible given symbols ζ_i for roots of unity [14].**

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 our running times are based on the time needed by the algorithm [12] 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 irreducibe 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?

The real buried treasure would be a polynomial time algorithm for determining the Galois group, regardless of solvability. A polynomial of degree n may have a Galois group as large as S_n, but a set of generators will be polynomial in size. We see no immediate way that a divide-and-conquer approach might solve this problem, but we do observe that some characteristics of the Galois group may be inferred without 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 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 [13, 18, 23], 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 probem, but we hope for, and would be delighted by, its solution.

APPENDIX

This algorithm computes a minimal block of imprimitivity. It can be easily modified to compute a tower of blocks.

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 $N_{(Q[x]/f(x))/Q}(f(x) - cz))$ is squarefree and factor $N_{(Q[x]/f(x))/Q}(f(x - cz))$ over Q,
$N_{(Q[x]/f(x))/Q}(f(x - cz)) = \prod_{i=1}^{l} G_i(x - cz)$
[At most n^3 c's in Z do not satisfy this condition.]

Step 2. For $i = 1 \cdots l$ 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 $Q[z]/f(z)$.]

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 $N_{(Q[x]/f(x))/Q}(f(x - cz))$ 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 $i = 1 \cdots l$, 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 factorization over $Q[t]/G_j(t)$.]

Step 7. Compute the graph $\Gamma_j = (V_j, E_j)$, 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 2.2. INTERSECTION.

input: $f(x) \in Z[x]$ and $h(x) \in Q[z]/f(z)$, where $f(x)$ is monic and irreducible over Q, and $h(x) \in Q[z]/f(z)$ is an irreducible factor of $g(x)$, which is a monic irreducible polynomial over Z

Step 1. Find $c \neq 0$ such that $N_x(h(x-cz))$ is squarefree and factor:
$H(x) = N_z(h(x-cz)) = \prod_{i=1}^{k} j_i^z(x)$ over $Q[z]/f(z)$,
[At most $(mn)^2$ c's in Z do not satisfy this condition, where $m =$ degree $(f(x))$ and $n =$ degree $(h(x))$.]

Step 2. Factor $H(x) = \prod_{i=1}^{l} k_i^w(x)$ over $Q[w]/g(w)$

Step 3. $q(t) \leftarrow$ constant term of $\gcd(f(x), g(t-cx))$ over $Q[t, x]/H(t)$
$p(t) \leftarrow (t - cq(t))$
[This computes z and w in terms of a primitive element for the field $Q[z, w]/(f(z), h(w))$ which is isomorphic to $Q[t]/H(t)$.]

Step 4. For $i = 1, \ldots, l$, do:
$j_i^z(x) \leftarrow j_i^{q(t)}(x)$

Step 5. For $j = 1, \ldots, l$, do:
$k_j^w(x) \leftarrow k_j^{p(t)}(x)$
[This rewrites the factorizations of $H(x)$ over $Q[z]/f(z)$ and $Q[w]/g(w)$ as factorization over $Q[t]/H(t)$.]

Step 6. Compute $\Gamma = \langle V, E_j \rangle$, a graph with vertices V, and edges E_j given by:
$V = \{j_i^z(x)\} \cup \{k_j^w(x)\}$
$E = \{\langle j_i^z(x), k_i^w(x) \rangle \mid \gcd(j_i^z(x), h_i^W(x)) \neq 1\}$

Step 7. Compute $Y = \{i \mid j_i^z(x)$ is connected to $j_1^z(x) = h(x)$ in $\Gamma\}$

Step 8. $B(x) \leftarrow \prod_{i \in Y} j_i^z(x)$

return: $B(x) \in Q[x, z]/(f(z))$, a polynomial whose coefficients determine the field $Q[x]/f(x) \cap Q[x]/g(x)$

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**$(f(z))$
$g_0(t) \leftarrow t^l + c_{l-1}(z)\, t^{l-1} + \cdots + c_0(z) \leftarrow C^z(t)$
[$C^z(t)$ 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. $t^k + a_{k-1}(z)\, t^{k-1} + \cdots + a_0(z) \leftarrow C^z(t)$

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

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

Step 6. $l \leftarrow 1$

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

Step 8. Else if $\beta^l(z) + d_{l-1}\beta^{l-1}(z) + \cdots + d_0 = 0$,
$h_i(x) \leftarrow x^l + d_{l-1}x^{l-1} + \cdots + d_0$
[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 $j = 0,..., l-1$, do:
Find $p_j(x)$ such that $p_j(\beta(z)) = c_j(z)$

Step **10.** $g_{i-1}(y) \leftarrow y^l + p_{l-1}(x)\, y^{l-1} + \cdots + p_0(x)$
[Then $Q[t]/h_{i-1}(t) \simeq Q[x, y]/(h_i(x), g_{i-1}(y))$.]

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

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

Step **13.** $B^x(t) \leftarrow \text{BLOCKS}(h_i(x))$;
$t^l + b_{l-1}(x)\, t^{l-1} + \cdots + b_0(x) \leftarrow B^x(t)$

Step **14.** For $j = 0,..., l-1$, do:
$c_j(z) \leftarrow b_j(\beta(z))$
[This will allow us to express $B^x(t)$ as a polynomial with coefficients which are polynomials in z and which has root x.]

Step **15.** $B^z(x) \leftarrow x^l + c_{l-1}(z)\, x^{l-1} + \cdots + c_0(z)$

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

Step **17.** $i \leftarrow i + 1$

return: $\{h_i(x), g_{i-1}(y) \mid i = 1,..., r\}$, 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 $i = 1,..., r$
(3) The Galois group of $g_{i-1}(y)$ over $Q[x]/h_i(x)$ 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 $h_r(x)$.

THEOREM 3.3. *Let $f(z) \in Z(z)$ of degree m be irreducible. Algorithm* **3.1** *computes $\{h_i, g_{i-1} \mid i = 1,..., r\}$ 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* $(g(x)) \leqslant m$, *and the coefficients of* $g(x)$ *are less than* $m^2 \log(m!\,[f(x)])$.

Proof. We consider the first iteration of Algorithm 3.1. Step 1 computes $C^z(t) = t^l + c_{l-1}(z)\, t^{l-1} + \cdots + c_0(z)$, whose roots $z_1, \ldots, z_k$ form a minimal block of imprimitivity containing $z = z_1$. If $C^z(t)$ is in $Q[t]$, then the Galois group of $f(x)$ over Q acts imprimitively on the set of roots of $f(z)$, and we are done. Otherwise we compute a primitive element $\beta(z)$ for the field $Q[a_{k-1}, \ldots, a_0]/f(z)$ (where the a_i are just renamed c_i) in Steps 4 and 5. That Step 4 and 5 are correct is immediate from van der Waerden [20, p. 139]. In Steps 6–8, we compute the minimal polynomial $h_1(x)$ for $\beta(z)$ over Q.

Now that we have a primitive element, x, for $Q[a_{k-1}(z), \ldots, a_0(z)]/f(z)$ we can rewrite $C^z(t)$ as $C^x(t)$, a polynomial over $Q[x]/h_1(x)$. This is done in Steps 9 and 10. Note that this means that $Q[t]/h_0(t) \simeq Q[x, y]/(h_1(x), g_0(y))$. Steps 11 and 12, in the case $i = 1$ are redundant. Observe that $C^x(t)$ has the same value before and after these two steps.

Next we call **BLOCKS** on $h_1(x)$. Let **BLOCKS** $(h_1(x)) = t^k + b_{k-1}(x)\, t^{k-1} + \cdots + b_0(x) = B^x(t)$. By the minimality of the block, the Galois group of $h_1(x)$ over $Q[b_{k-1}(x), \ldots, b_0(x)]/h_1(x)$ acts primitively on the roots of $h_1(x)$. We know that $Q[b_{k-1}(x), \ldots, b_0(x)]/h_1(x) = Q((\textit{elementary})\ \textit{symmetric functions in}\ z_1, \ldots, z_l)$ for some block $z_1, \ldots, z_l$. We find this block.

Let x be a root of $h_1(t)$. Then x is a root of $B^x(t)$. If we rewrite $B^x(t)$ as $B^z(t)$, a polynomial with coefficients in $Q[z]/f(z)$, x remains a root. Recall Lemma 3.2, and the discussion which followed it. Since x is a root of $B^x(t)$, the roots of

$$N_{(Q[x]/h_1(x))/(Q[b_{k-1}(x), \ldots, b_0(x)]/h_1(x))}(B^x(t)) = N_{Q(\rho_1)/Q(\rho_2)} B^{\rho_1}(t) = C^z(t)$$

are a block containing B_1. Because the Galois group of $h_1(x)$ over $Q[b_{k-1}(x), \ldots, b_0(x)]/h_1(x)$ acts primitively on the set of roots of $h_1(x)$, the roots of $C^z(t)$ are a minimal block containing B_1. We can calculate this norm by a resultant. In order to do so, we express $B^x(t)$ as a polynomial with coefficients in $Q[z, t]/(f(z), B^z(t))$. This is done in Steps 14 and 15. Since x is a root of $B^z(t)$, Step 16 computes $C^z(t)$ correctly.

Inductively suppose that Algorithm 4.1 has computed $\{h_i(x), g_{i-1}(y) \mid = 1, \ldots, k\}$ 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 $i = 1, \ldots, k$, and

(3) the Galois group of $g_{i-1}(y)$ over $Q[x]|h_i(x)$ acts primitively on the set of roots of $g_{i-1}(y)$,

and that $C^z(t)$ is a polynomial whose roots are the elements of the block B_{k+1}. We wil show that a single iteration of Algorithm 4.1 will produce $h_{k+1}(x)$ and $g_k(y)$, and a new $C^z(t)$ which satisfy the above conditions.

If $C^z(t) \in Q[t]$, we are done, since then the roots of $C^z(t)$ are $z_1, \ldots, z_r$ and we have satisfied conditions **(1)–(4)** of the theorem. Suppose $C^z(t) \notin Q[t]$. Then in Steps **3–5** we compute a primitive element $\beta(z)$ for Q((elementary) symmetric functions in the elements of B_{k+1}). In Steps **6** and 7 we determine $h_{k+1}(x)$, the minimal polynomial for $\beta(z)$ over Q.

Next we calculate $g_k(y)$. Since the Galois group of $B^z(x)$ over $Q[\beta(z)]/f(z)$ acts primitively on the set of roots of $B^z(x)$, $B^Z(t)$ is—almost—the $g_k(t)$ we want. The only difficulty is that $B^z(t)$ is written as a polynomial with coefficients in $Q[z]/f(z)$. This however, is easily circumvented, since $B^z(t)$ has coefficients which are in $Q[x]/h_{k+1}(x)$. We express them in terms of x in Step 9, and we write out $g_k(y)$ in Step **10.**

Now we are ready to find the next block. We seek to express $C^z(t)$ as a polynomial over $Q[x]/h_{k+1}(x)$; we proceed in the same manner as we did for $g_k(y)$. We do so in Steps **11–12.** Then B_{k+1} will consist of the roots of the norm of $C^z(t)$ over a subfield of $Q[x]/h_{k+1}(x)$, namely a minimal subfield. We compute this subfied by calling **BLOCKS** on $h_{k+1}(x)$; the subfield is determined by the elementary symmetric function of the elements of a minimal block of roots of $h_{k+1}(x)$, or more simply, by the coefficients of the polynomial returned by **BLOCKS** $(h_{k+1}(x))$ in Step **13.** In Steps **14** and **15** we rewrite the polynomial $B^x(t)$ as a polynomial in the variable t with coefficients in $Q[z]/f(z)$. Then by Lemma **3.2,** the polynomial we are seeking is:

$$
\begin{aligned}
&N_{(Q[x]/h_{k+1}(x))/(Q[b_{k+1}(x),\ldots,b_0(x)]/h_{k+1}(x))} C^x(t) \\
&\quad = N_{(Q[\beta(z)]/f(z))/(Q[b_{k+1}(x),\ldots,b_0(x)]/h_{k+1}(x))} C^x(t) \\
&\quad = \mathrm{Res}_x(B^z(x), C^x(t)) \\
&\quad = C^z(t).
\end{aligned}
$$

We are done. Let us now examine running time.

Observe that Algorithm **3.1** is looped through at most $\log m$ times, since each iteration produces a subfield between Q and $Q(\alpha)$. Let us consider the running time necessary for the first iteration.

The time needed for Step 1 is dominated by the call of **BLOCKS** on $f(z)$. Steps 2-4 take constant time. The loop of Step **5** is passed through a maximum of m times, with no more than $\log m$ nontrivial executions. The computations $a_j(z) \in ? \{1, \beta(z), \ldots, \beta^{m-1}(z)\}$ is done at most m^3 times for each $a_j(z)$, with each test requiring no more than $O(m^5)$ steps. (This is simply a linear algebra problem of testing independence; the bound is due to Edmonds **[4].)** Step 5 requires much less time than **BLOCKS** of Step 1.

The running time for Steps **6–12** is less than the time required for Step **5,** and is therefore dominated by Step 1. In Step **13,** we call **BLOCKS** on $h_1(x)$, **a** factor of $f(x)$. The time required for Steps **1–16** is dominated by the time required for Step 5. Thus the time required for the first iteration is dominated by **BLOCKS**$(h(x))$, where $h(x)$ **is** a factor of $f(x)$.

Subsequent iterations are dominated by this factor, and there are at most $\log m$ of them. Hence we conclude that the running time for FIELDS is less than $O(\log m \text{ BLOCKS}(g(x)))$, where $\text{degree}(g(x)) \leqslant m$, and $[g(x)] \leqslant [f(x)]^{m^2}$. ∎

ACKNOWLEDGMENTS

Warm thanks to Eric Lander, who originally proposed the approach of primitive groups. Thanks to Mike Artin, Barry Trager, and Rich Zippel, who carefully read an earlier draft and suggested improvements.

REFERENCES

1. E. ARTIN, "Galois Theory," Univ. of Notre Dame Press, Notre Dame, Ind., 1971.
2. M. ATKINSON. An algorithm for finding the blocks of a permutation group, *Math. Comp.* July (1975), 911–13.
3. P. J. CAMERON, Finite permutation groups and finite simple groups, *Bull.* London *Math. Soc.* 13 (1981), 1–22.
4. J. EDMONDS, Systems of distinct representations and linear algebra, *J. Nat.* Bur. *Stand. Ser. B,* 71, No. 4, (1967), 241–245.
5. H. EDWARDS, "Galois Theory," Springer-Verlag, New York, 1984.
6. M. FURST, J. HOPCROFT, AND E. LUKS, Polynomial time algorithms for permutation groups, *in* "Proc. Twenty-first Annu. IEEE Sympos. Found. Comput. Sci. 1980", pp. 36-41.
7. E. GALOIS, "Oeuvres Mathkmatiques," Gauthier-Villars, Paris, 1897.
8. J. L. LAGRANGE, "Rkflexions sur la Rksolution Algebraïque des Équations," Prussian Academy, 1770.
9. S. LANDAU, Factoring polynomials over algebraic number fields, *SIAM J. Cornput.* 14, No. 1, (1985), 184–195.
10. S. LANDAU, "On Computing Galois Groups, and its Application to Solvability by Radicals," Tech. Report TR-288, Laboratory for Computer Science, M.I.T.
11. S. LANG, "Algebra," Addison–Wesley, Reading, Mass., 1971.
12. A. K. LENSTRA, H. W. LENSTRA, AND L. LOVÁSZ, "Factoring Polynomials with Rational Coefficients," *Mathematische Annelan* 261 (1982), 513–534.
13. J. MCKAY, Some remarks on computing Galois groups, SIAM J. *Cornput.* 8, No. 3, (1979), 344–347.
14. G. MILLER, Constructing field extensions without using primitive elements, in preparation.
15. O. NEUGEBAUR AND A. SACHS, "Mathematical Cuneiform Texts," Amer. Orient. Soc., New Haven, Conn., 1945.
16. P. PÁLFY, A polynomial bound for the orders of primitive solvable groups, J. Algebra, July (1982), 127–137.
17. C. SIMS, Computational methods in the study of permutation groups, *in* "Computational Problems in Abstract Algebra," Pergamon, Elmsford, N.Y., 1970
18. R. P. STADUHAR, The determination of Galois groups, *Math. Comp. 27* (1973), 981–996.
19. B. TRAGER, Algebraic factoring and rational function integration, in "Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation," pp. 219–226.
20. B. L. VAN DER WAERDEN, "Modern Algebra," Ungar, New York, 1941.
21. H. WIELANDT, „Finite Permutation Groups," Academic Press, New York, 1964.
22. P. WEINBERGER AND L. ROTHSCHILD, Factoring polynomials over algebraic number fields, J. *Assoc. Comput. Mach.,* Dec. (1976), 335–350.
23. H. ZASSENHAUS, On the group of an equation *in* "Computers in Algebra and Number Theory: Proceedings" (G. Birkhoff and M. Hall, Eds.), Amer Math. Soc., Providence, R.I., pp. 69-88, 1971.

Printed by the St. Catherine Press Ltd., Tempelhof 41, Bruges, Belgium