ON COMPUTING GALOIS GROUPS AND ITS APPLICATION TO SOLVABILITY BY RADICALS

by

SUSAN EVA LANDAU

B.A., Princeton University
(1976)

M.S., Cornell University
(1979)

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

January, 1983

Signature of Author Susan Eva Landau
Department of Mathematics
January 7, 1983

Certified by Gary Lee Miller
Gary L. Miller
Thesis Supervisor

Certified by _____
Harvey Greenspan
Chairman, Applied Mathematics Department

Accepted by _____
Nesmith Ankeny
Chairman, Departmental Graduate Committee

Dedicated to the memory of Y.P.,

whose love of laughter and sharing is what makes research worthwhile

ON COMPUTING GALOIS GROUPS AND ITS APPLICATION TO SOLVABILITY BY RADICALS

by

SUSAN EVA LANDAU

Submitted to the department of Mathematics
on January 7, 1983 in partial fulfillment of the
requirements for the Degree of Doctor of Philosophy

ABSTRACT

This thesis presents a polynomial time algorithm for the basic question of Galois theory, checking solvability by radicals of a monic irreducible polynomial over the integers. It also presents polynomial time algorithms for factoring polynomials over algebraic number fields, for computing blocks of imprimitivity of roots of a polynomial under the transitive action of the Galois group on the roots of the polynomial, and for computing intersections of algebraic number fields. (In all of these algorithms it is assumed that the algebraic number field is given by a primitive element which generates it over the rationals, and that the polynomial in question is monic, with coefficients in the integers.) We also show how to express a root in radicals in terms of a straightline program in polynomial time.

The techniques used include methods from computational complexity and approaches from the theory of finite permutation groups. The results presented here rely on the recent work of Lenstra, Lenstra, and Lovász, in which a polynomial time algorithm for factoring polynomials over the integers is presented.

Many questions remain. Our divide-and-conquer approach answers the question of solvability without revealing the nature of the group in question; we do not even learn its order. We suggest this as one of the many open problems that remain to be tackled.

Thesis Supervisor: Dr. Gary L. Miller

Title: Associate Professor of Applied Mathematics

Acknowledgements

This thesis would not have been written without John Hopcroft. He urged me not to leave Cornell, and convinced me to take generals when I did choose to leave; he continued to encourage me after I had left, and when the opportunity came for me to attend M.I.T., I knew I had his support. That support has been of more help to me than he is aware.

Gary Miller, my advisor, has always been a source of enthusiasm and energy. He gave most generously of his time, and his curiousity and questions provoked many of the results presented here. A large number of the ideas in this thesis evolved during our conversations together. I owe him a most hearty thanks.

Warm thanks to my two readers:

Rich Zippel, whose course inspired the first result of this thesis, and who has tirelessly answered my frequent questions, and

Michael Artin, for his generosity in chocolate bars, ideas and time, and his willingness to learn a new vocabulary – the language of complexity – in talking with me.

It was never easy, and I count myself most fortunate in the love of my good friends. I would like to take this chance to thank Eric Lander for the sharing of his wisdom, mathematical and otherwise, and also to thank Larry Carter, Steve Mahaney, Patricia Sipe and Joan Hutchinsion for their strong and continued support. Sandeep Bhatt carefully read a draft of this thesis, and his gentle criticisms greatly improved it. My sister ran a one-woman cheering squad over the years and the laughter she raised was a good tonic.

Finally I owe much to Neil, who generously gave of his dreams so that I might pursue mine.

Table of Contents

Introduction 7

Chapter I: Background

1. Factoring Polynomials over the Integers 10
2. Sizes of Coefficients 12
3. The Norm 16
4. Computing Greatest Common Divisors 20

Chapter II: Factoring Polynomials over Algebraic Number Fields

1. An Algorithm 22
2. Primitive Elements 26
3. Corollaries 27
4. A Brief Introduction to Galois Theory 28

Chapter III: Finding Blocks of Imprimitivity

1. Background 32
2. An Algorithm 37
3. A Corollary 40

Chapter IV: Determing Solvability

1. The Fields Between Q and $Q(\alpha)$ 43
2. An Algorithm 49
3. The Fields Between Q and $Q(\alpha)$ and Solvability 53
4. Another Algorithm 55
5. How It Fits Together 59

Chapter V: Expressibility

1. Background 61

2. Bounds 63

3. A Straight Line Program 66

Questions, Conclusions, and More Questions 70

Appendix 72

References 74

Biographical Note 76

Introduction

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 – Zassenhaus, van der Waerden – 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. That is the main result of this thesis.

Galois transformed the question of sovability 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 show that there is a polynomial time algorithm for factoring polynomials over algebraic number fields. We do this 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 $Q = Q(\rho_0) \subseteq Q(\rho_1) \subseteq \cdots \subseteq Q(\rho_r) \subseteq Q(\rho_{r+1}) = Q[x]/f(x)$. The tower of fields we find is 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 start with a brief introduction to background algebraic number theory in Chapter I. This sets the stage for the algorithm for factoring polynomials over algebraic number fields presented in Chapter II.

Chapter III begins the discussion on 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 Chapter IV to succintly 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 surprisingly easy to answer, giving us a polynomial time algorithm for the question of solvability by radicals.

We discuss in Chapter V 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. The thesis concludes with a disscusion of open questions.

A note to the reader: This thesis is self contained, but we do assume some knowledge of algebra. Background and proofs of classical results may be found in Samuel [Sa], van der Waerden [vdW] or Wielandt [Wie]. In particular the results of Chapter I, §2, Chapter II, §4 and Chaper III §3 are more fully presented in Samuel, Chapter II, van der Waerden , Chapter VIII, and Wielandt, Chapter I respectively.

Chapter I

Background

1. Factoring Polynomials over the Integers

Mathematicians have long sought efficient algorithms for factoring polynomials over the rationals. In 1793 Frederick von Schubert showed that the problem of factoring over the integers was decidable [Kn]. If $f(x)$ is the polynomial one desires to factor, Von Schubert's idea was to compute $f(1), f(2), \ldots, f(n)$ where n is the degree of $f(x)$. Consider a possible sequence $d(1), \ldots, d(n)$ where $d(i)$ divides $f(i)$. A sequence defines a potential divisor of $f(x)$, which can be found by interpolation. All divisors of $f(x)$ can be found in this way – if one has enough time. The algorithm is highly exponential.

A polynomial is primitive if the greatest common divisor of its coefficients is 1. Gauss proved that if a primitive polynomial $f(x) \in Z[x]$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients. Thus to decompose a polynomial $f(x) \in Q[x]$ into irreducible factors is equivalent to factoring a primitive polynomial in $Z[x]$ into irreducible factors in $Z[x]$. For the remainder of this thesis we will concern ourselves with monic polynomials with integer coefficients.

If one raises questions of efficiency, one must begin by asking how much space is required

to write down the factors of $f(x) = x^n + a_{n-1}x^{n-1} \ldots + a_0$. The answer is: not very much. We present a simple bound here, a tighter result may be found in [Mi.]

Suppose $\alpha \neq 0$ is a root of $f(x)$. Then $|\alpha| \leq 1 + \max_i |a_i|$ [Ma]. We let $[\![\alpha]\!] = \max_i |\alpha_i|$, where the α_i's are the conjugates of α over Q. If $g(x)$ is a divisor of $f(x)$, the roots of $g(x)$ are a subset of the roots of $f(x)$, and $g(x) = \prod_{\substack{\alpha_j, \text{ a root} \\ \text{of } g(x)}} (x - \alpha_j)$. If $g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$, the b_i's are integers, then

$$b_i = \sum_{\substack{\alpha_{j_k}, \text{ a root} \\ \text{of } g(x)}} \alpha_{j_1} \ldots \alpha_{j_{n-i}}$$

Thus $|b_i| < 2^n [\![\alpha]\!]^i < (2[\![\alpha]\!])^n$, which means that each b_i can be expressed in $n(\log [\![\alpha]\!])$ digits. There are at most n factors of $f(x)$, and each factor has at most n non-zero coefficients; consequently the complete factorization of $f(x)$ requires no more than $n^3 \log(1 + \max_i |a_i|)$ space. The factorization of $f(x)$ has polynomial size length. A non-deterministic machine could guess the factorization and verify it by multiplying the factors together to obtain $f(x)$. It is clear that the verification can be done in polynomial time.

Algorithms which were developed for factoring polynomials over the integers had exponential running time. An important one which worked well on average was created by Zassenhaus in 1969 [Za]. His idea was to factor $f(x)$ mod p, for a carefully chosen prime p, and then to lift the factorization to p^k for a large integer k. (In 1969, Berlekamp [Be] discovered an algorithm which factored a polynomial of degree n over Z/pZ in $O(n^3 p)$ steps.) The factorization mod p^k is examined to give a factorization over the integers. This may be hard as the following example illustrates.

The polynomial whose roots are $\pm\sqrt{2} \pm \sqrt{3} \pm \sqrt{5} \pm \ldots \pm \sqrt{p_n}$, p_n a prime, factors into linear or quadratic factors mod m for every integer m [Be2,p.733.] If we consider a reducible polynomial $f(x)$ with roots in the above form, then factoring mod m gives no information on how to combine the linear and quadratic terms to yield a factorization of $f(x)$ over the integers.

Zassenhaus's algorithm has the problem that its worst case running time is exponential in the degree. For a time, it seemed it might be easier to check polynomial irreducibility than to factor. In 1979 Weinberger [Wei] showed that under the Generalized Riemann Hypothesis, testing irreducibility of polynomials is in polynomial time. In 1981 Cantor

[Can] proved that irreducible polynomials had succinct certificates.

These improvements had no effect on the worst case exponential running time for polynomial factorization. Finally, in 1982, Arjen Lenstra, Hendrik Lenstra and Lazlo Lovász announced an algorithm [L^3] to factor $f(x) = a_m x^m + \ldots + a_0 \in Z[x]$ into irreducible factors over $Z[x]$ in time

$$O(m^{9+\epsilon} + m^{7+\epsilon} \log^{2+\epsilon}(\Sigma a_i^2)),$$

for any $\epsilon > 0$. Their algorithm incorporated several new ideas. As in previous algorithms, they factored $f(x)$ over Z/pZ for a suitably chosen p, and raised that factorization to a factorization over Z/p^kZ. They then defined a lattice contained in $Z+Zx+Zx^2+\ldots+Zx^{m-1}$ whose basis equals $\{ p^k x^i \mid 0 \leq i \leq l \} \bigcup \{ h(x)x^i \mid 0 \leq i \leq m-l \}$, where $h(x)$ is an irreducible factor of $f(x)$ in Z/p^kZ, and deg $h(x) = l$. By finding a "small" element in the lattice – using a basis reduction algorithm – they determine a factor of $f(x)$.

The L^3 algorithm brings many important algorithms into polynomial time. It is natural to ask if their algorithm can be extended to larger domains. Two domains of interest are: transcendental extensions and algebraic extensions. In Chapter 2 we show how to factor polynomials over algebraic number fields in polynomial time. The remainder of this chapter is devoted to filling in the necessary background for that result.

2. Sizes of Coefficients

It is a simple matter to show that if $g(x)$ divides $f(x)$ in $Z[x]$, then $g(x)$ is polynomial size as a function of $f(x)$ to write down. The situation is only slightly more complex in the case of algebraic number fields. First 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. In our algorithms we will work with the number field in its formulation as $Q[t]/g(t)$, although certain of our proofs will be in terms of $Q(\alpha)$. 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 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.

Suppose $\gamma = g_0 + g_1\alpha + \ldots + g_{m-1}\alpha^{m-1}$ is an element in $Q(\alpha)$, and

$$\begin{aligned}
\beta &= b_{11} + b_{12}\alpha + \ldots + b_{1m}\alpha^{m-1} \\
\beta\alpha &= b_{21} + b_{22}\alpha + \ldots + b_{2m}\alpha^{m-1} \\
&\vdots \quad \vdots \quad \vdots \\
\beta\alpha^{m-1} &= b_{m1} + b_{m2}\alpha + \ldots + b_{mm}\alpha^{m-1}
\end{aligned}$$

If we define a map from $Q(\alpha)$ to $Q(\alpha)$ by:

$$\gamma \mapsto \beta\gamma,$$

then the map corresponds to multiplication of the vector $(g_0, \ldots, g_{m-1})$ by the matrix (b_{ij}). If the matrices corresponding to β and γ are **B** and **G**, then $\beta + \gamma$ corresponds to **B**+**G**, and $\beta\gamma$ corresponds to **BG**. The set of matrices generated in this way form a ring isomorphic to $Q(\alpha)$. The matrix viewpoint is useful in analyzing certain algorithms. For example, that we can quickly test linear independence over Q of a set of elements of a number field is easily proved using these notions from linear algebra. Generally however, we will refer to a number field as $Q(\alpha)$ or $Q[t]/g(t)$.

It is convenient for us to consider a special class of algebraic numbers, the algebraic integers. A number α is an *algebraic integer* iff it is a root monic polynomial over Z. Of course, any polynomial over Q can be multiplied through by its common denominator, yielding a (not necessarily monic) polynomial over Z. Suppose $\beta_1, \ldots, \beta_m$ satisfy $h(x) = h_m x^m + \ldots + h_0$, where the h_i's are in Z. Consider the following polynomial time transformation of $h(x)$ into a monic polynomial with integer coefficents:

$$\begin{aligned}
h_m^{m-1}h(x) &= (h_m x)^m + h_{m-1}(h_m x)^{m-1} + \ldots + h_m^{m-1}h_0 \\
&= t^m + h_{m-1}t^{m-1} + \ldots + h_m^{m-1}h_0 \\
&= g(t)
\end{aligned}$$

The roots of $g(t)$, $h_m\beta_1, \ldots, h_m\beta_m$, are all algebraic integers. For the remainder of this discussion we assume $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ are algebraic integers satisfying $g(t)$, a monic irreducible polynomial over Z.

The set of algebraic integers of $K = Q(\alpha)$ form a ring, frequently written O_K. This ring is a natural extension of the integers, and many theorems about the integers can be generalized for the number rings. Of significance to us is Gauss' Lemma. It states that if $f(x)$ is a polynomial in $Z[x]$, $f(x)$ can be factored as the product of two polynomials with rational coefficients iff $f(x)$ can be factored as the product of two polynomials with integer coefficients, and can be generalized to:

Proposition 1.1: Let $f(x) \in O_K[x]$. Then $f(x)$ factors as the product of two polynomials with coefficients in K iff $f(x)$ factors as the product of two polynomials with coefficients in O_K.

If we factor $f(x)$, a polynomial in a number ring, the factors of $f(x)$ also lie in the number ring. It is somewhat more complicated than it was in the case of the integers to show that factors of $f(x)$ over O_K will have short descriptions. We do so now. First we need to know what the ring of integers of an algebraic number field looks like. In general, computing a basis for the ring of integers of an algebraic number field is at least as hard as determining the squarefree part of an integer [Mar], and it may be as difficult as factoring. Fortunately it is not necessary to do. We observe the following proposition, whose proof appears in the appendix.

Proposition 1.2: Let α be an algebraic integer satisfying $g(t)$, a monic irreducible polynomial over Z. The ring of algebraic integers of $Q(\alpha)$ is contained in $(1/d)Z[\alpha]$, where

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

If we factor a polynomial over $Z[\alpha][x]$, we are guaranteed that the coefficients of the factors lie in $(1/d)Z[\alpha]$. In particular, if we show that an integer coefficient of a factor of a polynomial in a number field is less than the integer "a" say, then the coefficient can be written as b/d, where $|b| < |a||d|$. Thus bounding a coefficient in absolute value bounds it in length of description. (That the number of digits needed to write down d is polynomial in $|g(t)|$ follows from the fact that $\mathrm{disc}(g(t)) = (-1)^{\frac{m(m-1)}{2}} \mathrm{Resultant}(g(t), g'(t))$ [Be,p.161.] (The resultant is defined in Section 3.))

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. We have defined size of polynomials diffferently from Weinberger and Rothschild, but their proof bounding coefficient sizes of factors requires only minor modification.

Theorem 1.3 [Weinberger and Rothschild]: Let β be a root of $f(x) \in Z[\alpha][x]$, notation as above. Then $[\![\beta]\!] \leq [\![f(x)]\!]$. Assume that $f(x)$ is monic, and let

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

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 $|c_{ij}| < m![\![f(x)]\!]^n |g(t)|^{m^2}$.

proof: It is not difficult to see that $[\![\alpha + \beta]\!] \leq [\![\alpha]\!] + [\![\beta]\!]$, and that $[\![\alpha\beta]\!] \leq [\![\alpha]\!][\![\beta]\!]$. We have noted previously that $[\![\alpha]\!] \leq 1 + \max_i |a_i| = |g(t)|$. A similar argument shows that

$$\begin{aligned} [\![\beta]\!] &\leq 1 + \max_i [\![\beta_i]\!] \\ &\leq (1 + \max_{i,j} |b_{ij}|)(1 + \max_i |a_i|)^m \\ &\leq [\![f(x)]\!] \quad . \end{aligned}$$

Suppose $h(x) \mid f(x)$ in $Q(\alpha)[x]$. By Proposition 1.1, $h(x) \in (1/d)Z[\alpha][x]$. Now $h(x) = \prod_{i \in S}(x - \beta_i)$, for some $S \subseteq \{1, \ldots, n\}$. Then $[\![h_i]\!] \leq \binom{r}{i}[\![f(x)]\!]^i$. This in turn is bounded by $[\![f(x)]\!]^n$, since $2 \leq [\![f(x)]\!]$ and $i \leq n$. We have bounded $[\![h_i]\!]$ in absolute value, now we seek to bound the integer coefficients of h_i.

If $\gamma \in Q(\alpha)$, $\gamma = \sum_{j=0}^{m-1} r_j\alpha^j$, $r_j \in Q$. Define $\gamma_i = \sum_{j=0}^{m-1} r_j\alpha_i^j$, and define a map L : $C^n \mapsto C^n$ by $L(r_0, \ldots, r_{m-1}) = (\gamma_1, \ldots, \gamma_m)$. Note that this map is invertible and linear. It is invertible because it is a Vandermonde matrix formed from $\alpha_1 \ldots \alpha_m$. We have $\det(L) = \mathrm{disc}(g(t))^{1/2}$. Let $|\gamma|_\infty = \max_i |\gamma_i|$, and $|r|_\infty = \max_i |r_i|$. Since all of the $r_i \in Q$, $\gamma \in Q(\alpha)$, and $|\gamma|_\infty = [\![\gamma]\!]$. The action of L is multiplication by a matrix, which, by abuse-of-notation, we also call L, $rL = \gamma$. Thus $r = \gamma L^{-1}$, and $|r|_\infty \leq |\gamma|_\infty |L^{-1}|_\infty$,

where $|L^{-1}|_\infty = \max_j(\sum_{i=1}^{m} l_{ij})$. If $r_j = c_j/d$, then $|c_j| < d[\![f(x)]\!]^n |L^{-1}|_\infty$.

Next we bound $|L^{-1}|_\infty$. By expressing L^{-1} in terms of cofactors of L, we find that each entry of L^{-1} is bounded by

$$\frac{(m-1)![\![\alpha]\!]^{\frac{m(m-1)}{2}}}{|\det(L)|}$$

Therefore

$$|L^{-1}|_\infty < \frac{m![\![\alpha]\!]^{\frac{m(m-1)}{2}}}{(\mathrm{disc}(g(t)))^{1/2}}$$

Thus

$$|c_j| < \frac{d[\![f(x)]\!]^n m![\![\alpha]\!]^{\frac{m(m-1)}{2}}}{\mathrm{disc}(g(t))^{1/2}} = \mathrm{disc}(g(t))^{1/2}[\![f(x)]\!]^n m![\![\alpha]\!]^{\frac{m(m-1)}{2}}$$

A rough bound will do for us. We note that $\mathrm{disc}(g(t))^{1/2} \leq [\![\alpha]\!]^{\frac{m(m-1)}{2}}$, and that $[\![\alpha]\!] \leq |g(t)|$. Thus,

$$|c_j| < m![\![f(x)]\!]^n |g(t)|^{m^2}$$

∎

3. The Norm

It is often easier to compute in the rationals than in the algebraic number fields, because of the rationals' simpler structure. A useful tool is the norm, which relates elements in the number fields to elements in Q. Let $Q(\alpha)$ be an algebraic number field, where α satisfies $g(t)$, an irreducible polynomial over Q, and let $\beta = a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \in Q(\alpha)$. Then

$$Norm(\beta) = N(\beta) = \prod_i (a_0 + a_1\alpha_i + \ldots + a_{m-1}\alpha_i^{m-1})$$

If σ is an element of the Galois group of $g(t)$ over Q (see Chapter II, §4), then $\sigma(\alpha) = \alpha_j$, where α_j is a conjugate of α over Q. Then

$$\begin{aligned}\sigma_j(N(\beta)) &= \sigma_j(\prod_i (a_0 + a_1\alpha_i + \ldots + a_{m-1}\alpha_i^{m-1})) \\ &= \prod_i \sigma_j(a_0 + a_1\alpha_i + \ldots + a_{m-1}\alpha_i^{m-1}) \\ &= \prod_i (a_0 + a_1\alpha_i + \ldots + a_{m-1}\alpha_i^{m-1})\end{aligned}$$

since σ_j just permutes the α_i's; thus $N(\beta) \in Q$. The norm is multiplicative, i.e. $N(\gamma\beta) = N(\gamma)N(\beta)$. We can think of a polynomial $f(x) \in Q(\alpha)[x]$ as a polynomial in two variables x and α, 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 $f(x) \in Q(\alpha)[x]$, $N(f(x)) \in Q[x]$. Under appropriate hypotheses, 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 over the number field. This idea is due to Kronecker. We examine these hypotheses in greater detail.

Theorem 1.4: Let $f(x) \in Q(\alpha)[x]$ be irreducible. Then $N(f(x))$ is a power of an irreducible polynomial in $Q[x]$.

proof: Suppose not. Then $N(f(x)) = C(x)D(x) \in Q[x]$, where $C(x)$ and $D(x)$ are relatively prime. $N(f(x)) = \prod_i f_{\alpha_i}(x)$: therefore $f_\alpha(x)$ must divide $C(x)$ or $D(x)$ in $Q(\alpha)[x]$. Without loss of generality, $f_\alpha(x) \mid C(x)$, which implies that there exists $g_\alpha(x) \in Q(\alpha)[x]$ such that $f_\alpha(x)g_\alpha(x)=C(x)$. Let $\sigma : Q(\alpha)[x] \mapsto Q(\alpha_i)[x]$ be an isomorphism. Then $\sigma(C(x)) = C(x)$ since $C(x)$ is in $Q[x]$, but $\sigma(f_\alpha(x)) = f_{\alpha_i}(x)$ and $\sigma(g_\alpha(x)) = g_{\alpha_i}(x)$. Thus we have $f_{\alpha_i}(x) \mid C(x)$ for all α_i which are conjugates of α. Now $C(x)$ and $D(x)$ are relatively prime. Therefore for all α_i, $f_{\alpha_i}(x) \not| D(x)$, which implies that $N(f(x)) = \prod_i f_{\alpha_i}(x) = C(x)$, and consequently $N(f(x))$ is a power of an irreducible polynomial. ∎

Theorem 1.5: Let $f(x) \in Q(\alpha)[x]$ be such that $N(f(x))$ is squarefree. Then if $N(f(x)) = \prod_i G_i(x)$ is a factorization into irreducible polynomials in $Q[x]$, then $f(x) = \prod_i \gcd(f(x), G_i(x))$ is a factorization into irreducibles in $Q(\alpha)[x]$.

proof: Let $g_i(x) = \gcd(f(x), G_i(x))$. Then we need to show that each $g_i(x)$ is irreducible, and that each irreducible factor of $f(x)$ appears in $\prod_i g_i(x)$. Let $h(x)$ be an irreducible factor of $f(x)$ in $Q(\alpha)[x]$. By Theorem 1.4, $N(h(x))$ is a power of an irreducible polynomial. But $N(h(x)) \mid N(f(x))$, and $N(f(x))$ is squarefree; thus $N(h(x)) = G_i(x)$ for some i.

The norm is multiplicative; thus the norm of $f(x)$ equals the products of the norms of the irreducible factors of $f(x)$. Each $G_i(x)$ is the norm of some irreducible factor of $f(x)$. The $G_i(x)$'s are all irreducible and distinct, which implies that the $g_i(x)$'s are all distinct

and irreducible. Since all the irreducible factors of $f(x)$ appear as some $\gcd(f(x), G_i(x))$ we are done. ∎

Our algorithm should now be clear. We begin with $f(x)$. So long as $N(f(x))$ is squarefree, we factor it over the rationals, then compute gcd's to obtain a factorization over $Q(\alpha)[x]$. These steps – computing the norm, factoring over the rationals, and taking gcd's – are all in polynomial time. The question of what to do if $N(f(x))$ is not squarefree remains. Kronecker [Kr] observed that so long as $f(x)$ has no repeated roots in $Q(\alpha)[x]$, $f(x)$ can be "twiddled" so as to make $N(f(x))$ squarefree. The proof we present is due to Trager [Tr.]

Lemma 1.6: Let $f(x) \in Q(\alpha)[x]$ be a squarefree polynomial of degree n, where $[Q(\alpha) : Q]=m$. Then there are at most $\frac{(nm)^2}{2}$ integers s such that $N(f(x - s\alpha))$ is not squarefree.

proof: Instead we show that there are at most $\frac{(n(n-1)m(m-1))}{2}$ integers s such that $N(f(x-s\alpha))$ has a repeated root: this will immediately imply the result. Suppose that the roots of $f(x)$ are $\{\beta_i\}$, then the roots of $N(f(x - s\alpha))$ are $\{\beta_i + s\alpha_j\}$, where the α_j's are conjugates of α. Then $N(f(x - s\alpha))$ has a repeated root iff $\beta_i + s\alpha_j = \beta_k + s\alpha_l$, for some $i \neq k$ or $j \neq l$. This would mean $s = (\alpha_l - \alpha_j)/(\beta_k = \beta_i)$. (We can divide, since $f(x)$ squarefree means that $\beta_k \neq \beta_i$ for $k \neq i$.) Clearly there are at most $\frac{(n(n-1)m(m-1))}{2}$ such s. ∎

The algorithm we have suggested to factor polynomials requires the computation of norms. The coefficients of the norm are all symmetric functions in the α_i, since $N(f(x)) = \prod_i f_{\alpha_i}(x)$. The straightforward way of calculating takes exponential time. Fortunately there is a way around this difficulty. (The discussion which follows on resultants is from [vdW,§ 5.8]; we include it for the sake of completeness.)

Let

$$h(x) = h_r x^r + h_{r-1}x^{r-1} + \ldots + h_0$$
$$k(x) = k_s x^s + k_{s-1}x^{s-1} + \cdots + k_0$$

for $h_i, k_j \in K$, a field.

We define the *resultant*,

$$Res_x(h(x),k(x)) = \begin{vmatrix} k_s & 0 & \dots & 0 & h_r & 0 & \dots & 0 \\ k_{s-1} & k_s & 0 \dots & 0 & h_{r-1} & h_r & 0 \dots & 0 \\ k_{s-2} & k_{s-1} & k_s \dots & 0 & h_{r-2} & h_{r-1} & h_r \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ \underbrace{0 \quad 0 \quad 0 \dots k_0}_{r} & & & & \underbrace{0 \quad 0 \quad 0 \dots h_0}_{s} & & & \end{vmatrix}$$

Observe that $h(x)$ and $k(x)$ have common divisor $\phi(x)$ iff there are polynomials $j(x), l(x)$ where

$$h(x)j(x) = k(x)l(x)$$

and $\deg(j(x)) < s, \deg(l(x)) < r$. In this case, $\text{Res}_x(h(x),k(x)) = 0$, since the $r+s$ rows of the resultant are not linearly independent. The resultant also vanishes if $k_s = h_r = 0$. These are the only times the resultant vanishes. Let

$$h(x) = h_r(x-\alpha_1)...(x-\alpha_r)$$
$$k(x) = k_s(x-\beta_1)...(x-\beta_s).$$

We view the coefficients of $h(x), h_\mu$, as symmetric functions in the variables α's, and the coefficients of $k(x), k_\nu$, as symmetric functions in the variables β's. The resultant is homogeneous of degree s in the h_μ, and of degree r in the k_ν. Then $R(x) = \text{Res}_x(h(x),k(x))$ is equal to $h_r^s k_s^r$ times a symmetric function of the α_i, β_j. If we consider the roots α_i, β_j as indeterminates x_i, y_j, the polynomial $k(x)$ vanishes for $x_i = y_j$, since in this case $h(x)$ and $k(x)$ have a linear factor in common. Because the linear forms $x_i - y_j$ are relatively prime to one another, $R(x)$ must be divisible by the product

$$T = h_r^s k_s^r \prod_i \prod_j (x_i - y_j),$$

Now $k(x) = k_s \prod_j (x - y_j)$. If we substitute $x = x_i$, we see that:

$$\prod_i k(x_i) = k_s^r \prod_i \prod_j (x_i - y_j).$$

Therefore $T = k_s^r \prod_i k(x_i) = (-1)^{rs} h_s^r \prod_j h(y_j)$, and $\text{Res}_x(h(x),k(x)) = h_r^s \prod k(\alpha_i)$, where the α_i are roots of $h(x)$. Then

$$N(f(x)) = \prod_i f_{\alpha_i}(x) = \text{Res}_t(g(t), f(x,t))/g_m^n,$$

where $f(x,t)$ is $f(x)$ with t's substituted in for α's.

We have introduced the resultant because it is a computationally efficient way to compute the norm. We now have almost all the tools neccesary to factor polynomials over algebraic number fields. In the next section, we examine gcd algorithms; then we will be ready to factor polynomials over algebraic number fields.

4. Computing Greatest Common Divisors

Algebraic computation has benefitted from the fact that many classical algorithms in algebra and number theory are highly efficient. This includes the Euclidean algorithm; however, a naive implementation runs the problem of coefficient blowup. Collins, and Brown and Traub were able to resolve this difficulty by using the theory of subresultants. In our algorithm, we will need to compute gcd's of polynomials over Q and over algebraic number fields.

Theorem 1.7 [Brown]: Let $f(x)$ and $g(x)$ be polynomials over $Q[x]$, of degree m and n respectively. Then $\gcd(f(x),g(x))$ can be computed in $O(max(|f(x)|,|g(x)|)^2(max(m,n)^4))$ steps.

Corollary 1.8: Let α satisfy a monic irreducible polynomial $\gamma(t)$ over Z of degree μ. Let d be the discriminant of $\gamma(t)$. If $f(x)$ is of degree m and $g(x)$ is of degree n are polynomials over $O_K[x]$, $K = Q[t]/g(t)$, then the $\gcd(f(x),g(x))$ can be computed in

$$O(m((m+n)(\log [\![f(x)]\!] + \log [\![g(x)]\!]) + \mu \log |\gamma(t)|)^2((m+n)^7 + \mu^3))$$

steps.

proof: We perform Brown's algorithm 1 [Br2] with a minor modification. We assume that $f(x)$ and $g(x)$ are polynomials in two variables, x and t, and that we compute the gcd first with respect to x. The way we do this is to compute the gcd of the coefficients of $f(x)$ and $g(x)$. Suppose $c_1(t)$ and $d_1(t)$ are the respective gcd's of the coefficients. Then we compute $\gcd_{Q[t]/g(t)}(f(x)/c_1(t), g(x)/d_1(t))$. If $G_1(x) = f(x)/c_1(t), G_2(x) = g(x)/d_1(t)$, then we successively compute the subresultants $G_3,\ldots,G_k$ until the pseudoremainder $(G_{k-1},G_k) = 0$. The coefficients of the pseudoremainders $G_i(x)$ are polynomials in t. Each time however,

that we compute a pseudoremainder $G_i(x)$ we perform the first step of the gcd algorithm on the coefficients of $G_i(x)$ with respect to $g(t)$. This has the effect of reducing the coefficients of $G_i(x)$ mod $g(t)$, which is precisely what we want.

Computation of the subresultant requires $O((m+n)(\log [\![f(x)]\!] + \log [\![g(x)]\!])^2(m+n)^7)$ steps, since the number of variables, $v = 1$, the length, $l = (m+n)(\log [\![f(x)]\!] + \log [\![g(x)]\!])$, $\delta = 1$ and adds only a constant factor, and d and d_2 are bounded by $m+n$. Similarly, the time for each pseudodivision by $\gamma(t)$ is $O(((m+n)(\log [\![f(x)]\!] + \log [\![g(x)]\!]) + \mu \log |\gamma|(t))^2\mu^3)$ steps since the degrees, d_2, δ and d are less than $m+n$, and v, the number of variables, is 1. This process must be done at most $min(m,n)$ times; wlog $min(m,n)$. Thus the entire computation requires at most $O(m((m+n)(\log [\![f(x)]\!] + \log [\![g(x)]\!]) + \mu \log |\gamma(t)|)^2((m+n)^7 + \mu^3))$ steps. ∎

Chapter II

Factoring Polynomials over Algebraic Number Fields

1. An Algorithm

We have provided the necessary background for factoring polynomials over algebraic number fields. Let α be a root of $g(t)$, a monic irreducible polynomial with coefficients in Z, and discriminant d, and suppose $f(x)$ of degree n is a polynomial whose coefficients lie in O_K, where $K = Q(\alpha)$. We can think of $f(x)$ as a polynomial in two variables, x and α. (When there is no risk of confusion, we use $f(x)$ and $f(x,t)$ interchangeably.)

In Chapter I, we sketched an algorithm due to Kronecker, for factoring polynomials over an algebraic number field. We present it here. We find $h(x) = \gcd(f(x), f'(x))$. Then $h(x)$ is squarefree, and all the irreducible factors of $f(x)$ appear as factors of $h(x)$. We compute an integer "c" such that $N_{Q(\alpha)/Q}(h(x - c\alpha)) = F(x)$ is squarefree. Using the L^3 algorithm, we factor $F(x) = \prod_{i=1}^{r} F_i(x)$ over Q. By computing the $\gcd_{Q(\alpha)}(F_i(x), h(x))$ for $i = 1,\ldots,r$, we obtain a factorization of $h(x)$ over $Q(\alpha)$. This allows us to determine a factorization of $f(x)$ over $Q(\alpha)$. We now give an algorithm to factor $f(x)$ over $O_K[x]$ in $O((mn)^{9+\epsilon}\log^{2+\epsilon}((mn)^2 \mid g(t) \mid [\![f(x)]\!]))$ steps.

Algorithm 2.1 FACTOR

input: $g(t) \in Z[t]$, monic, irreducible

$f(x) \in Q[x,t]$; $f(x)$ with coefficients in O_K, $K = Q[t]/(g(t))$

Step 1: $c \leftarrow 1$

$j \leftarrow 0$

$c(t) \leftarrow \text{cont}(f(x,t))$

$f(x) \leftarrow f(x)/c(t)$

$k(x) \leftarrow \gcd_{Q[t]/g(t)}(f(x), f'(x))$

$h(x) \leftarrow f(x)/k(x)$

Step 2: $l(x) \leftarrow \text{Res}_t(g(t), h(x - ct))$

While $(\gcd(l(x), l'(x)) \neq 1)$, do:

$c \leftarrow c + 1$

$l(x) \leftarrow \text{Res}_t(g(t), h(x - ct))$

Step 3: Factor $l(x) = \prod_{i=1}^{r} F_i(x)$

Step 4: For $i = 1, \ldots, r$, do:

$f_i(x) \leftarrow \gcd_{Q[t]/g(t)}(F_i(x + ct), h(x))$

Step 5: If $(k(x) = 1)$ then return $\{ f_i(x) \}, c(t)$

Else for $i = 1, \ldots, r$, do:

While $\gcd(F_i(x + ct), k(x)) \neq 1$, do:

$j \leftarrow j + 1$

$f_{j+r}(x) \leftarrow \gcd(F_i(x + ct), k(x))$

$k(x) \leftarrow k(x)/f_{j+r}(x)$

return: $\{ f_i(x) \}, c(t)$, where $f_i(x)$ is irreducible and primitive over $O_K[x]$,

where $K = Q[t]/g(t)$, and $f(x) = c(t) \prod_{i=1}^{j+r} f_i(x)$

Theorem 2.1: Algorithm 2.1 computes a factorization of $f(x)$, a polynomial of degree n over $O_K[x]$ into irreducible factors in $O_K[x]$. It does so in $O((mn)^{9+\epsilon}\log^{2+\epsilon}(m^2n^2|g(t)|[\![f(x)]\!]))$ steps.

proof: The algorithm has four major steps. Step 1 transforms $f(x)$ into a primitive polynomial and computes the squarefree part of $f(x), h(x)$. In order to factor $f(x)$ it suffices to factor $h(x)$. Step 2 computes an integer c such that $Norm_{(Q[t]/g(t))/Q}(h(x-ct))$ is squarefree. Lemma 1.6 guarantees that there is a c less than $(\text{degree}(g(t))\text{degree}(f(x)))^2$ which yields $h(x-ct)$ which has squarefree norm.

In Step 3, we factor $l(x) = N(h(x-ct))$. Theorem 1.6 assures us that if $l(x) = \prod_{i=1}^{r} F_i(x)$ is a complete factorization of $l(x)$ in $Q[x]$, then

$$h(x-ct) = \prod_{i=1}^{r} \gcd(F_i(x), h(x-ct)) = \prod_{i=1}^{r} f_i(x-ct)$$

will be a complete factorization of $h(x-ct)$ in $Q(\alpha)[x]$. We are interested in a factorization of $h(x)$ however; instead we compute $f_i(x) = \gcd(F_i(x+ct), h(x))$. We are nearly done. All that remains to be done is the factorization of $k(x)$, but all irreducible factors of $k(x)$ appear as factors of $h(x)$. By computing gcd's, Step 5 computes a complete factorization of $k(x)$.

By the work of Collins, Brown and Traub on polynomial gcd's, it is clear that all of the above steps can be done in polynomial time. We do a careful analysis to obtain the bounds of the theorem. (Note that the work of Weinberger and Rothschild shows that $h(x)$ in Step 1, and the $f_i(x)$ in Steps 4 and 5 are polynomial size in $(\log [\![f(x)]\!], \log|g(t)|, m, n)$ to write down.)

Step 1 requires n gcd's of polynomials in a single variable to obtain $c(t)$, and one gcd over $Q[t]/g(t)$ to obtain $k(x)$ and $h(x)$. The time required for Step 1 is subsumed by the time required for Steps 2 and 4.

In Step 2, we must find a c such that $Norm_{(Q[t]/g(t))/Q}(h(x-ct))$ is squarefree. We compute the norm by resultants. The resultant is the deteriminant of a $2m \times 2m$ matrix whose entires are polynomials in x. The integer coefficients of these polynomials are bounded by $(mn)^{m+1}m![\![f(x)]\!]^n|g(t)|^{m^2}$ in absolute value, and therefore the integer coefficients of the resulting polynomial, the norm, are bounded by $(2m)!((mn)^{m+1}m![\![f(x)]\!]^n|g(t)|^{m^2})^{2m}$.

We need to determine if $N(h(x-ct))$ is squarefree; we do this by computing the gcd of $N(h(x-ct))$ and $N'(h(x-ct))$ over $Q[x]$. Now the roots of $N(h(x-ct))$ are of the form $\beta + c\alpha$, where β is a root of $f(x)$, and α is a root of $g(t)$. Thus

$$[\![\beta + c\alpha]\!] < c[\![\beta]\!][\![\alpha]\!] < (mn)^2[\![f(x)]\!]|g(t)|$$

It follows that the integer coefficients of $N(h(x-ct))$ and $N'(h(x-ct))$ are less than $((mn)^2[\![f(x)]\!]|g(t)|)^{mn}$ since the polynomials are of degree at most mn. By Brown [Br2] this gcd requires at most $O((mn(\log((mn)^2[\![f(x)]\!]|g(t)|))^2(mn)^4)$ $=O(m^6n^6[\![f(x)]\!]|g(t)|)$ steps.

Step 3 factors $l(x) = N(h(x-ct))$ which is squarefree. As before, the integer coefficients of $N(h(x-ct))$ are less than $((mn)^2[\![f(x)]\!]|g(t)|)^{mn}$ in absolute value, or require at most $mn\log(m^2n^2[\![f(x)]\!]|g(t)|)$ bits to write down. Thus $l(x)$ can be factored in $O((m^{7+\epsilon}n^{7+\epsilon})$ $(mn\log(m^2n^2[\![f(x)]\!]|g(t)|))^{2+\epsilon}))= O(m^{9+\epsilon}n^{9+\epsilon}\log^{2+\epsilon}(m^2n^2[\![f(x)]\!]|g(t)|))$ steps.

In Step 4, we compute at most n gcd's of polynomials. The factors determined in Step 3 of the Algorithm are of degree at most mn, and have coefficients of length at most $mn\log(m^2n^2[\![f(x)]\!]|g(t)|)$ bits, while $h(x)$ is of degree at most n, with integer coefficients requiring at most $n\log[\![f(x)]\!] + m^2\log|g(t)|$ bits. Thus this step can be done in $O((mn)^9(n[\![f(x)]\!] + m^2[\![g(t)]\!])^2))$ steps. Finally the running time in Step 5 is dominated by that of Step 4. Our total running time is dominated by Step 3 of the algorithm, and the theorem is proved. ∎

The running time of the algorithm we present to factor polynomials over algebraic number fields is dominated by the time required by the L^3 algorithm to factor polynomials over the integers. We expect that the running time of this algorithm will be improved. To simplify what is to follow, we let $F(\log|g(t)|, m, \log[\![f(x)]\!], n)$ be the time required to factor $f(x)$ of degree n over $Q[t]/g(t)$, where $g(t)$ is a monic irreducible polynomial of degree m over the integers, and $f(x) \in O_K$, where $K = Q[t]/g(t)$.

2. Primitive Elements

We observed earlier that an algebraic number field can be written as $Q(\alpha)$ for an appropriate α. In our algorithm, we assumed that the number field over which we are factoring was preseneted as $Q(\alpha)$. Suppose we were asked to factor $f(x) \in Q(\alpha,\beta)[x]$; how would we proceed? We could calculate a primitive element for $Q(\alpha,\beta)$, and apply the Algorithm 2.1 directly. Alternatively, we might observe that

$$N_{Q(\alpha,\beta)/Q}(f(x)) = N_{Q(\alpha)/Q}\big(N_{Q(\alpha,\beta)/Q(\alpha)}(f(x))\big).$$

In order to factor $f(x)$ over $Q(\alpha,\beta)$, we could compute $N_{Q(\alpha,\beta)/Q(\alpha)}(f(x))$, and then consider the question of factoring that polynomial over $Q(\alpha)$. Such an approach leads to a bootstrapping technique for factoring which is, in some cases, faster than the method of finding a primitive element. For later applications however, we have found it useful, and *not more costly* to obtain a primitive element.

If β satisfies $h(x)$, an irreducible polynomial over $Q(\alpha)$, then whenever $N_{Q(\alpha)/Q}(h(x-c\alpha))$ is squarefree, $Q(\beta + c\alpha) = Q(\alpha,\beta)$. This is a consequence of Theorem 1.6. We prove this result.

Proposition 2.2: Let α satisfy $g(t)$, a monic irreducible polynomial of degree m over Z, and let β satisfy $h(x)$, a monic irreducible polynomial of degree n over $K = Q(\alpha)$ with coefficients in O_K. Then there is an integer c less than $(mn)^2$ such that $Q(c\alpha + \beta) = Q(\alpha,\beta)$. Furthermore, let $f(x)$ be the minimal polynomial for $c\alpha + \beta$ over Q which has integer coefficients and is monic. Then $[\![f(x)]\!] \leq (mn[\![h(x)]\!]|g(t)|)^{mn}$ and $\deg(f(x)) = mn$.

proof: Pick an integer c such that $N_{Q(\alpha)/Q}(h(x - c\alpha))$ is squarefree and consider $h(x - c\alpha) = h(x - cy, y)$ as a polynomial in two variables. Then α is a root of $h(\beta - cy, y)$. Let the roots of $g(t)$ be $\alpha_1(= \alpha), \alpha_2, \ldots, \alpha_m$. Observe that $\alpha_j \neq \alpha$ is not a root of $h(\beta - cy, y)$ since otherwise $N_{Q(\alpha)/Q}(h(x - c\alpha)) = \prod_i h(x - c\alpha_i)$ would have a multiple root β , and would not be squarefree. We see that $y - \alpha = \gcd(h(\beta - cy, y), g(y))$. This means α is in $Q(\beta + c\alpha)$, and consequently that $Q(c\alpha + \beta) = Q(\alpha,\beta)$. Then $f(x) = N_{Q(\alpha)/Q}(h(x - c\alpha))$ is the minimum polynomial for $c\alpha + \beta$ over Q. Since the roots of $f(x)$

are $\{ \beta_i + c\alpha_j \mid 1 \leq i \leq n, 1 \leq j \leq m \}$,

$$\begin{aligned} [\![f(x)]\!] &\leq ([\![\alpha]\!]_i + c\beta_j)^{mn} \\ &\leq (mn[\![h(x)]\!]|g(t)|)^{mn}. \end{aligned}$$

That degree$(f(x)) = mn$ is obvious. ∎

3. Corollaries

The ability to factor allows many other computations. Questions whose solutions were infeasible are now in polynomial time. We list several consequences of Algorithm 2.1 before we turn to Galois theory.

Corollary 2.3: Factoring multivariate polynomials over algebraic number fields is polynomial time reducible to factoring multivariates over the rationals.

proof: The algebraic property necessary for the proofs of Theorems 2 and 3 is that $Q(\alpha)[x]$ is a unique factorization domain. Since $Q(\alpha)[x_1, \ldots, x_n]$ is also, Theorems 2 and 3 extend to these domains. To prove Lemma 4, we consider $f(x_1, \ldots, x_n) \in Q(\alpha)[x_1, \ldots, x_n]$ as a polynomial in x_1 with coefficients in $Q(\alpha)[x_2, \ldots, x_n]$. (Note that since we can factor $n+1$ variable polynomials over Q, we can compute the gcd of n variable polynomials over $Q(\alpha)$.) Let $\deg_{x_1}(f(x_1, \ldots, x_n)) = n_1$, and $[Q(\alpha) : Q] = m$. As before, we assume $f(x_1, \ldots, x_n)$ is squarefree; otherwise we take the gcd to obtain the square free part of $f(x_1, \ldots, x_n)$. Then $N(f(x_1, \ldots, x_n))$ has no repeated roots. Viewing $f(x_1, \ldots, x_n)$ as a polynomial in x_1 with coefficients in $Q(\alpha)[x_2, \ldots, x_n]$, it has n_1 roots. The proof of the lemma goes through as before, and we obtain our reduction. ∎

Kaltofen [Ka1],[Ka2], and A. Lenstra [Lpc] have independently shown that factoring a polynomial with a bounded number of variables over the rationals is polynomial time equivalent to factoring a univariate polynomial over the rationals. In light of Corollary 2.3 and the earlier [L^3] result, we conclude that factoring a polynomial with a bounded number of variables over an algebraic number field presented as $Q(\alpha)$ can be done in polynomial time.

Corollary 2.4: Let α satisfy $g(t)$, an irreducible polynomial of degree m over Z, and let β satisfy $f(x)$, an irreducible polynomial of degree n over $Z[\alpha]$. Then determining if the intersection of $Q(\alpha)$ and $Q(\beta)$ is Q can be done in time polynomial in $(\log|g(t)|, \log[\![f(x)]\!], m, n)$.

proof: Let $h(x)$ be the minimal polynomial of β over Q. If α does not satisfy $h(x)$, (i.e. α and β are not conjugates over Q), then $Q(\alpha) \cap Q(\beta) = Q$ iff $h(x)$ remains irreducible over $Q(\alpha)$. If α is a root of $h(x)$, then $Q(\alpha) \cap Q(\beta) = Q$ iff $h(x)/x - \alpha$ is irreducible over $Q(\alpha)$. ∎

Those number fields, $Q(\alpha)$, which are distinguished by the fact that α may be expressed as a combination of several m^{th} roots are called the *radical number fields.*

Corollary 2.5: Finding bases for radical number fields can be done in polynomial time.

Corollary 2.6: Finding bases for algebraic number fields can be done in polynomial time.

For a long time normal polynomials – polynomials which factor completely upon adjoing a single root – were most difficult to factor. In the next section, we will present a brief background to Galois theory. However we would like to note the following corollary:

Corollary 2.7: Let $f(x) \in Z[x]$ be of degree n. Then $f(x)$ can be checked for normality in time polynomial in $(\log|f(x)|, n)$. Furthermore, if $f(x)$ is normal, computing its Galois group can be done in time polynomial in $(\log|f(x)|, n)$.

4. A Brief Introduction to Galois Theory

Let K be an algebraic number field, and let $f(x)$ be a polynomial with coefficients in K, with roots $\alpha_1, ...\alpha_m$. 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 $K(\alpha_1, ..., \alpha_m)$ is called the *splitting field of f(x) over K.* We consider the set of automorphisms of $K(\alpha_1, ..., \alpha_m)$ which leave K fixed. These form a group, called the *Galois group of* $K(\alpha_1, ..., \alpha_m)$ *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 $K(\alpha_1, ..., \alpha_m)$.

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, for if β and γ are fixed by all σ in H, then so are $\beta \pm \gamma, \beta \times \gamma$, and (for $\gamma \neq 0$), β/γ. Furthermore H fixes K so that we have

$$K \subseteq K(\alpha_1, \ldots, \alpha_m)^H \subseteq K(\alpha_1, \ldots, \alpha_m) \quad .$$

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 $\alpha_1, ..., \alpha_m$, be irreducible over $K[x]$. Then:

(1) Every intermediate field $K(\beta)$, $K \subset K(\beta) \subset K(\alpha_1, ..., \alpha_m)$ 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 $K(\alpha_1, ..., \alpha_m)$ which are invariant under the action of H.

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

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

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. If

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

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

(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 $\sqrt[17]{1}$. We will require that all solutions to the equation in question be represented by expressions of the form:

$$\sqrt[v]{\sqrt[h]{p\ldots} + \sqrt[c]{\ldots}} \qquad (*)$$

(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, let us consider for a moment determining expressibility of a root in radicals over $Q(\zeta_m)$, where ζ_m is a primitive m^{th} root of unity. This will simplify the situation. (We will discuss the question of expressing roots of unity in terms of radicals in Chapter V.) Suppose a root α_i is expressible in terms of 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, $Q(\zeta_m) = F_k \subset F_{k-1} \subset \ldots \subset F_0$, 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, $G_0 \subset G_1 \subset \ldots \subset G_k = G$, 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. 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 can do this in polynomial time given generators of the group. Since there is at present no polynomial time algorithm for determining the generators of the Galois group, we do not use this approach. An obvious approach is to divide-and-conquer, and solvability provides a natural way to do this. 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 chapter.

Chapter III

Finding Blocks of Imprimitivity

1. Background

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*. If $B \neq \Omega$ is a maximal block of G we can consider an induced action of G on $\{B, \sigma_2 B \ldots \sigma_k B\}$. Our idea is to construct minimal blocks of imprimitivity, and to consider actions on the blocks. In this section we provide the background necessary for our algorithm. Our first theorem is the following well known characterization of primitive groups.

Theorem 3.1: Let $\alpha \in \Omega$, $|\Omega| \neq 1$. Then the transitive group G on Ω is primitive iff G_α is maximal.

proof: Let Λ be a nontrivial block containing α, and suppose $\beta \neq \alpha \in \Lambda$. Define

$$H = \{ \sigma \in G \mid \sigma(\Lambda) = \Lambda \} \quad .$$

Then $G_\alpha \subseteq H$. G is transitive, thus there is a $\sigma \in G$ with $\sigma(\alpha) = \beta$. In particular, there is a $\sigma \in H$ with $\sigma(\alpha) = \beta$. Then $G_\alpha \subsetneq H$. Furthermore $\Lambda \neq \Omega$, so $H \neq G$, and therefore G_α is not maximal.

Next assume there is a subgroup H of G with $G_\alpha \subsetneq H \subsetneq G$. We let

$$\Lambda = \{ \sigma(\alpha) \mid \sigma \in H \} \quad ,$$

and we claim that Λ is a block. If β is in $\Lambda \cap \tau\Lambda$ for some τ, and element of G, then

$$\beta = \sigma_1(\alpha) = \tau\sigma_2(\alpha)$$

with σ_1, σ_2 belonging to H. This means that $\sigma_1^{-1}\tau\sigma_2$ are elements in G_α. But σ_1, σ_2 are in H. and thus τ is an element of H. But $G_\alpha \subsetneq H$ means that Λ contains some element other than α. But $\Lambda = \tau\Lambda$ only for τ in H. We know that $H \subsetneq G$ implies that $\Lambda \neq \Omega$. Therefore G is imprimitive. ∎

Actually the same proof may be used to show the stronger:

Proposition 3.2: 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, the case that $f(x)$ is normal happens only rarely. But it is not much more difficult to construct minimal blocks in the general case.

Theorem 3.3: Let $\Lambda \subseteq \Omega$, and $\alpha \in \Omega$. Then

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

is a block of the transitive group G.

proof: Let σ be an element of G, and suppose $\Delta \cap \sigma\Delta \neq \emptyset$. Let α be in Δ, then α an element of $\tau\Lambda$ implies α is in $\sigma\tau\Lambda$. Then $\Delta \subseteq \sigma\Delta$. But we know that $|\Delta| = |\sigma\Delta|$, which means that $\Delta = \sigma\Delta$.

Next suppose $\beta \in \Delta \cap \sigma\Delta$. Since G is a transitive group, there is a $\tau \in G$ with $\tau(\alpha) = \beta$. Then α is an element of $\tau^{-1}\Delta$ and $\tau^{-1}\sigma\Delta$ as well as in Δ. This means that

$$\Delta = \tau^{-1}\Delta = \tau^{-1}\sigma\Delta$$

and in particular $\tau\Delta = \Delta$. Then Δ is a block of G. ∎

Corollary 3.4: Let

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

Then Λ is a block of G.

proof: We let $\Delta = \Lambda$. The corollary follows immediately from Theorem 3.3, since $\sigma(\alpha) = \alpha$ for all α in G_α. ∎

Theorem 3.1 gives a characterization of primitive groups. We offer as an alternate characterization one that will allow us to compute blocks of imprimitivity.

Theorem 3.5: 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 degree.

proof: We suppose G is not regular.

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

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

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

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

Suppose $\Lambda = \{\alpha\}$. Then $G_\alpha = G_\beta$, and we let

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

We know α, β are in Δ, so Δ is nontrivial. Furthermore G is transitive, so $\Delta \neq \Omega$. By Corollary 3.4, Δ is a block.

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

Proposition 3.6: 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, $\gamma \neq \alpha$, $\Lambda = \{\sigma(\alpha) \mid \sigma \in G_\alpha G_\gamma\}$.

proof: Let γ be in Λ, $\gamma \neq \alpha$. Then we let $\Delta = \{\sigma(\alpha) \mid \sigma \in G_\alpha G_\gamma\}$. Since $G_\alpha G_\gamma \subset G_\Lambda$, we have $\Delta \subset \Lambda$.

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 $G_\alpha G_\beta$. But $\alpha = \sigma_1^{-1}\tau\sigma_2(\alpha)$ means that $\sigma_1^{-1}\tau\sigma_2$ is an element of G_α. Then τ belongs to $G_\alpha G_\beta$, and $\tau\Delta = \Delta$. Therefore Δ is a block. But Λ is a minimal nontrivial block containing α; therefore $\Delta = \Lambda$. ∎

Proposition 3.6 provides the backbone of our algorithm. Since the roots of the irreducible factors of $f(x)$ form the orbits of G_α, the orbit structure of G_α can be determined from a factorization of $f(x)$ in $Q(\alpha)[x]$. Similarly we can 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 $Q(\alpha, \beta)[x]$, we can tie together the orbit structures of G_α and G_β in such a way as to determine if $G_\alpha G_\beta = G$. By transitivity, α can be fixed, and we need loop only over β.

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}. We know by Corollary 3.4 that 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 $\overline{\sigma}$ be the induced action of σ on $\alpha_1, \ldots, \alpha_k$. Then if $\overline{\sigma}(\alpha_1) = \alpha_j = p_j(\alpha_1)$, we have $\overline{\sigma}(\alpha_l) = \overline{\sigma}(p_l(\alpha_1)) = p_j(p_l(\alpha_1))$. 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:

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

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 3.7: 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 3.8: 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 $g_j(x)$ 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 Lemma 3.6, this will give us a minimal nontrivial block containing α_1, if one exists. In the next section we present an algorithm to compute the minimal blocks of imprimitivity, along with a proof of correctness and an analysis of running time.

2. An Algorithm

Algorithm 3.1 BLOCKS

input: $f(x) \in Z[x]$, $f(x)$ irreducible of degree n over Z

Step 1: Find $c \neq 0$ such that $N_z(f(x - cz))$ is squarefree and factor $N_z(f(x - cz))$ over Q,

$$N_z(f(x - cz)) = \prod_{i=1}^{l} G_i(x - cz)$$

[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 $Q[z]/f(z)$.]

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 $N_z(f(x - cz))$ 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 $\Gamma_j = (V_j, E_j)$, with vertices, V_j, and edges, E_j given by:

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

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

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

Theorem 3.9: If $f(x) \in Z[x]$ of degree n is irreducible, Algorithm 3.1 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 size less than $[\![f(x)]\!]^{n^2}$ over a field containing two roots of $f(z)$.

proof: By Proposition 2.2, Step 1 determines a primitive element for $Q[y,z]/(f(z), g_i^z(y))$. By Theorem 2.1, Step 2 factors $f(x) = \prod g_i(x)$ over $Q[z]/f(z)$. In Corollary 3.4 we demonstrated that the fixed points of G_z (which correspond exactly to the constant terms of the linear factors of $f(x)$ over $Q[x,z]/f(z)$ form a block. The induced action of G_z on the

minimal block can be determined from the Cayley table. Step 3 also computes a minimal block (which is trivial) for the case when G is a group of order p acting on p elements. Step 4 merely expresses the roots y and z of $f(x)$ in terms of a primitive element for the field $Q[t]/G_j(t) = Q[y,z]/(f(z), g_i^z(t))$; a proof of correctness appears in [van der Waerden, p. 139.] Step 5 rewrites the factorization of $f(x)$ in $Q[z]/f(z)$ in terms of $Q[t]/(G_j(t))$, and also expresses a factorization of $f(x)$ over $Q[y]/f(y)$ in terms of $Q[t]/G_j(t)$. Step 7 computes the graph Γ_j. By Lemma 3.8, Step 9 yields a polynomial whose roots form the block of imprimitivity

$$\Lambda = \{\, \sigma(\alpha_1) \mid \sigma \in G_{\alpha_1} G_{\alpha_j} \,\}.$$

Using Proposition 3.6 we conclude that Step 10 gives a polynomial whose roots form a minimal block containing α_1.

Let us now analyze the running time. Recall $F(\log|g(t)|, m, \log[\![f(x)]\!], n)$ is the time required to factor a polynomial of coefficient size $[\![f(x)]\!]$ and of degree n over $O_K[x]$, where $K = Q[t]/g(t)$, and $g(t)$ is a monic irreducible polynomial of degree m over Z. We let $\mathrm{GCD}(\log[\![f(x)]\!], k, \log[\![g(x)]\!], l, \log|h(t)|, m)$ be the time required to compute the gcd of two polynomials $f(x)$ and $g(x)$ in $O_K[x]$ of coefficent size $[\![f(x)]\!]$ and $[\![g(x)]\!]$ and of degree k and l respectively, where $K = Q[t]/h(t)$, and $h(t)$ is a monic irreducible polynomial over Z.

Let $\deg(f(x)) = n$. Step 1 of the algorithm is a preprocessing step for factoring $f(x)$ over $Q[z]/f(z)$. Step 3 requires at most n substitutions and polynomial divisions in addition to the time required to find blocks in a group of order n. This can be done in $O(n \log n)$ steps [At]. We cycle through Step 4 at most $O(n)$ times. Computing $p_j(t)$ and $q_j(t)$ requires one gcd over $Q[t]/G_j(t)$. Step 6 can be done in $O(n)$ steps. Step 7 is again a gcd, done at most $O(n^2)$ times. Step 8 can be done in $O(n^2)$ steps [AHU]. The overall running time is bounded by:

$$O\Big(F(\log|f(x)|, n, \log[\![f(x)]\!], n) + n^3 \mathrm{GCD}(\log[\![(f(x))]\!]^{n^2}, n, \log[\![(f(x))]\!]^{n^2}, n, \log|f(x)|, n)\Big) \quad ;$$

or, more simply, the time needed to find a minimal block of roots of $f(x)$ is the time needed for one factorization of $f(x)$ over $Q[z]/f(x)$, plus the time needed for n^3 gcd's of factors of $f(x)$ over a field containing two roots of $f(x)$. ∎

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 chapter we see how to 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. We present a generalization of Algorithm 3.1 in the next section.

3. A Corollary

Another way to think about Algorithm 3.1 is that it computes the intersection of $Q(\alpha_1)$ and $Q(\alpha_s)$. Observe that G_{α_1} is the subgroup of G belonging to the subfield $Q(\alpha_1)$, and that G_{α_s} is the subgroup of G belonging to $Q(\alpha_s)$. Then $G_{\alpha_1}G_{\alpha_s}$ is the subgroup of G belonging to $Q(\alpha_1) \cap Q(\alpha_s)$ [Theorem B, Chapter 2.] In a similar way we can compute $Q(\alpha) \cap Q(\beta)$ even when α and β are not conjugate over Q.

There is a difficulty if we view the intersection in terms of the minimal polynomials for α and β over Q, since the minimal polynomial for β over Q may factor over $Q(\alpha)$, in which case the intersection is ambiguous. In order for the problem to be well-defined, 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 $Q[x]/f(x)$ is well-defined. We present an algorithm which, given the polynomials $f(x)$ and $h(x)$, computes the intersection of $Q(\alpha)$ and $Q(\beta)$.

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 $\beta = \beta_1$. By Proposition 2.2, we know there exists a c less than $(mn)^2$ 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 $\{\beta_j + c\alpha_i \mid j = 1, \ldots, n; \quad i = 1, \ldots, m\}$.

Let $Q(\rho)$ be the splitting field of $H(x)$ over Q, and let G be its Galois group. Then $Q(\rho) = Q(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$, and G_α and G_β are subgroups of G. They are the

subgroups belonging to $Q(\alpha)$ and $Q(\beta)$ respectively. Consider

$$H(x) = j_1(x)\ldots j_k(x) \text{ in } Q(\alpha)[x], \text{ and}$$
$$= k_1(x)\ldots k_l(x) \text{ in } Q(\beta)[x],$$

where the $j_i(x)$ and $k_j(x)$ are irreducible factors of $H(x)$ over $Q(\alpha)$ and $Q(\beta)$ respectively, and $j_1(x) = h(x - c\alpha)$.

Let us define a graph Γ with Vertices, V, and Edges, E by:

$$V = \{ j_i(x) \} \cup \{ k_j(x) \}$$
$$E = \{ (j_i(x), k_j(x)) \mid \gcd(j_i(x), k_j(x)) \neq 1 \}$$

Again we compute the set of vertices $j_i(x)$ connected to $j_1(x)$, and we let

$$I(x) = \prod_{j_i(x) \text{ is connected to } j_1(x)} j_i(x)$$

and let $\Lambda = \{ \gamma_i \mid \gamma_i \text{ is a root of } I(x) \}$. We claim $\Lambda = \{ \sigma(\gamma_1) \mid \sigma \in G_\alpha G_\beta \}$. We observe:

Lemma 3.10: Let γ_i be a root of $j_i(x)$ in $Q(\alpha)[x]$. Then the roots of $j_i(x)$ are precisely $G_\alpha(\gamma_i)$.

It follows immediately that $\gcd(j_i(x), k_j(x)) \neq 1$ iff $G_\alpha \cap G_\beta \neq \emptyset$, where γ_i is a root of $j_i(x)$ and γ_j is a root of $k_j(x)$. This implies:

Lemma 3.11: Let α_i be a root of $j_i(x)$ in $Q(\alpha)[x]$. Then $\alpha_i \in \Lambda = \{ \sigma(\alpha_1) \mid \sigma \in G_\alpha G_\beta \}$ iff $g_i(x)$ is connected to $j_1(x)$.

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 3.1. This gives us the algorithm **INTERSECTION**, which runs in polynomial time.

Algorithm 3.2 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 $N_z(h(x - cz))$ is squarefree and factor:

$$H(x) = N_z(h(x - cz)) = \prod_{i=1}^{k} j_i^z(x) \text{ over } Q[z]/f(z),$$

[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 factorizations over $Q[t]/H(t)$.]

Step 6: Compute $\Gamma = \langle V_j, E_j \rangle$, a graph with vertices, V_j, 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 $Q[x]/f(x) \cap Q[x]/g(x)$

It follows from Lemmas 3.10 and 3.11 that Algorithm 3.2 correctly computes a polynomial whose coefficients determine the intersection of $Q[x]/f(x)$ with $Q[x]/g(x)$. The running time of Algorithm 3.2 is dominated by the time required by the factorization required in Step 2. The proof is quite similar to that of Theorem 3.9, and we do not repeat it here.

Theorem 3.12: If $f(x)$ in $Z[x]$ is monic and irreducible of degree n, and $h(x) \in Q[z, x]/f(z)$ is an irreducible factor of $g(x)$, a monic irreducible polynomial over Z, then Algorithm 3.2 determines the intersection of $Q[x]/f(x)$ and $Q[x]/g(x)$, where $Q[x]/f(x)$ and $Q[x]/g(x)$ are contained in $Q[x, y]/(f(x), h(y))$. Suppose the degree of $h(x)$ is m. Then Algorithm 3.2 works in $O(F(\log \|f(z)\|, n, \log |(N_{(Q[x]/f(x))/Q} h(x - cz))|, (nm)^2))$ steps, where c is an integer less than $(mn)^2$.

Chapter IV

Determining Solvability

1. The Fields Between Q and $Q(\alpha)$

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

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

We define $F_1 = Q(\beta_0, \beta_1, \ldots, \beta_{k_1-1})$. In Lemma 4.1 we show that F_1 is the fixed field of G_{B_1}. Then the minimum polynomial for $\alpha = \alpha_1$ over F_1 is $h_1(x)$. This is easy to see, for

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

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

We first 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 $\{\alpha_1, \ldots, \alpha_{k_1}\}$) acts primitively on the roots of $h_1(x)$. This is shown in Lemma 4.1. 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 $\alpha_2, \ldots, \alpha_m$, 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 4.1: 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 $K(\alpha_1, \ldots, \alpha_m)^{G_B} = K(\text{symmetric functions in } \{\alpha_1, \ldots, \alpha_k\})$.

proof: We proceed by induction. Assume that B is a maximal block of roots containing α_1, and let F denote $K(\alpha_1, \ldots, \alpha_m)$. First we note that $[F : K] = [G/G_B] = |\Omega|/|B| = m/k$. The first equality follows from part (4) of the Fundamental Theorem of Galois Theory. The second is a consequence of the First Isomorphism Theorem applied to a mapping from G onto an induced action on $B, \sigma_2 B, \ldots, \sigma_l B$, a complete block system. It is clear that $K(\text{symmetric functions of } \{\alpha_1, \ldots, \alpha_k\}) \subseteq F$. We show that $[K(\text{symmetric functions of } \{\alpha_1, \ldots, \alpha_k\}) : K] = m/k$ to complete the proof.

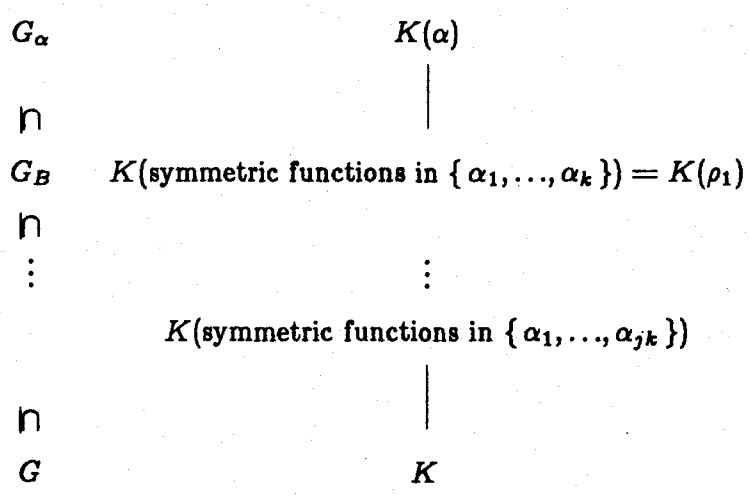

Figure 4.1: The Fields Between K and $K(\alpha)$ and Corresponding Groups

Let $a_0, a_1, \ldots, a_k$ be the symmetric functions evaluated at $\{\alpha_1, \ldots, \alpha_k\}$. Let $\rho_1 = a_0 + c_1 a_1 + \ldots + c_k a_k$ be a primitive element for $K(\text{symmetric functions in } \{\alpha_1, \ldots, \alpha_k\})$ over K, where the c_i's are in Z. (Note that the c's can be chosen less than m^3.) If we let $\rho_i = \sigma_i(\rho_1)$, then $p(x) = \prod_{i=1}^{m/k} (x - \rho_i)$ has coefficients over K. If $q(x)$ is a factor of $p(x)$ over K, then

$q(x) = \prod_j (x - \rho_j)$. In this case, $\sigma_{j_1}B \cup \ldots \cup \sigma_{j_l}B$ form a block, contradicting the maximality of the block B. We conclude that $p(x)$ is irreducible. Thus ρ_1 satisfies an irreducible polynomial of degree m/k over K, and $[K(\text{symmetric functions in } \{\alpha_1 \ldots \alpha_k\}) : K] = m/k$.

Now any block will be maximal over an appropriate subfield; assume inductively that B is a maximal block over $L = K(\text{symmetric functions in } \{\alpha_1 \ldots \alpha_{jk}\})$. Let H be the induced action of G on $\{\alpha_1 \ldots \alpha_{jk}\}$, $B = \{\alpha_1, \ldots, \alpha_j\}$ be the maximal block, and $F = L(\alpha_1, \ldots, \alpha_{jk})^{H_B}$. As before, $[F : L] = |H|/|H_B| = |\{\alpha_1, \ldots, \alpha_{jk}\}|/|\{\alpha_1 \ldots \alpha_k\}| = j$. If we define ρ_1 as a primitive element for F, it will satisfy an irreducible polynomial of degree j over L, by the same arguments as before. Thus

$$\begin{aligned} F &= L(\text{symmetric functions in } \{\alpha_1 \ldots \alpha_k\}) \\ &= K(\text{symmetric functions in } \{\alpha_1 \ldots \alpha_{jk}\}, \text{ symmetric functions in } \{\alpha_1 \ldots \alpha_k\}) \\ &= K(\text{symmetric functions in } \{\alpha_1 \ldots \alpha_k\}) \end{aligned}$$

since $\{\alpha_1, \ldots, \alpha_k\}$ is a subblock of $\{\alpha_1, \ldots, \alpha_{jk}\}$. ∎

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 the roots of $f(x)$. 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 4.1; 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 $g_i(y)$.

Of course we could determine F_1 by calling **BLOCKS** on $f(x)$. Then if

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

is the polynomial described earlier, $F_1 = Q(\beta_0, \ldots, \beta_{k-1})$, and $\rho_1 = \beta_0 + c_1\beta_1 + \ldots + c_{k-1}\beta_{k-1}$, each $c_i \in Z$, can be quickly found by Proposition 2.2.

Let $\sigma_1, \ldots, \sigma_j \in G$ be such that $\sigma_1 B_1, \ldots, \sigma_j B_1$, where σ_1 is the identity, form a complete block system for G acting on $\{\alpha_1, \ldots, \alpha_m\}$, 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 $\theta_i = \sigma_i(\rho_1)$, $i = 1 \ldots j$, then $\sigma_i(h_1(\rho_1)) = 0$, implies that $\sigma_i(\rho_1) = \theta_i$ is a root of $h_1(x)$. Applying **BLOCKS** to $g_1(x)$, returns a polynomial:

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

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

$$\begin{aligned} F_2 &= Q(\beta_{k_2-1}, \ldots, \beta_0) \\ &= Q(\text{symmetric functions in } \{\theta_1, \ldots, \theta_j\}) \\ &= Q(\text{symmetric functions in } \{\text{symmetric functions in } \{\alpha_1, \ldots, \alpha_{k_1}\}, \ldots \\ &\qquad \ldots, \text{symmetric functions in } \sigma_j\{\alpha_1, \ldots, \alpha_{k_1}\}\}). \end{aligned}$$

But $Q(\beta_{k_2-1}, \ldots, \beta_0)$ is a cumbersome way to name F_2; we would like to name F_2 in terms of the original roots of $f(x)$, $\alpha_1, \ldots, \alpha_m$. Fortunately, there is a simple way to do this.

Lemma 4.2: 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.

proof: Because the fields $Q(\tau), Q(\rho)$ are subfields of $Q(\alpha)$, we know that $Q(\rho) = Q(\text{symmetric functions in elements of } B)$, $Q(\tau) = Q(\text{symmetric functions in elements of } B_2)$, and 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 $B_1 \subset B_2$. We consider the induced action of G on B_2, and let $\sigma_1 B_1, \ldots, \sigma_{k_2} B_1$ 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,

$$\begin{aligned} N_{Q(\rho)/Q(\tau)}(h_1(x)) &= \prod_{i=1}^{k_2} \sigma_i(h_1(x)) \\ &= \prod_j \sigma_j\Big(\prod_{\substack{\alpha_i \in \text{minimal} \\ \text{block ctg } \alpha=\alpha_1}} (x-\alpha_i)\Big) \\ &= \prod_j \prod_{\substack{\alpha_i \in \text{minimal} \\ \text{block ctg } \alpha=\alpha_1}} \sigma_j(x-\alpha_i) \\ &= \prod_{i=1}^{k_1 k_2} x-\alpha_i \end{aligned}$$

will give a polynomial whose roots $\alpha_1, \ldots, \alpha_{k_1 k_2}$ are a block of $\alpha_1, \ldots, \alpha_m$ which contains $\alpha_1, \ldots, \alpha_{k_1}$. 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 $\alpha_1, \ldots, \alpha_m$ directly. Recall that the coefficients of $B(x)$, $\beta_{k_2-1}, \ldots, \beta_0$ are elements of $Q[y]/h_1(y) = Q(\rho)$, and that $Q(\beta_{k_2-1}, \ldots, \beta_0)$ $= Q(\tau)$ is a subfield of $Q(\rho)$. If $\gamma_0, \ldots, \gamma_{jk-1}$ are the symmetric functions in $\alpha_1, \ldots, \alpha_{k_1 k_2}$, again we can determine

$$\rho_2 = \gamma_0 + c_1\gamma_1 + \ldots + c_{k_1 k_2}\gamma_{k_1 k_2},$$

where $Q(\rho_2) = Q(\gamma_0, \ldots, \gamma_{k_1 k_2})$, 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 $F_k = Q$.

We give a simple argument to show that the $h_i(x)$ have succinct descriptions. Although the bound we give is not best possible, it is an easy argument which demonstrates that the polynomials have polynomial size descriptions. The polynomial $f(x)$ is monic with coefficients in Z, which means that $\alpha_1, \ldots, \alpha_m$ are algebraic integers. Since any sum or product of algebraic integers is also an algebraic integer, we know that the roots of $h_1(x)$ and $h_2(x)$ are algebraic integers. Therefore it suffices to show that $[\![h_i(x)]\!]$ is polynomially bounded in order to know that $h_i(x)$ is polynomially bounded in length of description. Now $h_i(x)$ is the minimal polynomial for $\rho_i = \beta_0 + c_1\beta_1 + \ldots + c_k\beta_k$ over Z, where the β_i are symmetric functions of the $\alpha_1, \ldots, \alpha_m$, and $k < m$. Then

$$\begin{aligned}
[\![\beta_i]\!] &\leq [\![\sum_{\substack{\text{all subsets of} \\ k \text{ distinct roots}}} \prod_{\substack{\alpha_{i_j} \in \\ \{\alpha_1, \ldots, \alpha_m\}}} \alpha_{i_1} \cdots \alpha_{i_k}]\!] \\
&\leq 2^m [\![\prod_{\alpha_{i_j} \in \{\alpha_1, \ldots, \alpha_m\}} \alpha_{i_1} \cdots \alpha_{i_k}]\!] \\
&\leq 2^m [\![\alpha]\!]^m.
\end{aligned}$$

This yields the following bound on the ρ_i's:

$$[\![\rho_i]\!] \leq m \cdot \max_i |c_i| \max_i [\![\beta_i]\!] \leq m \cdot m^4 \cdot 2^m [\![\alpha]\!]^m = M.$$

If

$$h_i(x) = \prod_{\substack{\rho_j \text{ a conjugate} \\ \text{of } \rho_i \text{ over } Q}} (x - \rho_j),$$

we conclude that $[\![h_i(x)]\!] \leq (2M)^m$. Using Weinberger and Rothschild [Theorem 1.3], we can also obtain a bound on the coefficients of $g_i(y)$. Recall that

$$g_i(y) = \prod_{\substack{\alpha_i \text{ a conjugate} \\ \text{of } \alpha_1 \text{ over } Q(\rho_i)}} (y - \alpha_i)$$

Thus if $g_i(y) = y^k + \gamma_{k-1}y^{k-1} + \ldots + \gamma_0$, the γ_i's are algebraic integers, and are elements of $Q(\rho_i)$. With

$$\gamma_i = \left(\frac{1}{d}\right) \sum_{j=0}^{l-1} g_{ij}\rho^j$$

and d = disc$(h_i(x))$, by Theorem 1.3 we have

$$|g_{ij}| \leq m! [\![f(x)]\!]^m |h(x)|^{m^2} \leq m! [\![f(x)]\!]^{3m^2},$$

a rough bound which is sufficient for our purposes. Since $[\![\rho_i]\!] \leq M$,

$$\text{disc}(h_i(x)) \leq (2M)^{m^2} \leq [\![f(x)]\!]^{m^3},$$

and consequently,

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

We have shown:

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

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

In the next section we present an algorithm for determining the $h_i(x)$ and $g_i(y)$, along with a proof of correctness and an analysis of running time.

2. An Algorithm

Algorithm 4.1 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: $C^x(t) \leftarrow t^k + q_{k-1}(x)t^{k-1} + \ldots + q_0(x)$
[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: $B^x(t) \leftarrow$ BLOCKS$(h_i(x))$;
$t^l + b_{l-1}(x)t^{l-1} + \ldots + b_0(x) \leftarrow B^x(t)$

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

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

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

Step 17: $i \leftarrow i + 1$

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

Theorem 4.3: Let $f(z) \in Z(z)$ of degree m be irreducible. Algorithm 4.1 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 $[\![g(x)]\!] \leq m![\![f(x)]\!]^{m^2}$.

proof: We consider the first iteration of Algorithm 4.1. Step 1 computes $C^z(t) = t^l + c_{l-1}t^{l-1} + \ldots + c_0(z)$, whose roots $z_1, \ldots, z_k$ form a minimal block of imprimitivity containing $z = z_1$. If $C^z(t) \in Q[t]$, then the Galois group of $f(z)$ over Q acts imprimitively on the roots of $f(z)$, and we are done. Otherwise we compute a primitive element for $\beta(z)$ for the field $Q[a_{k-1}(z), \ldots, a_0(z)]/f(z)$ in Steps 4 and 5. That Steps 4 and 5 do so correctly is immediate from van der Waerden [vdW,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 $Q[t]/h_0(t) \simeq Q[x,y]/(h_1(x), g_0(y))$. Steps 11 and 12, in the case of $i = 1$, 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**$(h_1(x)) = t^k + b_{k-1}(x)t^{k-1} + \ldots + b_0(x) = B^x(t)$. 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 $Q[b_{k-1}(x), \ldots, b_0(x)]/h_1(x) = Q($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 4.2, and the discussion which followed it. Since x is a root of $B^x(t)$, the roots of

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

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 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 Algorithm 4.1 has computed $\{\, h_i(x), g_{i-1}(y) \mid i = 1,\ldots,k \,\}$ 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 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 will show that a single iteration of Algorithm 4.1 will produce $h_{k+1}(x), g_k(y)$, 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 $z_1,\ldots,z_m$, and we have satisfied conditions 1,2,3, and 4. Suppose $C^z(t) \notin Q[t]$. Then in Steps 3-5 we compute a primitive element, $\beta(z)$, for Q(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 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 is however, 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 $g_k(y)$ 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 subfield by calling **BLOCKS** on $h_{k+1}(x)$; the subfield is determined by the symmetric functions 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 4.2 the polynomial we are seeking is:

$$N_{\left(Q[x]/h_{k+1}(x)\right)/\left(Q[b_{k+1}(x),\ldots,b_0(x)]/h_{k+1}(x)\right)}C^x(t)$$
$$= N_{\left(Q[\beta(z)]/f(z)\right)/\left(Q[b_{k+1}(x),\ldots,b_0(x)]/h_{k+1}(x)\right)}C^x(t)$$
$$= Res_x(B^z(x), C^x(t))$$
$$= C^z(t).$$

We are done. Let us now examine the running time.

Observe that Algorithm 4.1 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 computation $a_j(z) \in ?\{1, \beta(z), \ldots, \beta^{m-1}(z)\}$ 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 to test independence; the bound is due to [Edm.]) 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 same factor, and there are at most $\log m$ of them. Hence we conclude that the running time for **FIELDS** is less than $O(\log m BLOCKS(g(x)))$, where degree$(g(x)) \leq m$, and $[\![g(x)]\!] \leq [\![f(x)]\!]^{m^2}$. ∎

3. The Fields Between Q and $Q(\alpha)$ and Solvability

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 $Q(\beta_i)$.

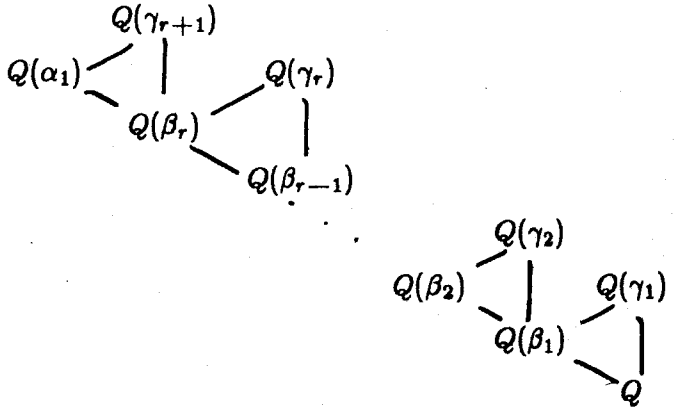

Figure 4.2: The Primitive Extensions Between Q and $Q(\alpha)$

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 $i = 1, \ldots, r$.

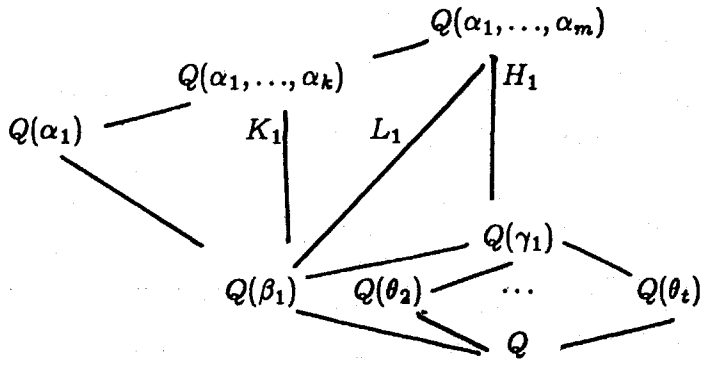

Figure 4.3: $H_1 \subseteq K_1^t$

This is suprisingly easy to answer, for primitive solvable groups are highly structured, which greatly limits their size.

Theorem 4.4 [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. In Section 4 we present this algorithm with a proof of correctness and an analysis of running time.

4. Another Algorithm

Algorithm 4.2 GALOIS

input: $f(x) \in O_K[x]$, monic, irreducible of degree m over $K = Q(\theta)$, where θ is an algebraic integer of degree l over Q, and O_K is the ring of integers of K

Step 1: $g(y) \leftarrow f(y)$

Step 2: Find $c \neq 0$ such that $N_{\left(K[y]/g(y)\right)/K}(f(x-cy))$ is squarefree
[Then $N_{\left(K[y]/g(y)\right)/K}(f(x-cy))$ generates $K(\alpha,\beta)$ where α and β are roots of $g(y)$ and $f(x)$ respectively.]

Step 3: Factor $N_{\left(K[y]/g(y)\right)/K}(f(x-cy)) = \prod_{j=1}^{k} G_j(x)$ over K

Step 4: If there is a $G_j(x)$ such that degree$(G_j(x))$>degree$(g(x))$,
$g(y) \leftarrow G_j(y)$ and go to 2
Else $n \leftarrow$degree$(g(y))$

Step 5: For $i = 1,\ldots,m$, do:
$f_i(x) \leftarrow \gcd_{K[y]/g(y)}(G_i(x+cy), f(x))$
$q_i(y) \leftarrow$ constant term of $f_i(x)$

Step 6: Factor $g(x) = \prod_{i=1}^{n} x - p_i(y)$

Step 7: For $i = 1,\ldots,n$, do:

Step 8: For $j = 1,\ldots,m$, do:
If $p_i(q_j(y)) = q_l(y)$ in $Q[y]/g(y)$, $\tau_i(j) \leftarrow l$
[This just means that $\sigma_i(\alpha_j) = \alpha_l$, for α_j, α_l roots of $f(x)$]

return: $\{\tau_i \mid i = 1,\ldots,n\}$, and $g(y)$, where
1) $K[y]/g(y)$ is the splitting field for $f(x)$ over K, and
2) The τ_i's acting on $\alpha_1,\ldots,\alpha_m$, the roots of $f(x)$, form the Galois group of $f(x)$ over K

Theorem 4.5: 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 4.2 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.

proof: The proof will be by induction. As before, we show correctness, and then analyze running time. Without loss of generality, let us assume the roots of $f(x)$, $\alpha_1,\ldots,\alpha_m$, are ordered so that there is a $t \leq m$, with $\alpha_{i+1} \notin K(\alpha_1,\ldots,\alpha_i)$ for $i<t$, and $\alpha_{i+1} \in$

$K(\alpha_1, \ldots, \alpha_i)$ for $i \geq t$. Each time we adjoin a root α_{i+1} of $f(x)$ to $K(\alpha_1, \ldots, \alpha_i)$, we will compute a primitive element for $K(\alpha_1, \ldots, \alpha_{i+1})$ over K, and a minimal polynomial for that element. In the algorithm we call these "y" and "$g(y)$" respectively; in the proof we call the i^{th} primitive element β_i, and its minimal polynomial over K, $g_i(y)$. Recall Proposition 2.2 which says that if $G_j(x)$ is an irreducible factor of $N_{\left(K(y)/g(y)\right)/K}(f(x - cy))$, then $K[z]/G_j(z) \simeq K[x, y]/(g(y), f_j(x))$. We observe that it is not really necessary to factor $f(x)$ over $K(\beta)$ in order to determine if $f(x)$ splits into linear factors in that field. For, if $g(y)$ of degree l is the minimal polynomial for β over K, and $h(x) \in K[x, y]/g(y)$ is of degree k, then $N_{\left(K[y]/g(y)\right)/K}(h(x))$ is a polynomial of degree lk over K. In particular, if $G_j(x)$ is an irreducible factor of $N_{\left(K[y]/g(y)\right)/K}(f(x - cy))$ in $K[x]$ which is of degree $m >$ degree$(g(y))$, then $\gcd_{K[y]/g(y)}(G_j(x + cy), f(x))$ is nonlinear. This observation will save us the work of factoring $f(x)$ until we reach a splitting field for $f(x)$ over K. We are now ready to proceed with the proof.

We claim that each iteration of Steps 2-4 adjoins a root α_i of $f(x)$ to K and computes a primitive element, β_i, for $K(\alpha_1, \ldots, \alpha_i)$ over K. Suppose first that $f(x)$ is normal, that is, $f(x)$ factors completely in $K[y]/f(y)$. In that case each of the $G_i(x)$'s will be of the same degree as $f(y) = g(y)$, and we will fall through to the second part of the algorithm.

Next suppose that $f(x)$ is not normal, and adjoin a single root of $f(x)$ to K. Then at least one of the irreducible factors of $f(x)$ in $K[x, y]/f(y)$ is not linear. If $f_j(x)$ is such a factor, then $G_j(x) = N_{\left(K[y]/g(y)\right)/K}(f_j(x - cy))$ is a factor of $N_{\left(K[y]/g(y)\right)/K}(f(x - cy))$ whose degree is greater than the degree of $g(y)$. On the first iteration of Steps 2-4 let β be a root of $G_j(x)$, where $\beta = \alpha_1 + c\alpha_2$, where c is an integer less than $(m^2 l)^2$. By Proposition 2.2, $K(\beta) = K(\alpha_1, \alpha_2)$. On subsequent iterations β_{i+1} will be a root of (the new) $G_j(x)$, an irreducible factor of $N_{\left(K[y]/g(y)\right)/K}(f(x - cy))$. Then

$$K[y]/g(y) \simeq K[y]/G_j(y) \simeq K(\beta_{i+1}) \simeq K(\beta_i, \alpha_{i+1})$$

by induction. We fall through to Step 5 only when $f(x)$ factors into linear factors in $K[y]/g(y)$; equivalently, when we have adjoined $\{\alpha_1, \ldots, \alpha_t\}$ to K, and have computed a primitive element y for $K(\alpha_1, \ldots, \alpha_t)$ over K. Then $K[y]/g(y)$ is the splitting field of $f(x)$ over K.

In Step 5, we factor

$$f(x) = \prod_{i=1}^{m} f_i(x) = \prod_{i=1}^{m} (x - q_i(y))$$

over $K[y]/g(y)$. In Step 6 we factor

$$g(x) = \prod_{i=1}^{n} (x - p_i(y)).$$

(By the construction of $g(y)$, we know that $g(x)$ splits completely in $K[y]/g(y)$.)

The Galois group of $g(x)$ over K, G, is a group of order n acting on n elements; thus for each $i = 1, \ldots, n$ there is a unique $\sigma_j \in G$ with $\sigma_j(1) = i$. The Galois group of $f(x)$ over K is the induced action of G on the roots of $f(x)$, $\alpha_1, \ldots, \alpha_m$, which we write as $q_1(y), \ldots, q_m(y)$. Without loss of generality we assume that $\sigma_j(1) = i$. An alternative way to say this is that $\sigma_i(y) = p_i(y)$. Then $q_i(y)$ is the constant term of the $f_i(x)$, $\sigma_i(\alpha_j) = \sigma_i(q_j(y)) = p_i(q_j(y))$. Let $\{\tau_i \mid i = 1, \ldots, n\}$ be the induced action of G on $\alpha_1, \ldots, \alpha_m$, so that $\tau_i(j) = l$ iff $p(q_j(y)) = q_l(y)$. Thus Algorithm 4.2 returns the set $\{\tau_i\}$ which form the Galois group of $f(x)$ over K.

The running time analysis breaks up into two parts, just as the proof of correctness did. First we consider the time needed for Steps 1-4, which calculates β_i and $g_i(y)$. Let $n_i = [K(\alpha, \ldots, \alpha_i) : K]$, and $d_i = [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]$. We first bound the size of $g_i(y)$. The roots of $g_i(y)$ are conjugates over K of $\alpha_1 + c_2\alpha_2 + \ldots + c_i\alpha_i$, where $c_i \in Z$. By Lemma 1.6 $|c_i| \leq (d_i n_{i-1})^2 = n_i^2$. Then

$$\begin{aligned} [\![\alpha_1 + c_2\alpha_2 + \ldots + c_i\alpha_i]\!] &\leq [\![\alpha]\!](1 + c_2 + \ldots + c_i) \\ &\leq [\![\alpha]\!] i|c_i|, \text{ since } c_j < c_i \text{ for } j < i \\ &\leq [\![\alpha]\!] n_i^3. \end{aligned}$$

If $k(x)$ is the minimal polynomial for θ over Q, $|k(x)| \leq (2[\![\theta]\!])^m$. Then

$$[\![g_i(y)]\!] \leq (2[\![\alpha]\!] n_i^3)^{n_i^3} (2[\![\theta]\!]) m^3$$

by Weinberger and Rothschild [Theorem 1.3.] We further conclude that

$$[\![N_{(K[y]/g_i(y))/K}(f(x - cy))]\!] \leq (2[\![\alpha]\!] n_{i+1}^3)^{n_i+1} (2[\![\theta]\!])^m.$$

Let D_i be the time needed by Algorithm 4.2 on the i^{th} iteration. Then $T_i = D_i + D_{i-1} + \ldots + D_1$. We claim $D_i \leq 3(n_{i+1} l)^{9+\epsilon} (n_{i+1} \log n_i [\![f(x)]\!] + l^3 \log [\![\theta]\!])^{2+\epsilon}$. This is

because Steps 2-4 are dominated by the time it takes to factor $N_{(K[y]/g(y))/K}(f(x-cy))$ over K. By Propositon 2.1, the claim follows. Then

$$T_i \leq 3(n_{i+1}l)^{9+\epsilon}(n_{i+1}\log n_i[\![f(x)]\!] + l^3\log[\![\theta]\!])^{2+\epsilon} + 3(n_il)^{9+\epsilon}(n_i\log n_{i-1}[\![f(x)]\!] + l^3\log[\![\theta]\!])^{2+\epsilon} + \ldots \ldots + 3(n_1l)^{9+\epsilon}(n_1\log m[\![f(x)]\!] + l^3\log[\![\theta]\!])^{2+\epsilon}.$$

The time required by Algorithm 4.2 in Steps 2-4 is bounded by $O((|G|l)^{9+\epsilon}(|G|\log|G|[\![f(x)]\!] + l^3\log[\![\theta]\!])^{2+\epsilon})$.

Since $[\![f(x)]\!]$ and $[\![g(y)]\!]$ are both smaller than $[\![N_{(K[y]/g(y))/K}(f(x-cy))]\!]$, Steps 5 and 6 do not add to the time bound established for Steps 1-4. Similarly the computations of Steps 7 and 8, being straightforward divisions of polynomials ($n|G|$ of them), do not increase the running time of Algorithm 4.2. Consequently Algorithm 4.2 computes $g(y)$ and $\{\tau_i \mid i = 1,\ldots,n\}$ in $O((|G|l)^{9+\epsilon}(|G|\log|G|[\![f(x)]\!] + l^3\log[\![\theta]\!])^{2+\epsilon})$ steps. ∎

5. How it Fits Together

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 4.1.] 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. How does it all fit 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. We call **GALOIS** 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 4.4, 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 for

$$(a\ constant)n_{i-1}^{30}degree(h_i(y))^{9+\epsilon}(n_i^{3.25}\log n_i[\![g_{i-1}(y)]\!] + (degree(h_i(x))^3\log[\![h_i(x)]\!])^{2+\epsilon}$$

$= k_i$ steps, the time needed by GALOIS to determine a Galois group of order 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 4.3 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: 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"

return: $f(x)$ IS SOLVABLE BY RADICALS if $f(x)$ is solvable by radicals,
$f(x)$ IS NOT SOLVABLE BY RADICALS otherwise

We conclude with the main result of this thesis:

Theorem 4.6: Let $f(x) \in Z[x]$ be monic and irreducible of degree m over Q. Then Algorithm 4.2 determines whether the roots of $f(x)$ are expressible in radicals in time polynomial in m and $\log |f(x)|$.

Chapter V

Expressibility

1. Background

We recall:

The Fundamental Theorem on Equations Solvable by Radicals:

(1) If one root of an irreducible equation $f(x)$ over a field K can be represented in the form:

$$\sqrt[g]{\sqrt[h]{p}+\sqrt[c]{\cdots}} \qquad (*)$$

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 of the form (*) in such a way that in the successive adjunctions of $\sqrt[n]{a}$, the exponents are prime numbers, and the equations $x^n - a$ are irreducible each time.

For the first four chapters of this thesis, we were concerned with the problem of determining solvability of an irreducible polynomial over the rationals. 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 chapter we exhibit a straight line program which does

so in polynomial time. Classical results are presented in §1, and a discussion on bounds appears in §2. The straight line program is presented in the final section of this chapter.

Let K be an algebraic number field which contains the n^{th} roots of unity. Then $K(\sqrt[n]{a})$ is a Galois extension of K, and the map $\sqrt[n]{a} \mapsto \zeta_n \sqrt[n]{a}$, where ζ_n is a primitive n^{th} 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 n^{th} root of unity. For each element γ in $K(\alpha)$ we can form the *Lagrange resolvent*:

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

The Lagrange resolvent is a K-linear map from $K(\alpha)$ onto itself, and can be thought of as a matrix. Then $(\zeta, \gamma) = 0$ iff γ is in the null space of this matrix. The following theorem shows that the Lagrange resolvent does not act trivially on $K(\alpha)$.

Theorem 5.1 [E.Artin]: The elements of the Galois group of $K(\alpha)$ over K are linearly independent over K.

proof: It is clear that if $a\sigma(x) = 0$ for $x \neq 0$, then $a = 0$. Suppose there is a relation

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_m\sigma_m(x) = 0 \tag{1}$$

with none of the $a_i = 0$. Let m be chosen as small as possible. Then we know $m \geq 2$. Since σ_1 and σ_2 are distinct, there is a b in K such that $\sigma_1(b) \neq \sigma_2(b)$. (Note that this means $\sigma_1(b) \neq 0$.) We have

$$a_1\sigma_1(bx) + a_2\sigma_2(bx) + \ldots + a_m\sigma_m(bx) = 0 \tag{2}$$

which implies

$$a_1\sigma_1(x)\sigma_1(b) + a_2\sigma_2(x)\sigma_2(b) + \ldots + a_m\sigma_m(x)\sigma_m(b) = 0. \tag{3}$$

We divide equation (3) by $\sigma_1(b)$, and subtract it from equation (1). The first term cancels, and we obtain:

$$(a_2\frac{\sigma_2(b)}{\sigma_1(b)} - a_2)\sigma_2(x) + \ldots + (a_m\frac{\sigma_m(b)}{\sigma_1(b)} - a_m)\sigma_m(x) = 0 \tag{4}$$

Because the first term in equation (4) is not zero, this is a relation of shorter length than equation (1), which was chosen to be minimal. Thus it must be the case that $\sigma_1, \ldots, \sigma_n$ are linearly independent over K. ∎

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

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

This means that $(\zeta, \gamma)^n$ is fixed by σ, and thus that $(\zeta, \gamma)^n$ is in K. But we also know from (**) 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 5.2: 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 5.2. Clearly roots of unity play a special role in the question of expressibility, and we show:

Lemma 5.3: The p^{th} roots of unity, p a prime, are expressible as "irreducible radicals" over K.

proof: We do this by induction on p. If $p = 2$, the roots of unity are ± 1, and there is nothing to show. Suppose we have shown the lemma to be true for all primes less than p. Now the field with the p^{th} roots of unity is cyclic of order $p - 1 = p_1^{a_1} \ldots p_k^{a_k}$ over K. We adjoin to K the $p_1^{th}, \ldots, p_k^{th}$ roots of unity which by induction we have assummed to be expressible as radicals over K. Then Theorem 5.2 applies. ∎

2. Bounds

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 Chapter IV 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 $Q(\beta_{i+1})$. (See Figure 4.2.) In light of Theorem 5.2, we find it necessary to 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. The proof is similar to that for expressing β_i as radicals in polynomial time, and we begin by proving the bound for the β_i's. We find elements $\tilde{\beta}_i$ such that $Q(\tilde{\beta}_i) = Q(\zeta_l, \beta_i)$. In order to prove that we can express $\tilde{\beta}_i$ by a straight line program in polynomial time, we must first obtain bounds on $[\![\tilde{g}_i(x)]\!]$ and $[\![\tilde{k}_i(y)]\!]$, the minimal polynomials for $\tilde{\beta}_i$ over $Q(\tilde{\beta}_{i+1})$ and for $\tilde{\gamma}_i$ over $Q(\tilde{\beta}_i)$ respectively. The bounds we present are not best possible; they are simplified for the sake of readability.

Lemma 5.4: If $\tilde{h}_i(x)$ is the minimal polynomial for $\tilde{\beta}_i$ over Q, then $|\tilde{h}_i(x)| \leq |f(x)|^{m^6}$. If $\tilde{g}_i(x)$ is the minimal polynomial for $\tilde{\beta}_i$ over $Q(\tilde{\beta}_{i+1})$, then $[\![\tilde{g}_i(x)]\!] \leq |f(x)|^{m^{12}}$.

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 $x^{l-1} + x^{l-1} + \ldots + 1$ over $Q[x]/h_{i+1}(x)$. By Weinberger and Rothschild [Theorem 1.3], $[\![z(y)]\!] \leq m_i! |h_{i+1}(x)|^{m_i^2}$.

The roots of $h_{i+1}(x)$ are symmetric functions in a block of roots of $f(x)$, which means that $|h_{i+1}(x)| \leq |f(x)|^m$. Thus $[\![z(y)]\!] \leq m_i! |f(x)|^{m m_i^2}$. We can now use Proposition 2.2 to determine 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

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

Now $\tilde{g}_i(y)$ will be a factor of $g_i(y)$, the polynomial described in Algorithm 4.3. Since $g_i(y)$ is an irreducible factor of $h_i(y)$, we have

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

This implies that

$$\begin{aligned}[\![\tilde{g}_{i+1}(y)]\!] &\leq m!(|f(x)|^{m^9})^{m^2}|h_{i+1}(x)|^{m^2} \\ &\leq m!|f(x)|^{m^{11}}|f(x)|^{m^8} \\ &< |f(x)|^{m^{12}}.\end{aligned}$$

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

Lemma 5.5: If $\tilde{k}_i(x)$ is the minimal polynomial for $\tilde{\gamma}_i$ over $Q(\tilde{\beta}_{i+1})$, then $[\![\tilde{k}_i(x)]\!] \leq |f(x)|^{m^9}$.

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

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

over $Q(\beta_{i+1})$, where $\theta_2, \ldots, \theta_t$ are the conjugates of β_i over $Q(\beta_{i+1})$, and the c_i's are integers less than m^3. Then by Weinberger and Rothschild [Theorem 1.3],

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

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

$$\begin{aligned}[\![\tilde{k}_i(x)]\!] &\leq m!([\![k_i(x)]\!])^m|h_{i+1}(x)|^{m^2} \\ &\leq m!|f(x)|^{m^8}(|f(x)|^{m^6})^{m^2} \\ &< |f(x)|^{m^9}.\end{aligned}$$

∎

In order 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 $\log|f(x)|$, then the former can also be solved in polynomial time, since there are at most $\log m$ 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 $\{e\} = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_r = H$, where H_k is normal in H_{k+1}, and H_{k+1}/H_k is of prime order [Sims],[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 do this using Proposition 2.2. 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 $[\![b_j]\!] \leq [\![\tilde{\gamma}_i]\!]^{m^3} < (|f(x)|^{m^7})^{m^3} = |f(x)|^{m^{10}}$. We let $\theta_k = b_0 + c_1 b_1 + \ldots + c_{l-1}b_{l-1}$, $c_i \in Z$, be a primitive element by using Proposition 2.2 in the usual way. Then $[\![\theta_k]\!] < (m^7|f(x)|^{m^{10}})$, and if $\tilde{j}_k(x)$ is the minimal polynomial for θ_k over Q,

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

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

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

We conclude:

Lemma 5.6: Let $\tilde{j}_k(x)$ be the minimal polynomial for θ_k over Q. Then $|\tilde{j}_k(x)| \leq |f(x)|^{m^{14}}$.If $i_k(x)$ is the minimal polynomial for θ_k over $Q(\tilde{\beta}_{k-1})$, then $[\![\tilde{i}_k(x)]\!] < |f(x)|^{m^{21}}$.

3. A Straight Line Program

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.

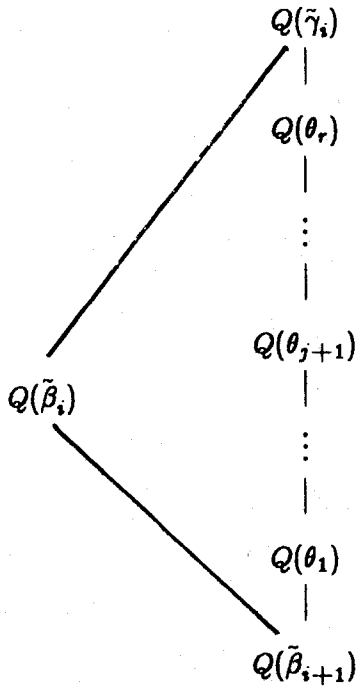

Figure 5.1: The Cyclic Extensions Between $Q(\tilde{\beta}_{i+1})$ and $Q(\tilde{\gamma}_i)$

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 necessary to also construct $q_j(x, y) \in Q[x, y]$, $j = 0, \ldots, s$, where $\theta_{j+1} = q_j(\sqrt[d_j]{p_j(\theta_j)}, \theta_j)$. 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 that how to express α over $Q(\zeta)$ in a straight line program in polynomial time. Finally ζ will be expressed in a similar way.

We proceed by induction, beginning with η_1. Consider the Lagrange resolvent of $Q(\theta_1)$ over $Q(\tilde{\beta}_{i+1})$, 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

$$[\![r_1(x)]\!] \leq ((d_1[\![\theta_1]\!])^{d_1})^{d_1^3} = (d_1[\![\theta_1]\!])^{d_4}$$

[Edm.] 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, and we conclude by Weinberger and Rothschild [Theorem 1.3] 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

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

By Lemma 5.6, $|\tilde{j}_o(x)| < |f(x)|^{m^{14}}$, and $[\![\theta_1]\!] < |f(x)|^{m^{14}}$. By a rough approximation using Weinberger and Rothschild, we find

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

Next we determine and bound $q_1(x, y)$. Our argument is that the minimal polynomial for θ_1 over Q is of bounded size (Lemma 5.6), and thus its factors over $Q(\theta_0)$ are also bounded. We find an integer c_1 such that $\nu_1 = \theta_0 + c_1 \sqrt[d_1]{\eta_1}$ is a primitive element for $Q(\theta_1)$ over Q. Then ν_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 $\theta_1 = t_1(\nu_1)$ has polynomial size coefficients. Furthermore the polynomial $q_1(x, y) \in Q[x, y]$ such that $\theta_1 = q_1(\sqrt[d_1]{\eta_1}, \theta_1) = t_1(y + c_1 x)$ also has polynomial size coefficients.

For the inductive step it suffices to replace 0 by i, and 1 by $i + 1$, because all of our bounds are a priori established by Lemmas 5.4-5.6. 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 $l_i(x) \in Q[x]$, then the coefficients of $l_i(x)$ are polynomial in size. This follows 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 5.7: 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 5.3 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 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 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, the following theorem suggests that this may not possible, at least for roots of unity.

Theorem 5.8 [Shapiro]: Let $c(x)$ be such that $\varphi^{c(x)}(x) = 2$ for $x > 2$. Then $2^{c(x)} < x \leq 2 \cdot 3^{c(x)}$.

Shapiro's function $C(x)$ is the number of field extensions we need to write $\varphi(x)$ as radicals over Q. Then $C(x) = O(\log x)$. The field which contains ζ_l expressed in radicals will be of degree $l^{\log l}$ over Q, so there is little hope that the actual radical expression for ζ_l will be polynomial in size. This indicates that Theorem 5.7 may be the best we can do.

Questions, Conclusions, and More 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. 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 Chapter IV, 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) Can the running time for factoring polynomials over algebraic number fields (Algorithm 2.1) be improved?

3) In Chapter III 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 3.1 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 we used to determine solvability has the surprising

characteristic that it answers that question without even determining the order of the group. We ask:

4) 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 disc$(f(x))$ is a square in Q [Lang, pp.199-200.] 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], [Za2], 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 insights on this problem short of the results presented in this thesis, but we hope for, and would be delighted by, its solution.

Appendix

Suppose α satisfies an irreducible polynomial $g(t)$ of degree m over Q; then $1, \alpha, \ldots, \alpha^{m-1}$ form a basis for $Q(\alpha)$ over Q. Recall the matrix (b_{ij}) defined by:

$$\begin{aligned}
\beta &= a_{11} + a_{12}\alpha + \ldots + a_{1m}\alpha^{m-1} \\
\beta\alpha &= a_{21} + a_{22}\alpha + \ldots + a_{2m}\alpha^{m-1} \\
&\vdots \quad \vdots \quad \vdots \\
\beta\alpha^{m-1} &= a_{m1} + a_{m2}\alpha + \ldots + a_{mm}\alpha^{m-1}
\end{aligned}$$

for $\beta \in Q(\alpha)$. We define the *trace* of β, $\mathrm{Tr}(\beta)$, to be $\sum_{i=1}^{m} b_{ii}$. Note that this definition is independent of the choice of basis for $Q(\alpha)$ over Q. Observe also that $\mathrm{Tr}_{Q(\alpha)/Q}(\beta + \gamma) = \mathrm{Tr}_{Q(\alpha)/Q}(\beta) + \mathrm{Tr}_{Q(\alpha)/Q}(\gamma)$. We are now ready to prove:

Proposition 1.2: Let α be an algebraic integer satisfying $g(t)$, a monic irreducible polynomial over Z. Then the ring of algebraic integers of $Q(\alpha)$ is contained in $(1/d)Z[\alpha]$, where

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

proof: Let $\deg(g(t)) = m$; then $1, \alpha, \ldots, \alpha^{m-1}$ are a basis for $Q(\alpha)$ over Q. Furthermore $1, \alpha, \ldots, \alpha^{m-1}$ are all algebraic integers. Assume $f(x) = (x - \alpha)(x^{m-1} + \beta_{m-2}x^{m-2} + \ldots + \beta_0)$ in $Q(\alpha)[x]$, and let $\omega_i = \frac{\beta_i}{f'(\alpha)}$ for $i = 0, \ldots, m-1$, with $\beta_{m-1} = 1$. We claim $\mathrm{Tr}(\alpha^i \omega_j) = \delta_{ij}$.

Let

$$h_j(x) = \left(\sum_{i=1}^{m} \frac{f(x)}{x - \alpha_i} \frac{\alpha_i^j}{f'(\alpha_i)} \right) - x^j \qquad j = 0, \ldots, m-1.$$

We claim $\alpha_1, \ldots, \alpha_m$, are the roots of $h_j(x)$. Observe that

$$f'(x) = \sum_{l=1}^{m} \prod_{l \neq k} (x - \alpha_l).$$

Then

$$f'(\alpha_i) = \prod_{l \neq i} (\alpha_i - \alpha_l).$$

Since $\frac{f(x)}{(x-\alpha_i)} \frac{1}{f'(alpha_i)} = 1$, we are done. But this means that $h_j(\alpha_i) = 0$, for $i = 1, \ldots, m$. Because $h_j(x)$ is a polynomial of degree less than m, it must be the case that $h_j(x)$ is identically zero. That is to say,

$$\sum_{i=1}^{m} \frac{f(x)}{x - \alpha_i} \frac{\alpha_i^j}{f'(\alpha_i)} = x^j \qquad \text{for } j = 0, \ldots, m-1.$$

That $\mathrm{Tr}(\frac{f(x)}{x - \alpha_i} \frac{\alpha_i^j}{f'(\alpha_i)}) = x^j$ follows immediately, since the polynomials $\frac{f(x)}{x - \alpha_i} \frac{\alpha_i^j}{f'(\alpha_i)}$ are all conjugate, and the trace is additive. Then $\mathrm{Tr}\left(\beta_i x^i \frac{\alpha^j}{f'(\alpha_i)}\right) = x^j$ if $i = j$, and 0 otherwise. Thus $\mathrm{Tr}\left(\frac{\beta_i}{f'(\alpha_i)} \alpha^j\right) = \delta_{ij}$.

Let $d \neq 0$ be such that $d\frac{\beta_i}{f'(\alpha_i)}$ is an algebraic integer. Let $\gamma = a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \in Q(\alpha)$ be integral over Q (i.e. satsify an integer monic polynomial over Q.) Then $d\frac{\beta_i}{f'(\alpha)}\gamma$ is integral over Q, as is $\mathrm{Tr}\left(d\frac{\beta_i}{f'(\alpha)}\gamma\right) = da_i$. But $da_i \in Q$ implies $da_i \in Z$. Therefore $\gamma \in (1/d)Z(\alpha)$.

Since β_i is an algebraic integer, d is a divisor of $f'(\alpha)$. Then

$$\begin{aligned} f'(\alpha) &= \sum_i \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= \prod_{i \neq j} (\alpha_i - \alpha_j) \text{ since } \prod_{j \neq i} (\alpha_i - \alpha_j) = 0 \text{ for } 1 \neq 1 \\ &= (-1)^{\frac{m(m-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{m(m-1)}{2}} \mathrm{disc}(g(t)). \end{aligned}$$

This completes the proof. ∎

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.

[B-O] M. Ben-Or, "Probabilistic Algorithms in Finite Fields," *Proc. Twenty-second Annual IEEE Symposium on the Foundations of Computer Science,* 1981, pp. 394-398.

[Be] E.R. Berlekamp, *Algebraic Coding Theory,* McGraw-Hill, New York, 1968.

[Be2] E.R. Berlekamp, "Factoring Polynomials over Large Finite Fields," *Mathematics of Computation, 24,* 1970, pp. 713-735.

[Br] W.S. Brown, "On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors," *JACM, Vol. 18, No. 4,* October 1971, pp. 478-504.

[Br2] W.S. Brown, "The Subresultant PRS Algorithm," *ACM Transactions on Mathematical Software, Vol. 4, No. 9,* Sept. 1978, pp. 241-249.

[BT] W.S. Brown and J.F. Traub, "On Euclid's Algorithm and The Theory of Subresultants," *JACM, Vol. 18, No. 4,* Oct. 1971, pp. 505-514.

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

[Can] D.G. Cantor, "Irreducible Polynomials with Integral Coefficients Have Succinct Certificates," *Journal of Algorithms.*

[Co] G. Collins, "The Calculation of Multivariate Polynomial Resultants," *JACM, Vol. 18, No. 4,* Oct. 1971, pp. 515-532.

[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.

[Ka1] E. Kaltofen, "A Polynomial Reduction from Multivariate to Bivariate Polynomial Factorization," *Proc. Fourteenth Annual ACM Symposium on Theory of Computing,* 1982, pp. 261-266.

[Ka2] E. Kaltofen, "A Polynomial-Time Reduction from Bivariate to Univatiate Integral Polynomial Factorization," *Proc. Twenty-third Annual IEEE Symposium on Foundations of Computer Science,* 1982, pp. 57-64.

[KMS] E. Kaltofen, D.R. Musser, and B.D. Saunders, "A Generalized Class of Polynomials Which are Hard to Factor," *Proc. 1981 ACM Symposium on Symbolic and Algebraic Computation,* pp. 188-194.

[Kn] D. Knuth, *The Art of Computer Programming, Vol. II: Seminumerical Algorithms,* Addison Wesley, Mass., 1969.

[Kr] L. Kronecker, *Gründzige Einer Arithmetischen Theorie der Algebraischen Grössen,* Druck und Verlag von G. Riemer, Berlin, 1882.

[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.

[Lang2] S. Lang, *Algebraic Number Theory,* Addison-Wesley, Mass., 1970.

[L^3] 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.

[Mar] D. Marcus, *Number Fields,* Springer Verlag, New York, 1977.

[Ma] M.Marden, *Geometry of Polynomials,* American Mathematical Society, Providence, Rhode Island, 1966, p.123.

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

[Mi] M.Mignotte, "An Inequality about Factors of Polynomials," *Mathemtatics of Computation, Vol.28,* 1974, pp.1153-1157.

[Mu] D.R. Musser, "Multivariate Polynomial Factorization," *JACM Vol. 22,* 1975, pp. 291-308.

[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.

[Sa] P. Samuel, *Algebraic Theory of Numbers,* Kershaw Publishing, Ltd., London, 1972.

[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.

[Wei] P.J. Weinberger, "Finding the Number of Factors of a Polynomial," unpublished manuscript.

[WR] P. Weinberger and L. Rothschild, "Factoring Polynomials over Algebraic Number Fields," *JACM,* Dec. 1976, pp. 335-350.

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

[Weyl] H. Weyl, *Algebraic Theory of Numbers,* Princeton University Press, Princeton, N.J., 1940.

[Za1] H. Zassenhaus, "On Hensel Factorization,I," *Journal of Number Theory, Vol.1, No.1, July 1969,* pp.291-311.

[Za2] 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.