POLYNOMIAL TIME ALGORITHMS FOR GALOIS GROUPS

Susan Landau

Math Department

Wesleyan University

Middletown, CT. 06457

Abstract:

In this paper we present several polynomial time algorithms for Galois groups. We show:

(i) There are polynomial time algorithms to determine:

(a) if the Galois group of an irreducible polynomial over Q is a p-group.

(b) the prime divisors of the order of a solvable Galois group

(ii) Using the classification theorem for finite simple groups, there is a polynomial time algorithm to determine whether an irreducible polynomial over Q has Galois group S_n or A_n.

We consider several techniques for computing Galois groups, including the Chebatorev Density Theorem, and their applicability to polynomial time computations.

Introduction:

In a description of his algorithm to determine whether a polynomial has roots expressible in radicals, Galois wrote, "... the calculations are impractical." Galois's technique involved factoring a polynomial of degree n!. In the century and a half since Galois, research has concentrated on finding the group for polynomials of small degree. Very little work has been done on general techniques, in part because until recently algorithms

for factoring polynomials required exponential time. The discovery of a polynomial time algorithm for factoring polynomials over the rationals [L^3], and over algebraic number fields [AKL,La] enabled the developement of a polynomial time algorithm for determining solvability by radicals [LaMi.]

It is an easy matter to compute the Galois group of a polynomial f(x), a monic irreducible polynomial over Z; a simple bootstrapping algorithm which consists of factoring f(x) over K=Q[t]/f(t), adjoining a root of f(x) to K, computing a primitive element for this field over Q, and repeating this procedure until f(x) splits completely has a running time which is polynomial in the size of f(x) and the size of its Galois group [La.] And therein lies the difficulty. For if f(x) is of degree n over Q, its Galois group may be as large as S_n. What we seek is an algorithm which has running time a polynomial in the size of f(x).

Although S_n has n! elements, its generating set is polynomial in size. In fact, a transitive group on n elements has a generating set of no more than 2n elements [Ba], thus allowing the possibility of construction of Galois groups in time polynomial in the size of f(x).

In [LaMi] we gave a polynomial time algorithm to determine if f(x), a monic irreducible polynomial over Z, has roots expressible in radicals. We checked the solvability of the Galois group without actually determining the group, its order or structure. In this paper we explore those problems, and give polynomial time solutions to certain questions. Our result in [La Mi] relied heavily on the divide-and-conquer techniques of primitive permutation groups, and we use these ideas again in this paper.

Finite simple groups are the building blocks of finite groups. The success of group theorists is classifying all finite simple groups will undoubtedly bear fruit in many settings; it does so already in the computational one of this paper. Theorems dependent on the classification of finite simple groups will be marked (S.) This paper is organized as follows: II Background, III Polynomial