THE COMPUTATION OF GALOIS GROUPS

Leonard SOICHER

No.: MPA V4

Cet article est une copie de la thèse de Leonard Soicher acceptée pour l'obtention du grade "Master of Computer Science" à l'Université Concordia, Montréal, P. Québec, le 16 avril 1981.

ABSTRACT

THE COMPUTATION OF GALOIS GROUPS

Leonard Soicher

We discuss methods of computing invariants of the conjugacy class of the Galois group of a separable polynomial f(x) over K, n = deg(f) > 0. The aim is to determine the class of Gal(f/K) in S_n. We concentrate on the case K = Q and f(x) is irreducible over K.

The main tool discussed is the resolvent polynomial. For F in $K[x_1,\ldots,x_n]$, the factorization of a resolvent polynomial is used to determine the orbit length partition of $\{F(x_{1P},\ldots,x_{nP}) : P \text{ in } S_n\}$ under the action of Gal(f/K).

An important class of resolvent polynomials considered are the "linear" resolvent polynomials, where $F = e_1x_1+\ldots+e_rx_r$, e_i in K and $0<r\leq n$. The use of linear resolvents in determining Gal(f/K) is discussed. A new, practical, exact method of computing linear resolvents is described, as well as the computer implementation of this method over the integers.

For every transitive permutation group G of degree up to 7, we have computed a polynomial f(x) such that Gal(f/Q) = G. We also list many new examples of polynomials with PSL(3,2) as Galois group over Q.

ACKNOWLEDGEMENTS

I would like to thank my teacher and supervisor, Prof. J. McKay, for his superb guidance and support throughout this work.

I also thank the following people who made their results and/or computer programs available to me: G. Butler, D. Ford, G. Kolesova, H. Kisilevsky, E. Regener and R. Rohlicek.

Also, to my friends and family I say thank you for your encouragement and support.

This research was funded by the Natural Sciences and Engineering Research Council of Canada and by the Government of Quebec.

TABLE OF CONTENTS

LIST OF TABLES

APPENDIX 1

APPENDIX 2

APPENDIX 3

NOTATION

tS	the image of t under the mapping S,
$\|C\|$	the cardinal of the set C,
K	a field,
$\mathrm{char}(K)$	the characteristic of K,
$K(v_1,\ldots,v_n)$	the field extension of K obtained by adjoining $v_1,\ldots,v_n$ to K,
$R[x_1,\ldots,x_n]$	the polynomials in the indeterminates $x_1,\ldots,x_n$ with coefficients in R,
$f(x)$	a polynomial in $K[x]$,
$\deg(f)$	the degree of $f(x)$,
$\mathrm{disc}(f)$	the discriminant of $f(x)$,
$f'(x)$	the formal derivative of $f(x)$,
$G(N/K)$	the Galois group of the normal extension N over K,
$\mathrm{Gal}(f/K)$	the Galois group of $f(x)$ over K,
Q	the field of rational numbers,
Z	the ring of rational integers,
p	a positive prime,
Z_p	the field of integers modulo p,
$i \bmod p$	the image of i under the natural homomorphism from Z onto Z_p,
$F \bmod p$	F with its coefficients replaced by their images mod p (F a (multivariate) polynomial with coefficients in Z),

f mod g	the remainder upon division of f(x) by g(x),
res(f,g)	the resultant of f(x) and g(x),
G	a group,
S_n	the symmetric group on {1,...,n},
A_n	the alternating group on {1,...,n},
$H \leq G$	H is a subgroup of G,
*	a group action,
rep(G,$\underline{C}$,*)	the representation of G into S_n defined by the action of G by * on the ordered set $\underline{C}$,
im(rep(G,$\underline{C}$,*))	the image of G under the preceding representation,
$\mathrm{stab}_G(c)$	the stabilizer in G of c,
$[e_1,\ldots,e_r]$	the multiset of elements $e_1,\ldots,e_r$,
mult(e,M)	the multiplicity of the element e in the multiset M,
mult(v,f)	the multiplicity of v as a zero of f(x),
gcd(a,b)	the greatest common divisor of a and b,
a|b	a divides b,
a||b	a divides b and gcd(a,b/a) = 1,
a <-- expression	the value of a is replaced by the value of the expression.

CHAPTER 1

INTRODUCTION

Galois theory gives an elegant answer to the question of whether a polynomial equation, $f(x) = 0$, over a suitable field K (e.g. the rationals) is solvable by radicals. "Solvable by radicals" means that the zeros of $f(x)$ can be expressed as finite expressions in the coefficients of $f(x)$, where the only permitted operations are the field operations and the extraction of roots. In Galois theory, to each polynomial $f(x)$ over K, there is an associated group G called the Galois group of $f(x)$ over K. The structure of this group describes the structure of the smallest field extension of K containing all the zeros of $f(x)$, and the equation $f(x) = 0$ is solvable by radicals if and only if G is a solvable group [VDW,p.173].

In this thesis we study the problem of computing the Galois group of a given polynomial $f(x)$, with distinct zeros, over a field K. We are especially interested in the case $K = Q$, the field of rational numbers, and when $f(x)$ is irreducible over K. The thesis is intended as a contribution to the domain of symbolic and algebraic computation.

We assume the reader is familiar with basic algebra including group theory, field extension theory and Galois theory. References for this algebra are [BIR,VDW].

1.1 BASIC DEFINITIONS AND RESULTS

We define our terms and state several useful basic results.

1.1.1 GROUP ACTIONS

We define the action of a group on a set. This is fundamental as we will be concerned with determining the action of the Galois group on various sets.

DEFINITION 1.1. Let C be a set and G be a group. We say that G acts on C (by *), if for each pair (c,S) where c in C and S in G, there is defined an element c*S in C such that for all c in C and S,T in G the following axioms hold:
(1) $c*1_G = c$, where 1_G is the identity element of G, and
(2) (c*S)*T = c*(ST).

Let G be a group, C a set, and suppose G acts on C by *. Let c be in C.

The orbit containing c (under G) is defined by

$$c*G = \{c*S : S \text{ in } G\}.$$

|c*G| is called the orbit length. The set of orbits of C

under G,

$$\{c*G : c \text{ in } C\},$$

partitions C. This partition of C induces a partition of |C|, called the <u>orbit</u> <u>length</u> <u>partition</u> of C under G. This partition of |C| consists of the lengths of the distinct orbits of C under G.

The <u>stabilizer</u> of c in G is defined by

$$\text{stab}_G(c) = \{S \text{ in } G : c*S = c\}.$$

Let S,T in G, c,d in C and $H = \text{stab}_G(c)$. It is straightforward to show that the following facts are true (see [NEU]):

(1) $c*S = c*T$ if and only if $HS = HT$; that is, iff S and T are in the same right coset of $\text{stab}_G(c)$ in G.

(2) $\text{stab}_G(c*S) = S^{-1}HS$.

(3) Suppose that $|C| = n < \infty$, and let an ordering of the elements of C be $\underline{C} = (c_1,\ldots,c_n)$. Then there is a natural permutation representation (homomorphism):

$$\text{rep}(G,\underline{C},*) : G \dashrightarrow S_n,$$

where $S \dashrightarrow \overline{S}$ under this represention, and $\overline{S}$ is defined by:

$$i\overline{S} = j \text{ if and only if } c_i*S = c_j,$$

for all S in G and i in $\{1,\ldots,n\}$. The kernel of $\text{rep}(G,\underline{C},*)$ is

$$\bigcap_{i=1}^{n} \mathrm{stab}_G(c_i).$$

The subgroup of S_n which is the image of rep(G,$\underline{C}$,*) is denoted by im(rep(G,$\underline{C}$,*)).

Let H = im(rep(G,$\underline{C}$,*)), and let P be a permutation in S_n. Consider a new ordering of the elements of C:

$$\underline{C}' = (c'_1,\ldots,c'_n) = (c_{1P},\ldots,c_{nP}).$$

Then im(rep(G,$\underline{C}$',*)) = PHP^{-1}.

1.1.2 THE GALOIS GROUP OF A POLYNOMIAL

Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial in K[x], $a_n \neq 0$, n = deg(f) > 0.

DEFINITION 1.2. We say that a field extension N of K is a _splitting_ _field_ of f(x) over K if:
(1) f(x) can be factored into linear factors, f(x) = $a_n(x-v_1)\ldots(x-v_n)$, in N[x], and
(2) N is generated over K by $v_1,\ldots,v_n$, that is, N = $K(v_1,\ldots,v_n)$.

We call $v_1,\ldots,v_n$ the _zeros_ of f(x), and we may assume that f(x) is monic (a_n = 1).

From field-extension theory we know that for the given field K, and f(x) in K[x], we can always construct a splitting field of f(x) over K and this splitting field is unique up to field isomorphism. Thus we may speak of _the_ splitting field of f(x) over K.

DEFINITION 1.3. Let L be a field. An automorphism of L is a 1-to-1 mapping, S, of L onto L such that for all elements a,b in L, (ab)S = (aS)(bS) and (a+b)S = (aS)+(bS).

DEFINITION 1.4. Let N be the splitting field of f(x) over K. The Galois group of N over K, denoted by G(N/K), is the group of all the automorphisms of N which fix each element in K.

Let N be the splitting field of f(x) over K and let G = G(N/K). We call f(x) separable if its zeros in N are distinct. Many of the results of Galois theory apply only to the splitting fields of separable polynomials (the so-called normal and separable extensions: if N is the splitting field of separable f(x) over K, then each element w in N is a zero of a unique separable, monic, irreducible polynomial over K.) We now assume that f(x) is a separable polynomial over K.

Let an ordering of the (distinct) zeros of f(x) be $\underline{V}$ = $(v_1,\ldots,v_n)$. G sends a zero of f(x) to a zero of f(x) (see Lemma 2.6) and thus G acts on the set V = $\{v_1,\ldots,v_n\}$ by *, where the action is defined by $v_i*S = v_iS$ for every S in G and i in {1,..,n}. Thus there is the natural representation

$$\mathrm{rep}(G(N/K),\underline{V},*) : G(N/K) \dashrightarrow S_n$$

as described in Section 1.1.1. This representation is faithful since if an element T is in the kernel of rep(G(N/K),$\underline{V}$,*), then T must fix each of the v_i as well as the elements of K. Since V generates N over K, T must be the identity element.

DEFINITION 1.5. The Galois group of f(x) over K, Gal(f/K), with respect to the ordering $\underline{V} = (v_1,\ldots,v_n)$ of the zeros of f(x), is defined to be im(rep(G(N/K),$\underline{V}$,*)).

If we do not fix an ordering of the zeros of f(x), then Gal(f/K) can be determined at best to within conjugacy in S_n. This is stronger than to within isomorphism and in this thesis we are usually not concerned with the problem of ordering the zeros of f(x). If we do not specify an ordering of the zeros of f(x) and we state that Gal(f/K) = G, we mean that for some ordering of the zeros of f(x), Gal(f/K) = G with respect to that ordering.

1.1.3. THE FUNDAMENTAL THEOREM OF GALOIS THEORY

For later reference, we state the Fundamental Theorem of Galois Theory (for a detailed discussion see [BIR]).

THEOREM 1.6. Let G = G(N/K) be the Galois group of the splitting field N of a separable polynomial f(x) over K. There is a 1-to-1 correspondence between the subgroups H of G and the subfields L of N which contain K. Given L, the corresponding subgroup H is the group of all the automorphisms in G which fix every element in L. Given H, the corresponding subfield L consists of all the elements of N left fixed by every automorphism in H. For each L, the corresponding subgroup H is the Galois group of N over L, and $|H|$ is the degree of N over L.

In particular, if an element b in N is left fixed by all automorphisms in G(N/K), then b belongs to the base field K, the subfield of N corresponding to G(N/K).

1.1.4 THE FUNDAMENTAL THEOREM ON SYMMETRIC POLYNOMIALS

We state the Fundamental Theorem on Symmetric Polynomials.

THEOREM 1.8. ([VDW,p.81]) Let R be a commutative ring with identity and let A in $R[x_1,\ldots,x_n]$ be a symmetric polynomial (that is, $A(x_1,\ldots,x_n) = A(x_{1P},\ldots,x_{nP})$ for every P in S_n). One can construct a unique polynomial B in $R[x_1,\ldots,x_n]$ such that $A = B(s_1,\ldots,s_n)$, where s_i is the i-th elementary symmetric polynomial (that is, $s_i = \sum x_{j_1}\ldots x_{j_i}$, where the sum is taken over all $1\leq j_1<\ldots<j_i\leq n$).

If monic $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$ has zeros $v_1,\ldots,v_n$, then $a_i = (-1)^i s_i(v_1,\ldots,v_n)$, for $i=1,\ldots,n$. Thus if R is a commutative ring with identity, then any symmetric polynomial over R in the zeros of f(x) can be expressed as a polynomial over R in the coefficients of f(x).

1.1.5 THE RESOLVENT POLYNOMIAL

Let $F = F(x_1,\ldots,x_n)$ be a polynomial in $K[x_1,\ldots,x_n]$ and let P be a permutation of $\{1,\ldots,n\}$. We define

$$F*P = F(x_{1P},\ldots,x_{nP}).$$

We call $F*P$ a <u>conjugate function</u> of F. In this way any permutation group on $\{1,\ldots,n\}$ acts on $K[x_1,\ldots,x_n]$ as a group of ring automorphisms.

DEFINITION 1.9. Let F be in $K[x_1,\ldots,x_n]$, $f(x)$ in $K[x]$, and $n = \deg(f) > 0$. Let the zeros of $f(x)$ be $v_1,\ldots,v_n$. The <u>resolvent polynomial</u> associated with F and $f(x)$, $R(F,f)$, is defined by:

$$R(F,f) = \prod_{i=1}^{k} (x - F_i(v_1,\ldots,v_n)),$$

where $\{F_1,\ldots,F_k\} = F*S_n$ (F_i distinct functions). We may take $F_i = F*P_i$ $(i=1,\ldots,k)$, where $\{P_1,\ldots,P_k\}$ is a set of right coset representatives of $\mathrm{stab}_{S_n}(F)$ in S_n (see Section 1.1.1).

The coefficients of $R(F,f)$ are symmetric polynomials over K in $v_1,\ldots,v_n$ and hence by the Fundamental Theorem on Symmetric Polynomials, the coefficients of $R(F,f)$ can be expressed as polynomials over K in the coefficients of $f(x)$. We also note that $R(F,f)$ is independent of the ordering of the zeros of $f(x)$.

An important resolvent polynomial we consider in this thesis is what we call the linear resolvent polynomial.

DEFINITION 1.10. Let $f(x)$ be in $K[x]$, $n = \deg(f) > 0$, and let $e_1,\dots,e_r$ be in K, $0<r\leq n$. Let the multiset $M = [e_1,\dots,e_r]$. The linear resolvent polynomial associated with M and $f(x)$, $LR(M,f)$, is defined to be the resolvent polynomial associated with F and $f(x)$, when $F = F(x_1,\dots,x_n) = e_1x_1+\dots+e_rx_r$.

1.1.6 THE DISCRIMINANT

An important symmetric function of the zeros of a polynomial $f(x)$ is the discriminant of $f(x)$.

DEFINITION 1.11. Let $f(x)$ be in $K[x]$, $n = \deg(f) > 1$, and let the zeros of $f(x)$ be $v_1,\dots,v_n$. The discriminant of $f(x)$, $\mathrm{disc}(f)$, is defined by

$$\mathrm{disc}(f) = \prod_{i<j}(v_i - v_j)^2.$$

We note that $\mathrm{disc}(f) = 0$ if and only if the zeros of $f(x)$ are not distinct.

The discriminant of monic $f(x)$ can be computed efficiently using the relationship (see [CHI,p.283-286]):

$$(1.1) \quad \mathrm{disc}(f) = (-1)^{n(n-1)/2}\mathrm{res}(f,f'),$$

where $\mathrm{res}(f,f')$ is the resultant of $f(x)$ and its formal derivative $f'(x)$. The resultant and formal derivative are discussed in Section 3.2.

1.1.7 THE SPECIALIZATION TO Q

Let monic separable $f(x)$ be in $Q[x]$, $n = \deg(f) > 0$. We take the splitting field of $f(x)$ over Q to be a subfield of the complex numbers. Secondly, if we wish to compute $\mathrm{Gal}(f/Q)$ we may assume that $f(x)$ has rational integer coefficients, for, if not, we may apply the following transformation to $f(x)$:

Let c be the least common multiple of the denominators of the coefficients of $f(x)$. Then

$$g(x) = c^n f(x/c)$$

is a monic polynomial in $Z[x]$. If $(v_1,\ldots,v_n)$ are the zeros of $f(x)$ then $(cv_1,\ldots,cv_n)$ are the zeros of $g(x)$, and with respect to these orderings, $\mathrm{Gal}(g/Q) = \mathrm{Gal}(f/Q)$.

1.2 CONTENT AND CONTRIBUTION OF THIS THESIS

Let $f(x)$ be a separable polynomial in $K[x]$, $n = \deg(f) > 0$.

In this thesis we are concerned with the problem of computing $\mathrm{Gal}(f/K)$ when we have a factorization algorithm for polynomials in $K[x]$. Although there exists a finite algorithm for solving this problem (see Section 2.1), from a feasible computational viewpoint, finding Gal(f/K) is difficult.

In this thesis we pay special attention to the case where K = Q and f(x) is irreducible over K. In this case Gal(f/K) is transitive (see Proposition 2.7). We note that for reducible f(x) the most efficient methods of finding Gal(f/K) would probably include determining the intersections of the splitting fields of pairs of irreducible factors of f(x).

We will discuss algorithms which determine invariants of the conjugacy class of Gal(f/K), when given f(x). The aim is to efficiently determine enough information to specify a representative of the conjugacy class of Gal(f/K). We use the tables in Appendix 1 of non-conjugate transitive permutation groups (of degree up to 8), and invariants of their respective conjugacy classes. These tables were supplied by G. Butler.

In Chapter 2 we discuss computational methods used to determine invariants of Gal(f/K), including work done previously. We discuss in detail the use of resolvent polynomials and show how the linear resolvent can be used in determining Gal(f/K).

In Chapter 3 we describe a new, practical, exact algorithm which uses polynomial resultants to compute linear resolvent polynomials. Our algorithm requires some restrictions on the base field K when char(K)$\neq$0.

In Chapter 4, we implement the algorithm of Chapter 3 over K = Z_p, for p sufficiently large, as a modular algorithm which computes linear resolvents over Z for monic polynomials f(x) in Z[x]. Also in Chapter 4, we include examples which illustrate methods described in this thesis.

An extension of this work would be to develop practical exact methods to compute an arbitrary resolvent polynomial.

For every transitive permutation group G of degree up to 7 we have computed a polynomial f(x) such that Gal(f/Q) = G. These polynomials appear in Appendix 2. This is the first such list of which the author is aware. In Appendix 3 we list new examples of degree 7 polynomials with the simple group PSL(3,2) as Galois group. These polynomials were found by computer searching as were many other of our examples.

CHAPTER 2

METHODS OF DETERMINING GALOIS GROUPS

In this chapter we discuss algorithms to determine properties of the Galois group of a polynomial. The aim is to determine sufficient properties efficiently to specify the conjugacy class of the Galois group. We include work done previously in this chapter, and our discussion centres on the resolvent polynomial.

For an historical perspective on (computational) Galois theory see [DEH,MAT,FOU-1].

2.1 DETERMINING THE GALOIS GROUP IN FINITELY MANY STEPS

Let f(x) be in K[x], n = deg(f) > 0, furthermore suppose f(x) has distinct zeros, $v_1,\ldots,v_n$, in the splitting field of f(x) over K.

If there is an algorithm for factoring multivariate polynomials over K then one can determine Gal(f/K) in a finite number of steps using a method detailed in van der Waerden [VDW,p.189]. We note that such a factoring algorithm exists when there is an algorithm for factorizing univariate polynomials over K [VDW,p.135].

This Galois group algorithm proceeds as follows:

Form the expression

$$t = x_1v_1+\ldots+x_nv_n,$$

where $x_1,\ldots,x_n$ are indeterminates. Let $t_1,t_2,\ldots,t_{n!}$ be the distinct expressions obtained from t by applying all the possible permutations to the indices of the x_i. Set

$$F = F(z,x_1,\ldots,x_n) = \prod_{i=1}^{n!}(z - t_i).$$

F has coefficients symmetric in the v_i and hence the coefficients of F can be expressed in terms of the coefficients of f(x) and the x_i. Let the factorization of F into irreducible factors over $K[z,x_1,\ldots,x_n]$ be

$$F = F_1F_2\ldots F_r.$$

The permutations of the x_i which leave invariant any factor, say F_1, form a group G.

THEOREM 2.1 ([VDW,p.189]) If we assume that the zeros of f(x) are ordered so that $x_1v_1+\ldots+x_nv_n$ is a zero of F_1, then Gal(f/K) = G.

This method is clearly impractical from a computational point of view. However, the result of Theorem 2.1 is used to prove [VDW,p.191] a computationally useful result for the case K = Q. This result is stated in Theorem 2.2.

2.2 THE DETERMINATION OF CYCLE TYPES IN Gal(f/Q)

Let $f(x)$ be a monic separable polynomial in $Z[x]$, $n = \deg(f) > 1$, and let p be a prime.

We define the <u>cycle type</u> of a permutation P in S_n to be the partition of n induced by the lengths of the disjoint cycles of P. The <u>factor type</u> of f(x) mod p is defined to be the partition of n induced by the degrees of the irreducible factors of f(x) mod p over Z_p. A useful method to discover information about Gal(f/Q) is to determine cycle types of permutations in Gal(f/Q) by factorizing f(x) mod p over Z_p for primes p not dividing disc(f). This method has been discussed by many authors including van der Waerden [VDW], Zassenhaus [ZAS-2] and McKay [MCK].

THEOREM 2.2. For any prime p not dividing disc(f), the factor type of f(x) mod p is the cycle type of some permutation in Gal(f/Q).

The following result which follows from the density theorem of Chebotarev may also be used (see [SCH,LAG]).

THEOREM 2.3. Let T be a partition of n. Then as $k \dashrightarrow \infty$, the proportion of occurrences of T as the factor type of f(x) mod p_i, $i=1,\ldots,k$, ($p_1,\ldots,p_k$ distinct primes) tends to the proportion of permutations in Gal(f/Q) having the cycle type T.

We may factorize f(x) mod p over Z_p using the algorithm of Berlekamp [KNU,p.420-429]. However, as we are only interested in the factor type of f(x) mod p, we may use the partial factorization method described by Knuth [KNU,p.429-430], which provides us with the necessary information.

Tables 3C,...,8C in Appendix 1 contain the distribution of permutation cycle types in transitive permutation groups of degrees 3 to 8 respectively. These tables are used when applying Theorems 2.2 and 2.3. Applying Theorem 2.2, we can determine cycle types of permutations in Gal(f/Q). After doing this, we exclude permutation groups as candidates for Gal(f/Q) which do not contain permutations having these determined cycle types. Applying Theorem 2.3, we can make an educated guess as to Gal(f/Q) after factorizing f(x) mod p for a "sufficient" number of primes p. Note, however, that there are two distinct groups of even permutations of degree 8 (T32 and T33) having the same number of elements of each cycle type.

If Gal(f/Q) = S_n or A_n then we can usually quickly determine Gal(f/Q) by applying Theorem 2.2 and using the fact that $\mathrm{Gal}(f/Q) \leq A_n$ iff disc(f) is a rational integral square (see Proposition 2.12).

We now give an example of a polynomial having S_6 as Galois group over Q.

EXAMPLE 2.4. Let $f(x) = x^6+2x+2$; $\mathrm{disc}(f) = -2^6 89.227$. $f(x)$ is irreducible over Q using Eisenstein's criterion with the prime 2. The factor type of $f(x)$ mod 7 is $(3,2,1)$ and the factor type of $f(x)$ mod 11 is $(5,1)$. Hence $\mathrm{Gal}(f/Q)$ is transitive and contains permutations with cycle types $(3,2,1)$ and $(5,1)$. This implies that $\mathrm{Gal}(f/Q) = S_6$ (see Table 6C in Appendix 1).

We now give an example which shows how useful Theorem 2.3 can be to make an educated guess as to Gal(f/Q).

EXAMPLE 2.5. Let $f(x) = x^7-14x^5+56x^3-56x+22$; $\mathrm{disc}(f) = 2^6 7^{10}$. $f(x)$ mod p was factored over Z_p for the 42 primes p in the interval [2,193] which do not divide disc(f). For one prime the factor type is (1^7), for thirty primes the factor type is $(3^2,1)$ and for eleven primes it is (7). Referring to Table 7C in Appendix 1, one feels confident from this information that Gal(f/Q) = 7T3, the Frobenius group of order 21. In fact one can show that Gal(f/Q) is indeed 7T3 (see Section 4.3, Example 4.1). Note that since disc(f) is a square, $\mathrm{Gal}(f/Q) \leq A_7$. This, together with the cycle types in Gal(f/Q) we have determined, has narrowed the candidates for Gal(f/Q) down to 7T3, 7T5, and 7T6 (= A_7).

Complex conjugation is an automorphism of the complex numbers. If f(x) is separable over Q, then complex conjugation induces an element in Gal(f/Q) of cycle type $(2^c,1^r)$, where c is the number of complex conjugate pairs of zeros of f(x) and r is the number of real zeros of f(x). The number of real zeros of a polynomial over Q can be determined by a Sturm polynomial remainder sequence [BUR,vol.1,p.198-203]. We note that the polynomial f(x) in Example 2.5 has all zeros real. This is a necessary condition for |Gal(f/Q)| to be odd.

The preceding factorizations modulo p, discriminants, and the number of real zeros, were calculated using program ONEPOLY written by Regener and Rohlicek.

2.3 THE RESOLVENT POLYNOMIAL

Let f(x) be separable over K, n = deg(f) > 0, and let an ordering of the zeros of f(x) be $\underline{V} = (v_1,\ldots,v_n)$. Resolvent polynomials are classical and computationally useful tools to determine Gal(f/K), and it is the method we concentrate on. For F in $K[x_1,\ldots,x_n]$, we use the resolvent polynomial R(F,f) (with distinct zeros) to determine the orbit length partition of $F*S_n$ under Gal(f/K).

2.3.1 THEORETICAL DEVELOPMENT

Let N be the splitting field of f(x) over K. Then G(N/K) acts on N in a natural way as a group of automorphisms. We now show that each orbit of elements in N under the action of G(N/K) consists precisely of the zeros of a monic irreducible polynomial over K. First we prove the following:

LEMMA 2.6. Let $W = \{w_1,\ldots,w_k\}$ be contained in N (w_i distinct), and $g(x) = \prod_{i=1}^{k}(x-w_i)$. Then G(N/K) maps W onto W if and only if g(x) is in K[x].

PROOF. Let $g(x) = \sum_{i=0}^{k} a_i x^i$, w in W, and S in G(N/K).

Suppose g(x) is in K[x]. As S is an automorphism of N fixing K we have:

$$0 = g(w) = g(w)S = \sum a_i S(w^i)S$$

$$= \sum a_i (wS)^i = g(wS).$$

Thus wS is in W for all w in W and S in G(N/K). Hence G(N/K) maps W onto W.

Conversely, suppose G(N/K) maps W onto W. Then each element S in G(N/K) induces a permutation of W. Thus $a_iS = a_i$ for each coefficient a_i of g(x) because a_i is a symmetric function of $w_1,\ldots,w_k$. This implies that a_i is in K. //

PROPOSITION 2.7. Let G = G(N/K), and w in $W = \{w_1,\ldots,w_k\}$ contained in N (w_i distinct). Denote by wG the set {wS : S in G}. Then W = wG if and only if $g(x) = \prod_{i=1}^{k}(x-w_i)$ is an irreducible polynomial over K.

PROOF. If wG = W, then by the previous lemma, g(x) is in K[x]. Suppose g(x) is reducible. Then g(x) has a factor h(x) in K[x] where $h(x) = \prod_{i \text{ in } I}(x-w_i)$, for some I properly contained in {1,...,k}. Then by the previous lemma G maps

$\{w_i : i \text{ in } I\}$ onto itself, which contradicts the fact that $wG = W$.

Conversely suppose that $g(x)$ is a irreducible polynomial in $K[x]$. By the previous lemma, we know that G maps W onto itself. Thus wG is contained in W. Suppose $wG = \{w_i : i \text{ in } I\}$, where I is properly contained in $\{1,\ldots,k\}$. Then by the previous lemma, $h(x) = \prod_{i \text{ in } I} (x-w_i)$ is in $K[x]$. Since $h(x)$ is a proper divisor of $g(x)$, we have arrived at the desired contradiction. //

We apply the preceding result to determine the information available from the factorization of a given resolvent polynomial.

Let F be in $K[x_1,\ldots,x_n]$. Recall that the resolvent polynomial over K associated with F and $f(x)$ is:

$$R(F,f) = \prod_{i=1}^{k} (x - F_i(\underline{V})),$$

where $\{F_1,\ldots,F_k\} = F^*S_n$ (F_i distinct).

For S in $G(N/K)$, let $S \dashrightarrow \overline{S}$ under the representation of $G(N/K)$ onto $\mathrm{Gal}(f/K)$ discussed in Section 1.1.2. First we show:

LEMMA 2.8. $F(\underline{V})S = F^*\overline{S}(\underline{V})$.

PROOF. $F(v_1,\ldots,v_n)S = F(v_1S,\ldots,v_nS)$
$= F(v_{1\overline{S}},\ldots,v_{n\overline{S}}) = F^*\overline{S}(v_1,\ldots,v_n)$. //

Thus Gal(f/K) acts on polynomials in the zeros of f(x) in precisely the same way that G(N/K) does.

PROPOSITION 2.9. Let t be in I contained in {1,...,k}.

(1) If F_t*Gal(f/K) = {F_i : i in I} and the $F_i(\underline{V})$ are distinct for i in I, then

$$g(x) = \prod_{i \text{ in } I} (x - F_i(\underline{V}))$$ is an irreducible polynomial over K.

(2) If $g(x) = \prod_{i \text{ in } I} (x - F_i(\underline{V}))$ is a non-repeated irreducible factor of R(F,f) then F_t*Gal(f/K) = {F_i : i in I}.

PROOF.

(1) Apply Lemma 2.8 and and Proposition 2.7.

(2) As N is separable over K, g(x) must have distinct zeros. By Proposition 2.7 and Lemma 2.8, {$F_i(\underline{V})$: i in I} = {F*P($\underline{V}$) : P in Gal(f/K)}. As g(x) is a non-repeated factor of R(F,f), for all i in I and j=1,...,k, $F_i(\underline{V}) = F_j(\underline{V})$ if and only if i=j. The result follows. //

COROLLARY 2.10. Suppose R(F,f) has distinct zeros. Then the orbit length partition of F*S_n under Gal(f/K) is the same as the partition of deg(R(F,f)) induced by the degrees of the irreducible factors of R(F,f) over K.

A method of dealing with the occurrence of repeated zeros of R(F,f) is the use of an appropriate Tschirnhaus transformation [BUR,vol.2,p.171-175] applied to f(x).

Now suppose $R(F,f)$ has distinct zeros: $F*P_1(\underline{V}),\ldots,F*P_k(\underline{V})$, where $\{P_1,\ldots,P_k\}$ is a set of right coset representatives of $\mathrm{stab}_{S_n}(F)$ in S_n. We see that $\mathrm{Gal}(f/K)$ acts on the zeros of $R(F,f)$ in the same way as it acts by right multiplication on the cosets $\{\mathrm{stab}_{S_n}(F)P_i\}$. $\mathrm{Gal}(R(F,f)/K)$ is the permutation group induced by this action. Note that the orbit length partition of $F*S_n$ under $\mathrm{Gal}(f/K)$ depends only on $\mathrm{stab}_{S_n}(F)$.

The following result is also of interest:

LEMMA 2.11. Let $F_t(\underline{V})$ be a zero of a non-repeated irreducible factor of the resolvent polynomial $R(F,f)$. Then $K(F_t(\underline{V}))$ is the fixed field corresponding to H, where $H \leq G(N/K)$ maps onto $\mathrm{stab}_{\mathrm{Gal}(f/K)}(F_t)$ under $\mathrm{rep}(G(N/K),\underline{V},*)$.

PROOF. Now $F_t(\underline{V})S = F_t(\underline{V})$ for all S in H. If $F_t(\underline{V})S = F_t(\underline{V})$ for some S not in H, then this implies that $F_t(\underline{V})$ is a repeated zero of $R(F,f)$, which is a contradiction. //

2.3.2 CONSTRUCTION AND FACTORIZATION OF RESOLVENTS

The resolvent polynomial $R(F,f)$ can be constructed by expanding $R(F,f)$ symbolically in the zeros of $f(x)$ and then determining the coefficients of $R(F,f)$ as polynomials in the coefficients of $f(x)$. See Lauer [LAU] for methods related to symmetric polynomials. Unfortunately, unless $\deg(R(F,f))$ is small or $f(x)$ is sparse, this leads to very extensive symbolic manipulation. However, if we use this method, we get an explicit formula for the coefficients of R(F,f) in terms of the coefficients of f(x). Such formulas have been published for specific resolvent polynomials in [BER,DEH,ERB,MAT].

In Chapter 3, we describe a new exact algorithm to construct linear resolvent polynomials. This algorithm does not expand the resolvent symbolically in the zeros of f(x).

For K = Q, monic f(x) in Z[x], and F in Z[x_1,...,x_n], we note that the coefficients of R(F,f) are algebraic integers and hence rational integers. Thus if we form R(F,f) using numerical approximations to the zeros of f(x) and we know that the accuracy of these approximations is such that the coefficients of R(F,f) are calculated to within an absolute error less than 1/2, then we can determine the coefficients of R(F,f) exactly by rounding. Stauduhar [STA-1,STA-2] uses this method (see Section 2.3.4).

In Section 4.1 we discuss a modular approach to computing R(F,f) when f(x) and F are as in the preceding paragraph.

We have assumed we have a factorization algorithm over K[x]. For K = Q, factorization algorithms are discussed in [KNU,p.431-434,SCH,ZAS-1]. In practice, for K = Q, monic f(x) in Z[x], and F in Z[x_1,...,x_n], one can determine candidates for factors of R(F,f) by using numerical approximations to the zeros of $f(x)$.

2.3.3 FUNCTIONS BELONGING TO GROUPS

Let F be in $K[x_1,\ldots,x_n]$ and $G = \mathrm{stab}_{S_n}(F)$. We say that F belongs to G. Note that for P in S_n, $F{*}P$ belongs to $P^{-1}GP$, and in addition, $F{*}P(\underline{V})$ is a zero of $R(F,f)$. Applying Proposition 2.9, we see that if $\mathrm{Gal}(f/K) \leq P^{-1}GP$ for some P in S_n, then $R(F,f)$ has a linear factor. Conversely, if $R(F,f)$ has a non-repeated linear factor then $\mathrm{Gal}(f/K)$ is contained some conjugate of G.

Resolvents where a linear factor determines if $\mathrm{Gal}(f/K)$ is contained in a group of interest are discussed in [BER,FOU-2,LEF,STA-1,STA-2]. Although linear factors are easy to find, the linear factor can give information only about the Galois group's containment in a group and its conjugates. The complete factorization of a well-chosen resolvent polynomial often distinguishes $\mathrm{Gal}(f/K)$ among many possible candidates.

2.3.3.1 THE ALTERNATING FUNCTION

Suppose $\mathrm{char}(K) \neq 2$ and $n>1$. Then the function

$$D = D(x_1,\ldots,x_n) = \prod_{i<j} (x_i - x_j)$$

belongs to A_n, and is called the alternating function. If P in S_n is a odd permutation, then $D{*}P = -D$. Thus

$$R(D,f) = x^2 - (D(\underline{V}))^2.$$

If f(x) has distinct zeros, then R(D,f) has distinct zeros and R(D,f) has a linear factor over K if and only if $D(\underline{V})^2 = \operatorname{disc}(f)$ is a square in K. Thus we have proved:

PROPOSITION 2.12. $\operatorname{Gal}(f/K) \leq A_n$ if and only if disc(f) is a square in K.

2.3.4 THE METHOD OF STAUDUHAR

In [STA-1], and in a condensed version [STA-2], Stauduhar describes an effective method of determining the Galois group over Q of a monic irreducible polynomial f(x) over Z. He describes the implementation of this method for n = deg(f) up to 8, and supplies tables of information necessary for this implementation. Schnackenberg [SCH] includes a discussion of Stauduhar's method in his thesis which surveys techniques to calculate Galois groups.

Stauduhar proceeds as follows:
Let $\underline{V} = (v_1,\ldots,v_n)$ be an ordering of the zeros of f(x) and suppose that with respect to this ordering we know that $\operatorname{Gal}(f/Q) \leq G$. (Initially we know that $\operatorname{Gal}(f/Q) \leq S_n$). If G has no transitive proper subgroups, then $\operatorname{Gal}(f/Q) = G$. Otherwise we check to see if $\operatorname{Gal}(f/Q) \leq H$, for each maximal transitive subgroup H of G.

For H a maximal transitive subgroup of G, we determine if $\mathrm{Gal}(f/Q) \leq P^{-1}HP$ for some P in G. Choose (from a table) a polynomial F in $Z[x_1,\ldots,x_n]$ such that $\mathrm{stab}_G(F) = H$ and consider the factor of R(F,f):

$$R_G(F,f) = \prod_{i=1}^{k} (x - F_i(\underline{V})),$$

where $F_i = F{*}P_i$ ($i=1,\ldots,k$, F_i distinct), $\{P_i\}$ a set of right coset representatives of H in G (obtained from a table). $\mathrm{Gal}(f/Q) \leq G$ implies that each element in Gal(f/Q) induces a permutation of the F_i. Hence $R_G(F,f)$ has rational integer coefficients which are determined by expanding $R_G(F,f)$ using high-precision approximations to the zeros of f(x) and then rounding the approximate coefficients of $R_G(F,f)$. If Gal(f/Q) is contained in some conjugate of H in G, then $R_G(F,f)$ has an integral zero. Conversely, if $R_G(F,f)$ has a non-repeated integral zero, then Gal(f/Q) is contained in some conjugate of H in G. We test each approximate zero z of $R_G(F,f)$ which appears to be integral to determine if $R_G(F,f)(\mathrm{round}(z)) = 0$. Suppose $R_G(F,f)$ has a non-repeated integral zero, $F{*}P(\underline{V})$, P in G. Then $\mathrm{Gal}(f/Q) \leq P^{-1}HP$. We may reorder the zeros of f(x) by setting $\underline{V}$ to $(v_{1P},\ldots,v_{nP})$, and with repect to this ordering, $\mathrm{Gal}(f/Q) \leq H$.

If Gal(f/Q) is contained in no maximal transitive subgroup of G, then Gal(f/Q) = G. Otherwise, we have determined that $\mathrm{Gal}(f/Q) \leq H$ with respect to the ordering $\underline{V}$, where H is a maximal transitive subgroup of G. We may then set G to H and repeat the entire process.

In [STA-1] the information available from a quadratic factor of a resolvent polynomial is discussed.

Stauduhar's method is straightforward and practical. However, highly accurate approximations to the zeros of f(x) are necessary, and one must have much tabulated information available. Furthermore a search down the subgroup lattice of S_n is required since if a function F belongs to G, then F is fixed by the elements of any subgroup of G.

2.3.5 THE USE OF LINEAR RESOLVENT POLYNOMIALS

As usual f(x) is a separable polynomial over K, with zeros $v_1,\dots,v_n$ and splitting field N. Let the multiset M = $[e_1,\dots,e_r]$, where e_i in K and $0<r\leq n$. We call r the <u>length</u> of M. We may also write

$$M = [a_1^{m_1},\dots,a_k^{m_k}],$$

where the a_i are distinct and $m_i>0$ is the <u>multiplicity</u> of a_i in M.

Recall that the linear resolvent polynomial LR(M,f) associated with M and f(x) is the resolvent polynomial R(F,f), where $F = e_1x_1+\dots+e_rx_r$. We treat any zero elements of M as symbolic placeholders. The degree of LR(M,f) is the number of ways of choosing r objects out of n, times the number of distinct permutations of the elements of M. Thus

(2.1) $\deg(LR(M,f)) = \binom{n}{r}\ r!/(m_1!\ldots m_k!)$
$= n!/(m_1!\ldots m_k!(n-r)!)$.

Linear resolvents form a general class of useful resolvent polynomials for f(x) of any degree. Often the factorization of linear resolvents of relatively low degree can be used to determine Gal(f/K) exactly.

2.3.5.1 ACTION ON SETS AND SEQUENCES

A permutation group $G \leq S_n$ acts on the r-sets contained in $\{1,\ldots,n\}$ where the action is defined by $\{i_1,\ldots,i_r\}*P = \{i_1P,\ldots,i_rP\}$ for all P in G. It is clear that the action of G on $F*S_n$, where $F = x_1+\ldots+x_r$, is equivalent to the action of G on the r-sets of $\{1,\ldots,n\}$. Thus the factorization of $LR([1^r],f)$ (with distinct zeros) determines the orbit length partition of $\{1,\ldots,r\}*S_n$ under Gal(f/K). McKay [MCK], and Erbach, Fischer and McKay [ERB] suggest using resolvents of this form in order to determine the transitivity on r-sets of Gal(f/K).

The following remark is of interest: Suppose f(x) is irreducible (Gal(f/K) is transitive) and n=rs, s an integer, $s\neq 1,n$. Then $LR([1^r],f)$ (with distinct zeros) has t irreducible factors of degree s if and only if Gal(f/K) has t systems of imprimitivity of s blocks of size r.

A permutation group $G \leq S_n$ acts on the set of r-sequences $(i_1,\ldots,i_r)$, with i_j in $\{1,\ldots,n\}$ and the i_j distinct $(j=1,\ldots,r)$. This action is defined by $(i_1,\ldots,i_r)*P = (i_1P,\ldots,i_rP)$ for all P in G. It is clear that the action of G on $F*S_n$, where $F = e_1x_1+\ldots+e_rx_r$, e_i distinct, is equivalent to the action of G on r-sequences.

Now suppose $LR(M,f) = LR([e_1,\ldots,e_r],f)$ has distinct zeros and the e_i are distinct. LR(M,f) is reducible iff Gal(f/K) is not r-ply transitive.

There is also a simple field theoretic interpretation to the factorization of this LR(M,f). Let $z = e_1v_{1P}+\ldots+e_rv_{rP}$ be a zero of LR(M,f) (P in S_n). We see that $\mathrm{stab}_{G(N/K)}(z) = \bigcap_{i=1}^{r} \mathrm{stab}_{G(N/K)}(v_{iP})$, and hence by LEMMA 2.11, $K(z) = K(v_{1P},\ldots,v_{rP})$. The degrees of the irreducible factors of LR(M,f) correspond to the degrees over K of non-conjugate subfields of N generated by r-sets of the zeros of f(x). In particular we note that if r=2 and f(x) is irreducible, then LR(M,f) has irreducible factors all of degree n if and only if $N = K(v_i)$ for each zero v_i of f(x), since $K(v_i) = K(v_j)$ for all i,j=1,...,n in this case. We also note that if r=n then LR(M,f) has degree n! and N = K(z) for each zero z of LR(M,f).

Tables 3D to 8D contain the orbit length partitions of r-sets and 2-sequences under the action of the transitive permutation groups of degrees 3 to 8 respectively. For irreducible f(x), these tables are used to determine candidates for Gal(f/K) given the factorization of a linear resolvent which determines the orbit lengths of the action of Gal(f/K) on r-sets or 2-sequences.

2.3.5.2 DIFFERENTIATING ALL TRANSITIVE GROUPS OF DEGREE UP TO 7

Suppose char(K)$\neq$2. If Gal(f/K) is transitive and we know from disc(f) whether Gal(f/K)$\leq A_n$, then for n=3,4,5,7, the conjugacy class of Gal(f/K) is determined completely by the orbit lengths of the action of Gal(f/K) on 2-sets, 3-sets and 2-sequences, with the exception of distinguishing group 5T3 from 5T5.

Group 5T3 can be distinguished from 5T5 (= S_5) in the following way. Let $F = (x_1+x_2-x_3-x_4)^2$ and note that $R(F,f)(x^2) = LR([1^2,-1^2],f)(x)$. We use this linear resolvent to compute R(F,f). For deg(f) = 5, deg(R(F,f)) = 15, and the orbit length partition of $F*S_5$ under 5T3 is (10,5).

For degree 6, all the transitive groups can be differentiated by disc(f) and the action on 2-sets, 3-sets and 2-sequences except to distinguish group T8 from T11, T9 from T13, and T14 from T16 (see Table 6D). To distinguish these groups one can use ad hoc techniques, or Stauduhar's method if K = Q.

We briefly outline a suitable ad hoc technique. We assume that all polynomials discussed have distinct zeros.

Let D = disc(f) not be a square in K, and $d(x) = x^2-D$. If we are working over Z we may take D to be the squarefree part of disc(f). Let r(x) be a monic irreducible factor over K of a resolvent polynomial R(F,f). Suppose $r(F_t(\underline{V})) = 0$ for some ordering $\underline{V}$ of the zeros of f(x) and F_t in F^*S_n. The following are equivalent:

(1) $\text{stab}_{\text{Gal}(f/K)}(F_t) \leq A_n$.

(2) $K(F_t(\underline{V}))$ contains $K(D^{1/2})$.

(3) SZ(r(x),d(x)) has a factor over K of degree deg(r) (see Section 3.2.5 for an explanation of SZ, and also see [VDW,p.126-127]).

Now suppose n = 6.

Suppose Gal(f/K) = T8 or T11. Let r(x) be the monic irreducible factor (over K) of degree 12 of $LR([1^3],f)$. Then Gal(f/K) = T8 if and only if SZ(r(x),d(x)) has a factor (over K) of degree 12.

Suppose Gal(f/K) = T9 or T13. Let r(x) be the monic irreducible factor of degree 2 of $LR([1^3],f)$. Then Gal(f/K) = T9 if and only if SZ(r(x),d(x)) has a factor of degree 2.

Suppose Gal(f/K) = T14 or T16. Let r(x) = LR($[1^3]$,f). Then Gal(f/K) = T14 if and only if SZ(r(x),d(x)) has a factor of degree 20.

CHAPTER 3

LINEAR RESOLVENT POLYNOMIAL CONSTRUCTION

In this chapter we describe an algorithm to construct any linear resolvent polynomial over a field K subject to the restrictions in Section 3.1. The algorithm is exact, uses polynomial resultants and does not expand the resolvent symbolically in the zeros of f(x). This approach was inspired by Trager [TRA], who used polynomial resultants in a similar manner to factorize polynomials over algebraic extension fields.

The usefulness of the linear resolvent in computing Gal(f/K) when we have a factorization algorithm over K[x] has been discussed in Section 2.3.5.

3.1 RESTRICTIONS ON THE FIELD

The linear resolvent algorithm is designed to work over an arbitrary field K, except for the following restrictions:

If $char(K) \neq 0$ then we require that $char(K) > D$, where D is the maximum degree of any polynomial used or constructed by the main algorithm or any sub-algorithm. If $char(K) \neq 0$, then char(K) is a prime, and $char(K) > D$ if and only if $char(K) \nmid D!$.

If K is finite, we need K large enough to construct required polynomials by interpolation. For this requirement, $|K|>2D$ is sufficient. We note that our interest is not in finding the Galois group of a polynomial over a finite field (such a Galois group is always cyclic), but we may use resolvent polynomials over finite fields in a modular algorithm (see Chapter 4).

3.2 POLYNOMIAL OPERATIONS

In this section we describe our basic operations on polynomials over K. We use these operations for the linear resolvent algorithm.

3.2.1 THE GREATEST COMMON DIVISOR

Let $f = f(x)$, $g = g(x)$ be polynomials in $K[x]$. We assume that $f(x)$ and $g(x)$ are not both the zero polynomial.

DEFINITION 3.1. The <u>greatest common divisor</u> of $f(x)$ and $g(x)$, denoted $\gcd(f,g)$, is defined to be the monic polynomial in $K[x]$ of largest degree dividing both $f(x)$ and $g(x)$.

If $\deg(g)>0$, by the polynomial division algorithm there exist $q(x)$, $r(x)$ in $K[x]$ such that $f(x) = q(x)g(x) + r(x)$, $0\leq\deg(r)<\deg(g)$. We denote this $r(x)$ by $f \bmod g$. As any common divisor of f and g divides $f \bmod g$, we may use the following recursive formulation of the gcd to compute

```
gcd(f,g):
    If g(x) is the zero polynomial,
    then gcd(f,g) = f(x)/(leading coefficient of f(x));
    else, if deg(g) = 0, then gcd(f,g) = 1;
    else, gcd(f,g) = gcd(g,f mod g).
```

Let e be a non-negative integer, and let N be the splitting field of f(x) over K. We say that f(x) has a zero v of multiplicity e, if $(x-v)^e || f(x)$ in N[x]. We write e = mult(v,f).

We note that gcd(f,g) over any extension L of K is the same as gcd(f,g) over K. This is because the gcd calculation is carried out exactly the same way over L. In particular, for L the splitting field of f(x)g(x), the zeros of gcd(f,g) are the common zeros of f and g, and if v is a zero of gcd(f,g), then mult(v,gcd(f,g)) = min{mult(v,f),mult(v,g)}.

3.2.2 THE RESULTANT

Let f = f(x), g = g(x) be polynomials in K[x]. Let f(x) = $a(x-v_1)\ldots(x-v_n)$ and g(x) = $b(x-w_1)\ldots(x-w_m)$ over the splitting field of f(x)g(x). Furthermore assume that n = deg(f) > 0, and m = deg(g).

We treat the resultant in a similar manner as Childs [CHI,p.283]. See also Collins [COL].

DEFINITION 3.2. The resultant of f(x) and g(x),

$$\operatorname{res}(f,g) = a^m b^n \prod_{i=1}^{n} \prod_{j=1}^{m} (v_i - w_j).$$ if $g \neq 0$, else

The resultant is a symmetric function of both the v_i and w_j, and hence res(f,g) is an element of K. The following facts are immediate consequences of Definition 3.2.

(1) $\operatorname{res}(f,g) = (-1)^{mn}\operatorname{res}(g,f)$.

(2) $\operatorname{res}(f,g) = a^m \prod_{i=1}^{n} g(v_i)$.

(3) If m = 0, then $\operatorname{res}(f,g) = b^n$. (For our purposes it is convenient to assume the degree of the zero polynomial is zero, so that here we do not exclude the possibility that b = 0.)

We use (1) and (2) to prove the following lemma.

LEMMA 3.3. Suppose m>0, and let r(x) = f mod g. Then $\operatorname{res}(f,g) = (-1)^{mn} b^{n-\deg(r)} \operatorname{res}(g,r)$.

PROOF. $\operatorname{res}(f,g) = (-1)^{mn}\operatorname{res}(g,f)$

$$= (-1)^{mn} b^n \prod_{i=1}^{m} (g(w_i)q(w_i) + r(w_i))$$

$$= (-1)^{mn} b^n \prod_{i=1}^{m} r(w_i)$$

$$= (-1)^{mn} b^{n-\deg(r)} \operatorname{res}(g,r). \quad //$$

Combining (3) and Lemma 3.3, we have a recursive formulation of res(f,g) similar to the recursive formulation of gcd(f,g). This formulation is used to compute res(f,g) efficiently. One can also compute the resultant or gcd non-recursively by using a polynomial remainder sequence.

3.2.3 THE FORMAL DERIVATIVE AND ITS ZEROS

The formal derivative of a polynomial over a field K is similar to the usual derivative of a real polynomial, and shares many common properties.

DEFINITION 3.4. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial over K. We define the formal derivative of f(x), denoted f' or f'(x), by

$$f' = f'(x) = \sum_{i=1}^{n} i a_i x^{i-1},$$

where ia_i means $a_i+\ldots+a_i$ (i times).

There is a important relationship between the multiplicity of zeros of f(x) and the zeros of f'(x), which we state in the following proposition.

PROPOSITION 3.5. Suppose f(x) has a zero v of multiplicity $e>0$. Then if $\mathrm{char}(K)\nmid e$, $\mathrm{mult}(v,f') = e-1$.

PROOF. Let $f(x) = (x-v)^e h(x)$.
Then $f'(x) = e(x-v)^{e-1}h(x) + (x-v)^e h'(x)$. Thus $\mathrm{mult}(v,f')\geq e-1$. Now if $(x-v)^e | f'(x)$, then $(x-v) | eh(x)$. This cannot happen as $\mathrm{char}(K)\nmid e$ implies that $e\neq 0$ and by the definition of multiplicity, x-v cannot divide h(x). //

COROLLARY 3.6. Suppose $\mathrm{char}(K)>n$. For each zero v of f(x) of multiplicity $e>1$, v is a zero of $\gcd(f,f')$ of multiplicity e-1, and gcd(f,f') has no other zeros.

3.2.4 "MULTIPLY ZEROS"

Let f(x) be a monic polynomial over K, n = deg(f), and let the zeros of f(x) be $v_1,\ldots,v_n$. Let d be an element of K. We want to calculate a monic polynomial of degree n having the zeros $dv_1,\ldots,dv_n$. The required polynomial is denoted MZ(d,f) (Multiply Zeros) and is computed as follows:

$$MZ(d,f) = d^n f(x/d), \text{ if } d\neq 0;\ x^n, \text{ if } d=0.$$

3.2.5 "SUM ZEROS"

Let f = f(x), g = g(x) be monic polynomials in K[x]. Let $f(x) = (x-v_1)\ldots(x-v_n)$ and $g(x) = (x-w_1)\ldots(x-w_m)$ over the splitting field of f(x)g(x).

We need to calculate the monic polynomial in K[x] of degree mn with zeros v_i+w_j, (i=1,...,n, j=1,...,m). This polynomial is denoted by SZ(f,g) (Sum Zeros) and we note that equality (3.1) holds as the left-hand side and the right-hand side are both degree mn monic polynomials having the same zeros.

$$(3.1) \qquad SZ(f,g) = \prod_{i=1}^{n} g(x-v_i).$$

Thus for any element y in K we know the value of SZ(f,g)(y). It is:

(3.2) $SZ(f,g)(y) = res(f(x),g(y-x))$.

If K is sufficiently large (and we assume it is), we can calculate $z_i = SZ(f,g)(y_i)$, using (3.2), for $i=1,2,\ldots,mn+1$ and y_i in K distinct. Then we can determine SZ(f,g) by interpolation. That is, we find the polynomial t(x) (= SZ(f,g)) of degree at most mn such that $t(y_i) = z_i$, for $i=1,2,\ldots,mn+1$. For interpolation algorithms, see [KNU,COL].

3.2.6 "POLYNOMIAL ROOT"

Finally, we need an algorithm to solve the following problem. Let k be a positive integer and let u(x) be a monic polynomial in K[x], deg(u) > 0. Suppose we know that $u(x) = r(x)^k$ for some unknown monic r(x) in K[x]. Denote this unique r(x) by PR(k,u) (Polynomial Root). We compute PR(k,u) using the algorithm POLYROOT, which follows. We assume char(K)>deg(u) or char(K)=0.

```
Algorithm POLYROOT;
Input: positive integer $k$ and monic polynomial $u(x)$ in $K[x]$,
    $\deg(u)>0$, such that $u(x) = r(x)^k$ for some unknown monic
    $r(x)$ in $K[x]$. We assume $\mathrm{char}(K)>\deg(u)$ or $\mathrm{char}(K)=0$.
Returns : $PR(k,u)$ ( $= r(x)$ ).
(1) if $k=1$ then return($u(x)$), and stop.
(2) set $t(x)$ <-- $u(x)/\gcd(u,u')$;
{$u'$ is the formal derivative of $u(x)$. $t(x)$ is separable, and
    the zeros of $t(x)$ are precisely the distinct zeros of
    $u(x)$ (recall Corollary 3.6).}
(3) set $r(x)$ <-- $t(x)$, and $s(x)$ <-- $u(x)$;
(4) while $\deg(r) < \deg(u)/k$, execute steps (4.1),...,(4.3);
    (4.1) set $s(x)$ <-- $s(x)/t(x)^k$;
    (4.2) set $t(x)$ <-- $\gcd(s,t)$;
{In the i-th iteration of this loop, at this point, the
        zeros of $t(x)$ are precisely the distinct zeros $v$ of
        $u(x)$ such that $\mathrm{mult}(v,u)>i$.}
    (4.3) set $r(x)$ <-- $t(x)r(x)$;
(5) return($r(x)$), and stop.
```

3.3 MULTISET OPERATIONS

We define the operations + and - for multisets. They are similar respectively to union and difference for sets, except that multiplicities are counted. We use these operations in the proof following and in the linear resolvent algorithm. $\mathrm{mult}(e,M)$ denotes the multiplicity of the element e in the multiset M.

Let M and N be multisets and let e an element of the "universal" set from which M and N draw their elements. Then $M + N$ is a multiset, and $\mathrm{mult}(e,M + N) = \mathrm{mult}(e,M) + \mathrm{mult}(e,N)$. $M - N$ is a multiset and $\mathrm{mult}(e,M - N) = \mathrm{mult}(e,M) - \mathrm{mult}(e,N)$ if $\mathrm{mult}(e,M) > \mathrm{mult}(e,N)$, and $\mathrm{mult}(e,M - N) = 0$ otherwise.

3.4 CONSTRUCTIVE PROOF

Let K be a field satisfying the restrictions described in Section 3.1. Let $f(x)$ be a monic polynomial in $K[x]$, $n = \deg(f) > 0$, and let the zeros of $f(x)$ be $v_1,\ldots,v_n$. Let $e_1,\ldots,e_r$ be in K, $0<r\le n$, and let $M = [e_1,\ldots,e_r]$. We now prove:

PROPOSITION 3.7. The linear resolvent polynomial $LR(M,f)$ can be constructed over K using only the operations MZ, SZ, and PR discussed in Section 3.2.

PROOF. By induction on r, the length of M.

If $r = 1$ then $LR(M,f) = MZ(e_1,f)$.

Now suppose $r>1$. Let $\overline{M} = [e_1,\ldots,e_{r-1}] = [a_1^{m_1},\ldots,a_k^{m_k}]$, where $a_1,\ldots,a_k$ are distinct and $m_i = \mathrm{mult}(a_i,\overline{M}) > 0$ for $i=1,\ldots,k$. By the inductive hypothesis we can compute

$$t(x) = SZ(\ LR(\overline{M},f),\ MZ(e_r,f)\ ).$$

For each zero w of $LR(\overline{M},f)$, $t(x)$ has precisely the zeros $w+e_rv_1,\ldots,w+e_rv_n$. Thus we see that

$$t(x) = (\prod_{i=1}^{k} LR(M_i,f)^{c_i})LR(M,f)^{c},$$

where $M_i = (\overline{M} - [a_i]) + [a_i+e_r]$,
$c_i = m_i\deg(LR(\overline{M},f))/\deg(LR(M_i,f))$,
and $c = (n-r+1)\deg(LR(\overline{M},f))/\deg(LR(M,f))$.
We can compute c_i and c using the expression (2.1) for the degree of a linear resolvent polynomial. In fact, by straightforward calculation involving these expressions, one sees that $c_i = \text{mult}(a_i+e_r,M_i)$ and that $c = \text{mult}(e_r,M)$.

By hypothesis we can construct

$$s(x) = \prod_{i=1}^{k} LR(M_i,f)^{c_i}.$$

Then the desired linear resolvent polynomial can be computed by:

$$LR(M,f) = PR(c,t(x)/s(x)). \quad //$$

3.5 ALGORITHM LINRESOLV

Let K be a field satisfying the restrictions stated in Section 3.1. Let f(x) be a monic polynomial in K[x], $n = \deg(f) > 0$. Let $e_1,\ldots,e_r$ be in K, $0<r\leq n$, and let the multiset $M = [e_1,\ldots,e_r]$.

The inductive proof of the preceding section motivates our recursive algorithm to construct LR(M,f), the linear resolvent associated with M and f(x). Changes from the method of the proof have been made for considerations of efficiency. The algorithm is called LINRESOLV and is detailed below.

```
Algorithm LINRESOLV;
Input: a monic polynomial $f(x)$ in $K[x]$ of degree $n > 0$, and
    a multiset $M = [e_1,\ldots,e_r]$, $0<r\leq n$, where $e_1,\ldots,e_r$ in K.
    We assume K satisfies the restrictions stated in Section
    3.1.
Output: LR(M,f), the linear resolvent polynomial associated
    with M and f(x).
(1) {If any of the elements in M equals 0 (the additive
    identity of K) then these zeros are significant as
    symbolic place holders. However, this step allows
    LR(M,f) to be calculated by considering just the maximal
    submultiset of M which contains only non-zero elements.}

    (1.1) set m <-- mult(0,M);
    (1.2) if m = 0 then go to step (2);
    (1.3) if m = r then set t(x) <-- "x",
          and go to step (1.6);
    (1.4) set $\overline{M}$ <-- M - $[0^m]$;
    (1.5) set t(x) <-- LR($\overline{M}$,f);
{recursive application of this algorithm}
```

```
    (1.6) set d <-- $\binom{n-r+m}{m}$, return($t(x)^d$), and stop.
(2) if r = 1 then return(MZ($e_1$,f)), and stop.
(3) Arrange the elements of M so that mult($e_r$,M)$\le$mult($e_i$,M), for i=1,...,r;
{This ensures that the degree of the polynomial constructed in step (4.2) is as small as possible.}
(4)
    (4.1) set $\overline{M}$ <-- [$e_1$,...,$e_{r-1}$]
    (= [$a_1^{m_1}$,...,$a_k^{m_k}$], where $a_1$,...,$a_k$ are distinct and $m_i$ > 0 for i=1,...,k.);
    (4.2) set u(x) <-- LR($\overline{M}$,f);
{using this algorithm recursively}
(5) set s(x) <-- $\prod_{i=1}^{k} \mathrm{LR}(M_i,f)^{c_i}$
    (where $M_i = (\overline{M} - [a_i]) + [a_i+e_r]$, and $c_i$ = mult($a_i+e_r$,$M_i$) );
{using this algorithm recursively}
(6)
    (6.1) set c <-- mult($e_r$,M), g(x) <-- MZ($e_r$,f);
    (6.2) set d to be a positive integer such that for all b = $a^c$, for some a in K,
    (i) $a^d$ is unique in K, for all solutions a in K of b = $a^c$, and
    (ii) we can efficiently compute this $a^d$.
{We may always take d=c.  However, it is most efficient to choose d as small as possible.  For example, when K = Q: if c is odd then let d=1, and $a^d$ is the unique c-th root
```

```
    in Q of b; if c is even then let $d=2$, and $a^d$ is the
    unique positive $(c/2)$-th root in Q of b.}
    (6.3) set m <-- $d(\deg(u)\deg(g)-\deg(s))/c+1$;
{$m = \deg(LR(M,f)^d)+1$}
    (6.4) for m distinct $y_i$ in K ($i=1,..,m$) such that
    $s(y_i) \neq 0$, set $z_i$ <-- $res(u(x),g(y_i-x))/s(y_i)$;
{This is where we need to assume that |K| is "large enough"}

{$z_i = SZ(u,g)(y_i)/s(y_i) = (LR(M,f)(y_i))^c$}
    (6.5) For each $z_i$, we know that $z_i = a_i^c$ for some
    $a_i$ in K.
{$a_i = LR(M,f)(y_i)$}
        For $i=1,...,m$ set $z_i$ <-- $a_i^d$;
{We can do this due to the choice of d as explained in step
    (6.2).}
(7) set t(x) to be the polynomial of degree m-1 such that
    $t(y_i) = z_i$, for $i=1,...,m$;
{using an interpolation algorithm}
(8) return(PR(d,t)), and stop.
```

3.6 REMARKS

As r increases, the efficiency of Algorithm LINRESOLV decreases markedly. However in practice, r is usually quite small; often $r \leq 3$. For a given field K, empirical observations can be made to determine the practical range for r and n. For example, using the implementation described in Chapter 4 over $K = Z_{10000139}$ and f(x) a degree 11 polynomial with no zero coefficients, to compute LR($[1^r]$,f) for r=2,3,4,5, it took respectively 3,13,129,426 CPU seconds.

When Algorithm LINRESOLV computes one resolvent polynomial, it must usually compute other resolvents recursively. If these "byproduct" resolvents are useful they should be saved. For example, to compute LR($[1^3]$,f), LINRESOLV must also compute LR($[1^2]$,f) and LR([1,2],f).

CHAPTER 4

IMPLEMENTATION AND EXAMPLES

Throughout this chapter the following holds: $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i}$ is in Z[x], with zeros $v_1,\ldots,v_n$. $M = [e_1,\ldots,e_r]$, with e_i in Z and $0<r\leq n$.

We discuss our modular algorithm to compute LR(M,f), and the computer implementation of this algorithm. We give examples of the determination of Galois groups over Q, using this implementation.

4.1 A MODULAR APPROACH TO COMPUTING RESOLVENTS

Let $S(x_1,\ldots,x_n)$ be a symmetric polynomial over Z. By the Fundamental Theorem on Symmetric Polynomials, $S = T(s_1,\ldots,s_n)$, for a unique T in $Z[x_1,\ldots,x_n]$ and s_i is the i-th elementary symmetric polynomial.
Let $f(x) \bmod p = x^n + \sum_{i=1}^{n} \overline{a}_i x^{n-i}$ have zeros $\overline{v}_1,\ldots,\overline{v}_n$, and $\overline{S}$, $\overline{T}$ be respectively S mod p, T mod p. Then over Z_p:

$$\overline{S}(\overline{v}_1,\ldots,\overline{v}_n) = \overline{T}(-\overline{a}_1,\overline{a}_2,\ldots,(-1)^n\overline{a}_n).$$

Thus

$$(4.1) \qquad S(v_1,\ldots,v_n) \bmod p = \overline{S}(\overline{v}_1,\ldots,\overline{v}_n).$$

We see that for any F in $Z[x_1,\ldots,x_n]$ such that $\mathrm{stab}_{S_n}(F) = \mathrm{stab}_{S_n}(F \bmod p)$:

(4.2) $\quad R(F,f) \bmod p = R(F \bmod p, f \bmod p)$,

where the latter resolvent is calculated over Z_p. To compute R(F,f) over Z, we can compute R(F,f) mod p_i (using (4.2)) for distinct primes p_i such that $\prod p_i > 2C$, where C is an upper bound on the magnitude of the coefficients of R(F,f). R(F,f) is then built up over Z using the Chinese Remainder Algorithm [KNU,p.268-276].

We calculate C by bounding the magnitude of the zeros of f(x), which allows us to calculate a bound on the magnitude of the zeros of R(F,f). If B is an upper bound on the magnitude of the zeros of R(F,f) and d = deg(R(F,f)), then

$$C = \max\{\tbinom{d}{i} B^i : 1 \leq i \leq d\}$$

is an upper bound on the magnitude of the coefficients of R(F,f).

4.1.1 BOUNDING THE ZEROS OF f(x)

We need to compute a bound A such that $A \geq |v_i|$ for all zeros v_i of f(x). Zassenhaus [ZAS-1] suggested

$$A = \max\{|a_i/\tbinom{n}{i}|^{1/i}/(2^{1/n}-1) : 1 \leq i \leq n\}.$$

We suggest the following method of computing a suitable bound. Let $g(x) = x^n - \sum_{i=1}^{n} |a_i| x^{n-i}$, and let $R>0$ be a strict upper bound on the magnitude of the real zeros of $g(x)$. (By Descartes rule of signs, $g(x)$ has at most one positive real zero (counting multiplicities), so we may take R to be the least positive integer such that $g(R)>0$.) Now note that for any complex number z such that $|z| \geq R$:

$$|f(z)| \geq g(|z|) \geq g(R) > 0.$$

Thus $R>|v_i|$ for each zero v_i of $f(x)$.

We have found this bound to be often much better than that of Zassenhaus, and we use our bound for the examples of Section 4.3.

4.2 THE IMPLEMENTATION

We have programmed algorithm LINRESOLV over $K = Z_p$, in the language PASCAL on the Concordia University CDC Cyber 170-800 computer. This program is used to compute LR(M,f) mod p_i for distinct primes p_i. LR(M,f) is built up over Z using the Chinese Remainder Algorithm, and then LR(M,f) is factorized using Hensel factorization [KNU,SCH,ZAS-1]. For these two operations we use programs written by D. Ford in the language ALGEB, on the PDP-11/34 computer. The language ALGEB was designed by D. Ford, and it allows computation with integers of arbitrary size.

4.2.1 LINRESOLV OVER $K = Z_p$

Z_p satisfies the restrictions of Section 3.1 if $p>2D$, where D is the maximum degree of any polynomial used in the program. In practice we choose p such that p^2 is nearly equal to the largest integer we can operate on ($10^7<p<2^{24}$ in our implementation).

Addition, subtraction, and multiplication over Z_p is implemented by doing these operations over the integers and then applying the PASCAL mod operator to the result. To divide we need multiplicitive inverses in Z_p. Given a in Z, $p \nmid a$, we need to determine b in Z such that ab mod p = 1. We know

$$1 = \gcd(a,p) = ab + tp,$$

for some b,t in Z. b can be computed using the (half) extended Euclidean algorithm [KNU,p.325].

The main problem which is dependent on the base field in the implementation of LINRESOLV is the choice of d in step (6.2). Using the notation of step (6) of Algorithm LINRESOLV, we claim that $d = \gcd(c,p-1)$ is appropriate. Note that

$$d = \gcd(c,p-1) = sc + t(p-1),$$

for some s,t in Z. Let $b = a^c$ for some a in Z_p. Then

$$b^s = a^{cs} = a^d.$$

This is because $y^{p-1} = 1$, for any $y \neq 0$ in Z_p. Now we need to show that $y^d = z^d$ for any y,z in Z_p such that $b = y^c = z^c$. We have

$$y^c = z^c \Rightarrow y^{cs} = z^{cs} \Rightarrow y^d = z^d.$$

When we use algorithm LINRESOLV over Z_{p_i} in order to compute LR(M,f) over Z we choose primes p_i such that $j \nmid (p_i-1)$ for $j=3,..,n$. In this case d is never greater than 2 in step (6.2).

4.3 EXAMPLES

EXAMPLE 4.1. Let $f(x) = x^7-14x^5+56x^3-56x+22$ (discussed in Example 2.5). We compute and factorize $L(x) = LR([1^3],f)$ of degree 35 to prove that Gal(f/Q) is group 7T3, the Frobenius group of order 21.

An upper bound on the magnitude of the zeros of f(x) is 5, and hence 15 is an upper bound on the magnitude of the zeros of L(x). An upper bound on the magnitude of the coefficients of L(x) is $(1/2)10^{42}$. L(x) mod p_i is computed for six primes $p_i>10^7$. This step requires 10 CPU seconds on the CDC Cyber. L(x) is constructed over Z using the Chinese Remainder Algorithm. Factorizing L(x) into irreducible factors over Q, we find $L(x) = L_1(x)L_2(x)L_3(x)$, where
$L_1(x) = x^7-28x^5+224x^3-448x+94$,
$L_2(x) = x^7-28x^5+224x^3-448x+192$, and

$L_3(x) = x^{21}-84x^{19}+2436x^{17}-31136x^{15}+6358x^{14}$
$+203840x^{13}-84392x^{12}-733824x^{11}+420728x^{10}+1480192x^9$
$-988064x^8-1652036x^7+1138368x^6+986496x^5-620928x^4$
$-284032x^3+137984x^2+27104x-10648.$

This factorization takes 12 minutes of CPU time on the PDP-11/34.

L(x) has distinct zeros and its factorization shows that the orbit length partition of 3-sets under Gal(f/Q) is $(7^2,21)$. From Table 7D in Appendix 1, we see that Gal(f/Q) is 7T3.

EXAMPLE 4.2. Let $f(x) = x^5+15x+12$; disc(f) = $2^{10}3^45^5$. f(x) is irreducible over Q, and since disc(f) is not a square, from Table 5A in Appendix 1 we see that Gal(f/Q) = 5T3 (the Frobenius group of order 20) or 5T5 (S_5).

Let $F = (x_1+x_2-x_3-x_4)^2$. We compute and factorize R(x) = R(F,f) of degree 15 to distinguish between the two candidates for Gal(f/Q) $(R(F,f)(x^2) = LR([1^2,-1^2],f)(x)$; see Section 2.3.5.2).

An upper bound on the magnitude of the zeros of f(x) is 3, and hence 144 is an upper bound on the magnitude of the zeros of R(x). An upper bound on the magnitude of the coefficients of R(x) is 10^{33}.

$R(x)$ mod p_i is computed for five primes $p_i>10^7$. This step requires 11 CPU seconds on the CDC Cyber. $R(x)$ is constructed over Z using the Chinese Remainder Algorithm. Factoring $R(x)$ into irreducible factors, we find $R(x) = R_1(x)R_2(x)$, where $\deg(R_1) = 5$ and $\deg(R_2) = 10$.

This factorization takes 2 minutes of CPU time on the PDP-11/34.

$R(x)$ has distinct zeros and its factorization shows that Gal(f/Q) acts intransitively on F^*S_5, and hence Gal(f/Q) is 5T3.

REFERENCES

[BER] Berwick, W.E.H., On soluble sextic equations, Proc. London Math. Soc. (2) 29 (1929), 1-28.

[BIR] Birkhoff, G. and MacLane, S., "A Survey of Modern Algebra", Macmillan, New York, 1965.

[BUR] Burnside, W.S. and Panton, A.W., "The Theory of Equations", vol. 1 and vol. 2, reprint, Dover, New York, 1960.

[CHI] Childs, L., "A Concrete Introduction to Higher Algebra", Springer-Verlag, New York, 1979.

[COL] Collins, G.E., The calculation of multivariate polynomial resultants, JACM, 18 (1971), 515-532.

[DEH] Dehn, E., "Algebraic Equations", reprint, Dover, New York, 1960.

[ERB] Erbach, D.W., Fischer, J. and McKay, J., Polynomials with PSL(2,7) as Galois group, J. Number Theory, 11 (1979), 69-75.

[FOU-1] Foulkes, H.O., The algebraic solution of equations, Science Progress, 26 (1931-2), 601-608.

[FOU-2] Foulkes, H.O., The resolvents of an equation of the seventh degree, Quart. J. of Math., 2 (1931), 9-19.

[KNU] Knuth, D.E., "The Art of Computer Programming", vol 2., 2-nd ed., Addison-Wesley, Reading, Mass., 1981.

[LAG] Lagarias, J.C. and Odlyzko, A.M., Effective versions of the Chebotarev density theorem, "Algebraic Number Fields (L-functions and Galois Properties)", Frolich, A., ed., Academic Press, 1977, 409-464.

[LAM] LaMacchia, S.E., Polynomials with Galois group PSL(2,7), Communications in Algebra, 8 (1980), 983-992.

[LAU] Lauer, E., Alorithms for symmetrical polynomials, Proc. 1976 ACM Symp. on Symbolic and Algebraic Comput., New York, 242-247.

[LEF] Lefton, P., Galois resolvents of permutation groups, Amer. Math. Monthly, 84 (1977), 642-644.

[LON] Long, C.T., "Elementary Introduction to Number

Theory", Heath, Lexington, Mass., 1972.

[MCK] McKay, J., Some remarks on computing Galois groups, SIAM J. Comput., 8 (1979), 344-347.

[MAT] Mathews, G.B., "Algebraic Equations", Cambridge University Press, London, 1930.

[NEU] Neumann, P.M., Stoy, G.A. and Thompson, E.C., "Groups and Geometry", vol. 1, The Mathematical Institute, Oxford, 1980.

[SCH] Schnackenberg, D., Calculation of Galois groups, Master's thesis, University of North Dakota, 1978.

[SHA] Shafarevich, I.R., Construction of fields of algebraic numbers with given solvable Galois group, Izv. Akad. Nauk. SSSR. Ser. Mat., 18 (1954), 525-578.

[STA-1] Stauduhar, R.P., The automatic determination of Galois groups, Ph.D. Dissertation, University of California, Berkeley.

[STA-2] Stauduhar, R.P., The determination of Galois groups, Math. Comput., 27 (1973), 981-996.

[TRA] Trager, B.M., Algebraic factoring and rational function integration, Proc. 1976 ACM Symp. on Symbolic and Algebraic Comput., New York, 219-226.

[TRI] Trinks, W., Ein Beispiel eines Zahlkorpers mit der Galoisgruppe PSL(3,2) uber Q, Manuscript, Universitat Karlsruhe, 1968.

[VDW] van der Waerden, B.L., "Modern Algebra", vol. 1, tr. Blum, F., Ungar, New York, 1953.

[ZAS-1] Zassenhaus, H., On Hensel factorization. I, J. Number Theory, 1 (1969), 291-311.

[ZAS-2] Zassenhaus, H., On the group of an equation, "Computers in Algebra and Number Theory", Birkhoff, G. and Hall, M., eds., SIAM and AMS Proc., 1971, 69-88.

APPENDIX 1

TABLES OF TRANSITIVE GROUPS OF DEGREE UP TO 8

(SUPPLIED BY G. BUTLER)

For each degree we present the information about the transitive groups of that degree in a set of tables. The groups are named T1, T2, etc..., for convenience, and if there may be confusion about the degree of the group we write nTi to mean the i-th group of degree n.

In Table A we list the order of the group, whether it contains only even permutations, the number of inequivalent minimal sets of imprimitivity of each possible type, and the number of conjugacy classes of elements. If the group has a faithful representation of smaller degree this is given in the column headed 'Other Representation', and if the group is known by a common name this name is given in the column headed 'Name'.

In Table B we give a set of generators for each group.

Table C sets out the number of elements of each group with each cycle type.

Table D gives the orbit length partitions of r-sets and 2-sequences (with distinct elements) under the action of each group.

The notation for the group names is as follows: n denotes the cyclic group of order n; p^n denotes an elementary abelian group of order p^n, where p is a prime; D_n denotes the dihedral group of order n; Q_8 is the quaternion group of order 8; A_n is the alternating group of degree n;

Σ_n is the symmetric group of degree n. If A and B are names for groups then A•B denotes a group with a normal subgroup isomorphic to A such that (A•B)/A is isomorphic to B; while AxB denotes the direct product.

Table 3A: groups of degree 3

Group	Order	Even	Number of classes	Name
T1	3	+	3	A_3
T2	6		3	Σ_3

Table 3B: group generators

a = (1,2,3)	b = (1,2)
T1 = <a>	T2 = <a,b>

Table 3C: cycle type distribution

	1^3	$\overset{2}{1}$	3
T1	1	.	2
T2	1	3	2

Table 3D

Orbit length partitions of sets and sequences under G

G	2-sets	2-sequences
$G \leq A_3$		
T1	3	3^2
$G \not\leq A_3$		
T2	3	6

Table 4A: groups of degree 4

Group	Order	Even	Imprimitive $[2^2]$	Number of classes	Name
T1	4		✓	4	4
T2	4	+	✓	4	2^2
T3	8		✓	5	D_8
T4	12	+		4	A_4
T5	24			5	Σ_4

Table 4B: group generators

a = (1,3,4)

b = (1,3)

c = (2,4)

d = (1,2)(3,4)

T1 = <ac>

T2 = <bc,d>

T3 = <ac,bc>

T4 = <a,d>

T5 = <ac,d>

Table 4C: cycle type distribution

		2		3	
	1^4	1^2	2^2	1	4
T1	1	.	1	.	2
T2	1	.	3	.	.
T3	1	2	3	.	2
T4	1	.	3	8	.
T5	1	6	3	8	6

Table 4D

Orbit length partitions of sets and sequences under G

G	2-sets	2-sequences
$G \leq A_4$		
T2	2^3	4^3
T4	6	12
$G \not\leq A_4$		
T1	2,4	4^3
T3	2,4	4,8
T5	6	12

Table 5A: groups of degree 5

Group	Order	Even	Number of Classes	Name
T1	5	+	5	5
T2	10	+	4	D_{10}
T3	20		5	5·4
T4	60	+	5	A_5
T5	120		7	Σ_5

Table 5B: group generators

a = (1,2,3,4,5)   c = (2,3,5,4)

b = (1,2)

T1	=	<a>	T4	=	<a,bab>
T2	=	$<a,c^2>$	T5	=	<a,b>
T3	=	<a,c>			

Table 5C: cycle type distribution

		2	2^2	3	3	4	
	1^5	1^3	1	2	1^2	1	5
T1	1	.	.	.	.	.	4
T2	1	.	5	.	.	.	4
T3	1	.	5	.	.	10	4
T4	1	.	15	.	20	.	24
T5	1	10	15	20	20	30	24

Table 5D

Orbit length partitions of sets and sequences under G

G	2-sets	2-sequences
$G \leq A_5$		
T1	5^2	5^4
T2	5^2	10^2
T4	10	20
$G \not\leq A_5$		
T3	10	20
T5	10	20

Table 6A: groups of degree 6

Group	Order	Even	Imprimitive		Number of Classes	Other Representations	Name
			$[2^3]$	$[3^2]$			
T1	6		✓	✓	6		6
T2	6		✓	✓	3	3T2	Σ_3
T3	12		✓	✓	6		D_{12}
T4	12	+	✓		4	4T4	A_4
T5	18			✓	9		$3\times\Sigma_3$
T6	24		✓		8		$2\times A_4$
T7	24	+	✓		5	4T5	$\Sigma_4/2^2$
T8	24		✓		5	4T5	$\Sigma_4/4$
T9	36			✓	9		$3^2 \cdot 2^2$
T10	36	+		✓	6		$3^2 \cdot 4$
T11	48		✓		10		$2\times\Sigma_4$
T12	60	+			5	5T4	L(2,5)
T13	72			✓	9		$3^2 \cdot D_8$
T14	120				7	5T5	PGL(2,5)
T15	360	+			7		A_6
T16	720				11		Σ_6

Table 6B: group generators

$a = (1,2,3)$

$b = (1,4)(2,5)(3,6)$

$c = (1,5,2,4)(3,6)$

$d = ab$

$e = bc^2$

$f = (1,2)$

$g = (1,3,5)(2,4,6)$

$h = fgfg^2$

$i = (1,3)(2,4)$

$j = (1,6)(2,5)(3,4)$

$k = (1,2,3,4,5)$

$l = (1,6)(2,5)$

$m = (2,3,5,4)$

T1	=	<d>
T2	=	<e,j>
T3	=	<d,e>
T4	=	<g,h>
T5	=	<a,b>
T6	=	<g,f>
T7	=	<g,h,i>
T8	=	<g,h,j>
T9	=	<a,b,e>
T10	=	<a,c>
T11	=	<f,g,i>
T12	=	<k,l>
T13	=	<a,b,c>
T14	=	<k,l,m>
T15	=	<c,k>
T16	=	<d,k>

Table 6C: cycle type distribution

						3					
		2	2^2		3	2		4	4	5	
	1^6	1^4	1^2	2^3	1^3	1	3^2	1^2	2	1	6
T1	1	.	.	1	.	.	2	.	.	.	2
T2	1	.	.	3	.	.	2	.	.	.	.
T3	1	.	3	4	.	.	2	.	.	.	2
T4	1	.	3	.	.	.	8	.	.	.	.
T5	1	.	.	3	4	.	4	.	.	.	6
T6	1	3	3	1	.	.	8	.	.	.	8
T7	1	.	9	.	.	.	8	.	6	.	.
T8	1	.	3	6	.	.	8	6	.	.	.
T9	1	.	9	6	4	.	4	.	.	.	12
T10	1	.	9	.	4	.	4	.	18	.	.
T11	1	3	9	7	.	.	8	6	6	.	8
T12	1	.	15	.	.	.	20	.	.	24	.
T13	1	6	9	6	4	12	4	.	18	.	12
T14	1	.	15	10	.	.	20	30	.	24	20
T15	1	.	45	.	40	.	40	.	90	144	.
T16	1	15	45	15	40	120	40	90	90	144	120

Table 6D

Orbit length partitions of sets and sequences under G

G	2-sets	3-sets	2-sequences
$G \leq A_6$			
T4	3,12	$4^2,6^2$	$6,12^2$
T7	3,12	$4^2,12$	6,24
T10	6,9	2,18	12,18
T12	15	10^2	30
T15	15	20	30
$G \not\leq A_6$			
T1	$3,6^2$	$2,6^3$	6^5
T2	$3^3,6$	$2,6^3$	6^5
T3	$3,6^2$	2,6,12	$6,12^2$
T5	6,9	2,18	$6^2,18$
T6	3,12	$6^2,8$	$6,12^2$
T8	3,12	8,12	6,24
T9	6,9	2,18	12,18
T11	3,12	8,12	6,24
T13	6,9	2,18	12,18
T14	15	20	30
T16	15	20	30

Table 7A: groups of degree 7

Group	Order	Even	Number of Classes	Name
T1	7	+	7	7
T2	14		5	D_{14}
T3	21	+	5	7·3
T4	42		7	7·6
T5	168	+	6	L(3,2)
T6	2520	+	9	A_7
T7	5040		15	Σ_7

Table 7B: group generators

a = (1,2,3,4,5,6,7)	c = (2,3)(4,7)
b = (2,4,3,7,5,6)	d = (1,2,3)

T1	=	<a>	T6	=	<a,d>
T2	=	$<a,b^3>$	T7	=	<b,d>
T3	=	$<a,b^2>$			
T4	=	<a,b>			
T5	=	<a,c>			

Table 7C: cycle type distribution

					3				4					
		2	2^2	2^3	3	2	3	3^2	4	2	4	5	5	6	
	1^7	1^5	1^3	1	1^4	1^2	2^2	1	1^3	1	3	1^2	2	1	7
T1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	6
T2	1	.	.	7	.	.	.	.	.	.	.	.	.	.	6
T3	1	.	.	.	.	.	.	14	.	.	.	.	.	.	6
T4	1	.	.	7	.	.	.	14	.	.	.	.	.	14	6
T5	1	.	21	.	.	.	.	56	.	42	.	.	.	.	48
T6	1	.	105	.	70	.	210	280	.	630	.	504	.	.	720
T7	1	21	105	105	70	420	210	280	210	630	420	504	504	840	720

Table 7D

Orbit length partitions of sets and sequences under G

G	2-sets	3-sets	2-sequences
$G \leq A_7$			
T1	7^3	7^5	7^6
T3	21	7^2,21	21^2
T5	21	7,28	42
T6	21	35	42
$G \nleq A_7$			
T2	7^3	7^3,14	14^3
T4	21	14,21	42
T7	21	35	42

Table 8A: groups of degree 8

Group	Order	Even	Imprimitive		Number of Classes	Other Representations	Name
			$[2^4]$	$[4^2]$			
T1	8		✓	✓	8		8
T2	8	+	3	✓	8		2x4
T3	8	+	7	✓	8		2^3
T4	8	+	5	✓	5	4T3	D_8
T5	8	+	✓	✓	5		Q_8
T6	16		✓	✓	7		
T7	16		✓	✓	10		
T8	16		✓	✓	7		
T9	16	+	3	✓	10		
T10	16	+	3	✓	10		
T11	16	+	✓	✓	10		
T12	24	+	✓		7		SL(2,3)
T13	24	+	✓	✓	8	6T6	$2xA_4$
T14	24	+	✓	✓	5	4T5	Σ_4
T15	32		✓	✓	11		
T16	32		✓	✓	11		
T17	32		✓	✓	14		
T18	32	+	✓	✓	14		
T19	32	+	✓	✓	11		
T20	32	+	✓	✓	11		
T21	32		✓	✓	11		
T22	32	+	✓	✓	17		
T23	48		✓		8		
T24	48	+	✓	✓	10	6T11	$2x \Sigma_4$

Table 8A (continued)

Group	Order	Even	Imprimitive		Number of Classes	Other Representation	Name
			$[2^4]$	$[4^2]$			
T25	56	+			8		$2^3 \cdot 7$
T26	64		✓	✓	16		
T27	64		✓	✓	13		
T28	64		✓	✓	13		
T29	64	+	✓	✓	16		
T30	64		✓	✓	13		
T31	64		✓	✓	16		
T32	96	+	✓		11		
T33	96	+		✓	10		
T34	96	+		✓	10		
T35	128		✓	✓	20		
T36	168	+			8		$2^3 \cdot (7 \cdot 3)$
T37	168	+			6	7T5	L(2,7)
T38	192		✓		16		
T39	192	+	✓		13		
T40	192		✓		13		
T41	192	+		✓	14		
T42	288	+		✓	14		
T43	336				9		PGL(2,7)
T44	384		✓		20		
T45	576	+		✓	16		
T46	576			✓	13		
T47	1152			✓	20		
T48	1344	+			11		$2^3 \cdot L(3,2)$
T49	20160	+			13		A_8
T50	40320				22		Σ_8

Table 8B: group generators

a = (1,4,6,8,2,3,5,7)

b = (1,3,5,7)(2,4,6,8)

c = (1,6)(2,5)(3,8)(4,7)

d = (1,8)(2,7)(3,6)(4,5)

e = (1,7)(2,8)(3,5)(4,6)

f = (1,7)(2,8)(3,6)(4,5)

g = (1,7,2,8)(3,5,4,6)

h = (3,4)(7,8)

i = (1,6)(2,5)(3,4)

j = (1,6)(2,5)(3,7)(4,8)

k = (1,6)(2,5)

l = (1,3)(2,4)(5,8)(6,7)

m = (1,5)(2,6)(3,7)(4,8)

n = (3,5,7)(4,6,8)

o = (1,4)(2,3)(5,6)(7,8)

p = (1,2)(7,8)

q = (1,6,2,5)(3,7)(4,8)

r = (5,6)

s = (1,3)(2,4)

t = (1,2)

u = (1,5)(2,6)

v = (3,4)

w = (1,3)(2,4)(7,8)

x = (2,4,3)(6,8,7)

y = (1,8)(2,5)(3,6)(4,7)

z = (6,8,7)

A = (1,2,3,4,5,6,7)

B = (2,4,3,7,5,6)

C = (2,3)(4,7)

D = (1,8)(2,4)(3,7)(5,6)

E = (1,8)(2,7)(3,4)(5,6)

F = (1,7,3,5)(2,8,4,6)

T1 = <a>

T2 = <b,c>

T3 = <b^2,e,c>

T4 = <b,d>

T5 = <a^2,g>

T6 = <a,f>

T7 = <a,h>

T8 = <a,i>

T9 = <b,e,c>

T26 = <a,f,b^2>

T27 = <a,t>

T28 = <a,u>

T29 = <b,e,f>

T30 = <b,p,iku>

T31 = <q,e,t>

T32 = <e,j,n>

T33 = <F,x>

T34 = <vsv,x,y>

Table 8B (continued)

T10 = <b,j>

T11 = <a^2,b^2,l>

T12 = <g,n>

T13 = <hj,n>

T14 = <n,o>

T15 = <a,f,h>

T16 = <a,b^2>

T17 = <a,e>

T18 = <b,e,j>

T19 = <b,f>

T20 = <b,p>

T21 = <q,e>

T22 = <a^2,b^2,j,e>

T23 = <n,w>

T24 = <c,n,s>

T25 = <A,D>

T35 = <a,f,t>

T36 = <A,D,B^2>

T37 = <A,B^2,E>

T38 = <v,e,n>

T39 = <j,n,s>

T40 = <j,n,shv>

T41 = <F,x,y>

T42 = <s,z,m>

T43 = <A,B,E>

T44 = <t,b,s>

T45 = <s,z,m,y>

T46 = <s,z,q>

T47 = <$vsxz^{-1}$,t,m>

T48 = <A,C,D>

T49 = <A,z>

T50 = <a,t>

Table 8C: cycle type distribution

							3	3				4	
		2	2^2	2^3		3	2	2^2	3^2	3^2	4	2	4
	1^8	1^6	1^4	1^2	2^4	1^5	1^3	1	1^2	2	1^4	1^2	2^2
T1	1	.	.	.	1	.	.	.	.	.	.	.	.
T2	1	.	.	.	3	.	.	.	.	.	.	.	.
T3	1	.	.	.	7	.	.	.	.	.	.	.	.
T4	1	.	.	.	5	.	.	.	.	.	.	.	.
T5	1	.	.	.	1	.	.	.	.	.	.	.	.
T6	1	.	.	4	5	.	.	.	.	.	.	.	.
T7	1	.	2	.	1	.	.	.	.	.	.	.	.
T8	1	.	.	4	1	.	.	.	.	.	.	.	.
T9	1	.	2	.	9	.	.	.	.	.	.	.	.
T10	1	.	2	.	5	.	.	.	.	.	.	.	.
T11	1	.	2	.	5	.	.	.	.	.	.	.	.
T12	1	.	.	.	1	.	.	.	8	.	.	.	.
T13	1	.	.	.	7	.	.	.	8	.	.	.	.
T14	1	.	.	.	9	.	.	.	8	.	.	.	.
T15	1	.	2	8	5	.	.	.	.	.	.	.	.
T16	1	.	6	.	5	.	.	.	.	.	.	.	.
T17	1	.	2	.	5	.	.	.	.	.	4	.	4
T18	1	.	6	.	13	.	.	.	.	.	.	.	.
T19	1	.	2	.	9	.	.	.	.	.	.	8	.
T20	1	.	6	.	5	.	.	.	.	.	.	.	.
T21	1	.	6	.	5	.	.	.	.	.	.	.	16
T22	1	.	6	.	13	.	.	.	.	.	.	.	.

Table 8C (continued)

							3	3				4	
		2	2^2	2^3		3	2	2^2	3^2	3^2	4	2	4
	1^8	1^6	1^4	1^2	2^4	1^5	1^3	1	1^2	2	1^4	1^2	2^2
T23	1	.	.	12	1	.	.	.	8	.	.	.	.
T24	1	.	6	.	13	.	.	.	8	.	.	.	.
T25	1	.	.	.	7	.	.	.	.	.	.	.	.
T26	1	.	6	8	13	.	.	.	.	.	4	.	4
T27	1	4	6	4	5	.	.	.	.	.	.	.	8
T28	1	.	10	.	9	.	.	.	.	.	.	8	16
T29	1	.	10	.	17	.	.	.	.	.	.	8	.
T30	1	.	6	8	5	.	.	.	.	.	4	.	20
T31	1	4	6	4	13	.	.	.	.	.	.	.	24
T32	1	.	6	.	13	.	.	.	32	.	.	.	.
T33	1	.	6	.	13	.	.	.	32	.	.	.	.
T34	1	.	6	.	21	.	.	.	32	.	.	.	.
T35	1	4	10	12	17	.	.	.	.	.	4	8	28
T36	1	.	.	.	7	.	.	.	56	.	.	.	.
T37	1	.	.	.	21	.	.	.	56	.	.	.	.
T38	1	4	6	4	13	.	.	.	32	32	.	.	24
T39	1	.	18	.	25	.	.	.	32	.	.	24	.
T40	1	.	6	24	13	.	.	.	32	.	12	.	12
T41	1	.	18	.	25	.	.	.	32	.	.	24	.
T42	1	.	6	.	21	16	.	48	64	.	.	.	.
T43	1	.	.	28	21	.	.	.	56	.	.	.	.

Table 8C (continued)

							3	3				4	
		2	2^2	2^3		3	2	2^2	3^2	3^2	4	2	4
	1^8	1^6	1^4	1^2	2^4	1^5	1^3	1	1^2	2	1^4	1^2	2^2
T44	1	4	18	28	25	.	.	.	32	32	12	24	36
T45	1	.	42	.	33	16	.	48	64	.	.	72	.
T46	1	.	42	.	9	16	.	48	64	.	.	72	144
T47	1	12	42	36	33	16	96	48	64	.	12	72	180
T48	1	.	42	.	49	.	.	.	224	.	.	168	.
T49	1	.	210	.	105	112	.	1680	1120	.	.	2520	.
T50	1	28	210	420	105	112	1120	1680	1120	1120	420	2520	1260

Table 8C (continued)

	4			5					
	3		5	2	5	6	6	7	
	1	4^2	1^3	1	3	1^2	2	1	8
T1	.	2	.	.	.	.	.	.	4
T2	.	4	.	.	.	.	.	.	.
T3	.	.	.	.	.	.	.	.	.
T4	.	2	.	.	.	.	.	.	.
T5	.	6	.	.	.	.	.	.	.
T6	.	2	.	.	.	.	.	.	4
T7	.	4	.	.	.	.	.	.	8
T8	.	6	.	.	.	.	.	.	4
T9	.	4	.	.	.	.	.	.	.
T10	.	8	.	.	.	.	.	.	.
T11	.	8	.	.	.	.	.	.	.
T12	.	6	.	.	.	.	8	.	.
T13	.	.	.	.	.	.	8	.	.
T14	.	6	.	.	.	.	.	.	.
T15	.	8	.	.	.	.	.	.	8
T16	.	4	.	.	.	.	.	.	16
T17	.	8	.	.	.	.	.	.	8
T18	.	12	.	.	.	.	.	.	.
T19	.	12	.	.	.	.	.	.	.
T20	.	20	.	.	.	.	.	.	.
T21	.	4	.	.	.	.	.	.	.
T22	.	12	.	.	.	.	.	.	.

Table 8C (continued)

	4			5					
	3		5	2	5	6	6	7	
	1	4^2	1^3	1	3	1^2	2	1	8
T23	.	6	.	.	.	.	8	.	12
T24	.	12	.	.	.	.	8	.	.
T25	.	.	.	.	.	.	.	48	.
T26	.	12	.	.	.	.	.	.	16
T27	.	20	.	.	.	.	.	.	16
T28	.	4	.	.	.	.	.	.	16
T29	.	28	.	.	.	.	.	.	.
T30	.	20	.	.	.	.	.	.	.
T31	.	12	.	.	.	.	.	.	.
T32	.	12	.	.	.	.	32	.	.
T33	.	12	.	.	.	.	32	.	.
T34	.	36	.	.	.	.	.	.	.
T35	.	28	.	.	.	.	.	.	16
T36	.	.	.	.	.	.	56	48	.
T37	.	42	.	.	.	.	.	48	.
T38	.	12	.	.	.	32	32	.	.
T39	.	60	.	.	.	.	32	.	.
T40	.	12	.	.	.	.	32	.	48
T41	.	60	.	.	.	.	32	.	.
T42	.	36	.	.	.	.	96	.	.
T43	.	42	.	.	.	56	.	48	84
T44	.	60	.	.	.	32	32	.	48

Table 8C (continued)

	4			5					
	3		5	2	5	6	6	7	
	1	4^2	1^3	1	3	1^2	2	1	8
T45	.	108	.	.	.	.	192	.	.
T46	.	36	.	.	.	.	.	.	144
T47	96	108	.	.	.	.	192	.	144
T48	.	252	.	.	.	.	224	384	.
T49	.	1260	1344	.	2688	.	3360	5760	.
T50	3360	1260	1344	4032	2688	3360	3360	5760	5040

Table 8D

Orbit length partitions of sets and sequences under G

G	2-sets	3-sets	4-sets	2-sequences
$G \leq A_8$				
T2	$4^3,8^2$	8^7	$2^3,4^2,8^7$	8^7
T3	4^7	8^7	$2^7,8^7$	8^7
T4	$4^5,8$	8^7	$2^3,4^4,8^6$	8^7
T5	$4,8^3$	8^7	$2^3,8^8$	8^7
T9	$4^3,8^2$	$8^3,16^2$	$2^3,4^2,8^3,16^2$	$8^3,16^2$
T10	$4^3,16$	$8^3,16^2$	$2,4^3,8^3,16^2$	$8^3,16^2$
T11	$4,8^3$	$8^3,16^2$	$2^3,8^4,16^2$	$8^3,16^2$
T12	4,24	$8,24^2$	$6,8^2,24^2$	$8,24^2$
T13	$4,12^2$	$8,24^2$	$2,6^2,8,24^2$	$8,24^2$
T14	$4,12^2$	$8,24^2$	$2,6^2,8,12^2,24$	$8,24^2$
T18	$4^3,16$	$8,16^3$	$2,4^3,8^3,32$	$8^3,32$
T19	4,8,16	8,16,32	$2,4,8^2,16,32$	8,16,32
T20	4,8,16	$8^3,32$	$2,4,8^2,16^3$	$8,16^3$
T22	$4,8^3$	$8^3,32$	$2^3,8^2,16^3$	$8,16^3$
T24	$4,12^2$	$8,24^2$	$2,6^2,8,24^2$	$8,24^2$
T25	28	56	14,56	56
T29	4,8,16	8,16,32	$2,4,8^2,16,32$	8,16,32
T32	4,24	24,32	$6,8^2,48$	8,48
T33	12,16	8,48	2,12,24,32	24,32
T34	12,16	8,48	$2,12^3,32$	24,32
T36	28	56	14,56	56
T37	28	56	$14^2,42$	56

Table 8D (continued)

G	2-sets	3-sets	4-sets	2-sequences
$G\leq A_8$				
T39	4,24	24,32	$6,8^2,48$	8,48
T41	12,16	8,48	2,12,24,32	24,32
T42	12,16	8,48	2,32,36	24,32
T45	12,16	8,48	2,32,36	24,32
T48	28	56	14,56	56
T49	28	56	70	56

Table 8D (continued)

G	2-sets	3-sets	4-sets	2-sequences
$G \not\leq A_8$				
T1	$4,8^3$	8^7	$2,4,8^8$	8^7
T6	$4,8^3$	$8^3,16^2$	$2,4,8^4,16^2$	$8,16^3$
T7	$4,8,16$	$8^3,16^2$	$2,4,8^2,16^3$	$8^3,16^2$
T8	$4,8,16$	$8^3,16^2$	$2,4,8^2,16^3$	$8,16^3$
T15	$4,8,16$	$8,16^3$	$2,4,8^2,16,32$	$8,16,32$
T16	$4,8,16$	$8^3,32$	$2,4,16^4$	$8,16^3$
T17	$4,8,16$	$8,16,32$	$2,4,16^2,32$	$8^3,32$
T21	$4,8^3$	$8^3,32$	$2^3,16^4$	$8,16^3$
T23	$4,24$	$8,24^2$	$6,16,24^2$	$8,48$
T26	$4,8,16$	$8,16,32$	$2,4,16^2,32$	$8,16,32$
T27	$4,8,16$	$8^3,32$	$2,4,16^4$	$8,16^3$
T28	$4,8,16$	$8,16,32$	$2,4,16^2,32$	$8,16,32$
T30	$4,8,16$	$8,16,32$	$2,4,16^2,32$	$8,16,32$
T31	$4,8^3$	$8^3,32$	$2^3,16^4$	$8,16^3$
T35	$4,8,16$	$8,16,32$	$2,4,16^2,32$	$8,16,32$
T38	$4,24$	$24,32$	$6,16,48$	$8,48$
T40	$4,24$	$24,32$	$6,16,48$	$8,48$
T43	28	56	$28,42$	56
T44	$4,24$	$24,32$	$6,16,48$	$8,48$
T46	$12,16$	$8,48$	$2,32,36$	$24,32$
T47	$12,16$	$8,48$	$2,32,36$	$24,32$
T50	28	56	70	56

APPENDIX 2

POLYNOMIALS WITH GIVEN TRANSITIVE GALOIS GROUPS OVER Q OF DEGREE UP TO 7

It is an unsolved problem whether any permutation group can appear as the Galois group of a polynomial over Q. For each solvable group G it is known that there exists a polynomial f(x) in Q[x] such that Gal(f/Q) = G (see [SHA]); however there does not appear to be a published general method of constructing this f(x) given any solvable G.

For each transitive permutation group G of degree 3 to 7, we have computed a polynomial f(x) such that Gal(f/Q) = G. These polynomials appear in Table A2.1. The notation nTi means group Ti of degree n. The splitting field of f(x) over Q is denoted by spl(f) and z_n denotes a primitive n-th root of 1.

For each polynomial f(x) in Table A2.1, we proved that Gal(f/Q) is the group indicated. Many of the polynomials f(x) are constructed so that spl(f) is contained in some known field. The methods of doing this include constructing f(x) to be a resolvent polynomial, constructing f(x) to be a composite polynomial, or if Gal(f/Q) is to be cyclic, by constructing f(x) such that spl(f) is contained in $Q(z_p)$, p prime (see [VDW,p.163-168]). This knowledge about spl(f) is used to reduce or eliminate the work necessary to determine Gal(f/Q). In fact, the only polynomials whose Galois groups are determined using other information than the splitting field, cycle types or discriminant are those f(x) with Gal(f/Q) = 5T2, 7T2, 7T3, or 7T5. These exceptions are proved to have the group indicated by using the factorization of specific linear resolvents.

Given G, to find monic f(x) in Z[x] such that Gal(f/Q) = G, where it is non-trivial to construct an appropriate splitting field, we do computer searching. If it is required that disc(f) is a square we proceed in the following way:

Let p be an odd prime. disc(f) a square implies disc(f) is a quadratic residue (square) mod p or disc(f) mod p = 0. ((p-1)/2 elements in Z_p are quadratic residues.) Note that disc(f) mod p = disc(f mod p), where disc(f mod p) is calculated over Z_p (see Section 4.1). We can calculate disc(f mod p) efficiently using equation (1.1), and for non-zero d in Z_p, we use Euler's criterion [LON,p.111] that d is a quadratic residue if and only if $d^{(p-1)/2} = 1$.

We search over all polynomials in a given set, and return those f(x) such that disc(f mod p_i) = 0 or disc(f mod p_i) is a quadratic residue, for all (small, consecutive) odd primes p_i in a given set S. In practice $30 \leq |S| \leq 40$. The discriminants over Z of the found polynomials f(x) are then calculated as well as Gal(f/Q).

The above search method to find polynomials with square discriminants is faster than a method which forms the complete discriminant over Z for every polynomial f(x) tested, because f(x) can be rejected as soon as disc(f mod p) is found to be a non-residue for some odd prime p. Also, working mod p allows us to perform this search using a very limited integer size. For example, this search has been implemented on the PDP-11/34 in the language PASCAL; using only 16 bits to represent an integer.

One can also search for monic f(x) in Z[x] such that disc(f mod p_i) = 0 or the factor type of f(x) mod p_i is the cycle type of some permutation in the required group of f(x) (for all (small, consecutive) primes p_i in a fixed set). McKay and Rohlicek use this technique, and in this way they found the polynomial in Table A2.1 with Galois group 7T2.

Table A2.1

Polynomials f(x) such that Gal(f/Q) = G.

G	disc(f)	f(x)	Remarks
Degree 3			
T1	7^2	x^3+x^2-2x-1	$spl(f)=Q(z_7+z_7^{-1})$
T2	$-2^2 3^3$	x^3+2	
Degree 4			
T1	5^3	$x^4+x^3+x^2+x+1$	$spl(f)=Q(z_5)$
T2	2^8	x^4+1	$spl(f)=Q(z_8)$
T3	-2^{11}	x^4-2	
T4	$2^{12}3^4$	$x^4+8x+12$	
T5	229	x^4+x+1	
Degree 5			
T1	11^4	$x^5+x^4-4x^3-3x^2+3x+1$	$spl(f)=Q(z_{11}+z_{11}^{-1})$
T2	$2^{12}5^6$	$x^5-5x+12$	
T3	$2^4 5^5$	x^5+2	
T4	$2^{16}5^6$	$x^5+20x+16$	
T5	19.151	x^5-x+1	

Table A2.1 (continued)

G	disc(f)	f(x)	Remarks
Degree 6			
T1	-7^5	$x^6+x^5+x^4+x^3+x^2+x+1$	$spl(f)=Q(z_7)$
T2	$-2^{16}3^{21}$	x^6+108	$spl(f)=spl(x^3+2)$
T3	$-2^{11}3^6$	x^6+2	
T4	$2^6 3^8$	x^6-3x^2-1	$spl(f)=spl(x^4+8x+12)$
T5	-3^{11}	x^6+3x^3+3	
T6	$-2^6 3^8$	x^6-3x^2+1	$Gal(x^3-3x+1/Q)=A_3$
T7	$2^6 229^2$	x^6-4x^2-1	$spl(f)=spl(x^4+x+1)$
T8	229^3	$x^6-3x^5+6x^4-7x^3+2x^2+x-4$	$spl(f)=spl(x^4+x+1)$
T9	$2^8 3^9$	x^6+2x^3-2	
T10	$2^{10}3^6 5^4$	$x^6+6x^4+2x^3+9x^2+6x-4$	$f(x)=(x^3+3x+1)^2-5$
T11	$-2^{11}5^2 7^2$	x^6+2x^2+2	
T12	$2^{36}5^8$	$x^6+10x^5+55x^4+140x^3+175x^2+170x+25$	$spl(f)=spl(x^5+20x+16)$
T13	$-2^8 733$	$x^6+2x^4+2x^3+x^2+2x+2$	$f(x)=(x^3+x+1)^2+1$
T14	$5^{20}19^3 151^3$	$x^6+10x^5+55x^4+140x^3+175x^2-3019x+25$	$spl(f)=spl(x^5-x+1)$
T15	$2^{16}3^6 5^6$	$x^6+24x-20$	
T16	$-2^6 89.227$	x^6+2x+2	
Degree 7			
T1	$29^6 17^2$	$x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$	$spl(f)=Q(z_{29}+z_{29}^{12}+z_{29}^{-1}+z_{29}^{-12})$
T2	$-3^6 7^9$	$x^7+7x^3+7x^2+7x-1$	
T3	$2^6 7^{10}$	$x^7-14x^5+56x^3-56x+22$	
T4	$-2^6 7^7$	x^7+2	
T5	$7^8 17^2$	$x^7-7x^3+14x^2-7x+1$	
T6	$3^6 7^8$	$x^7+7x^4+14x+3$	
T7	$-2^6 5.233.787$	x^7+2x+2	

APPENDIX 3

POLYNOMIALS WITH PSL(3,2) AS GALOIS GROUP OVER Q

Polynomials f(x) such that Gal(f/Q) = PSL(3,2) (group T5 in Table 7A of Appendix 1) have attracted interest over many years ([ERB,LAM,TRI] and their references). Recently, LaMacchia [LAM] has constructed an infinite family of polynomials with PSL(3,2) as Galois group over Q.

In Table A3.1 we list integral f(x) such that Gal(f/Q) = PSL(3,2). We found these f(x) by searching for polynomials with square discriminants as described in Appendix 2. All polynomials searched are of the form:

$$f(x) = x^7 + \sum_{i=0}^{5} a_i x^i,$$

where $7|a_i$ and $|a_i| \leq M$ for $i=1,\ldots,5$; and $1 \leq a_0 \leq 2M$. The sets of polynomials searched are:

(1) $\{f(x) : M = 14\}$,

(2) $\{f(x) : M = 28, \text{ and } a_4, a_2 = 0\}$,

(3) $\{f(x) : M = 56, a_4, a_2 = 0, \text{ and each of}$
$a_5, a_3, a_1 \text{ is in } \{0, \pm 2^j 7 : 0 \leq j \leq 3\}\ \}$.

We know of no monic f(x) in Z[x] such that Gal(f/Q) = PSL(3,2) and $\mathrm{disc}(f) < 7^8 17^2$.

We did some similar searching in an effort to find degree 11 polynomials f(x) such that Gal(f/Q) = PSL(2,11) or

Gal(f/Q) = M_{11}, the sporadic simple group of Mathieu of order 7920. No such f(x) was found.

Table A3.1

Polynomials f(x) such that Gal(f/Q) = PSL(3,2)

disc(f)	f(x)
$2^6 3^6 5^4 7^8$	$x^7-14x^5-14x^4+14x^3-14x^2+2$
$3^6 7^8 11^2 73^2$	$x^7-14x^5-7x^4+7x^3-7x^2+11$
$2^{20} 7^8$	$x^7-7x^5-14x^4-7x^3-7x+2$
$7^8 17^2$	$x^7-7x^5-7x^4+7x^3+14x^2+7x+2$
$2^6 3^4 7^8$	$x^7-7x^5-7x^4+7x^3+14x^2+7x+3$
$2^6 7^8 13^2 19^2$	$x^7-7x^5-7x^4+14x^3+14x^2-14x+6$
$2^{10} 5^2 7^8$	$x^7-7x^5+7x^3-7x+4$
$2^{12} 7^8 23^2$	$x^7-7x^5+7x^3+14x^2-14x+8$
$2^{14} 7^8$	$x^7-7x^5+14x^3-14x+8$
$2^{12} 7^8 17^2$	$x^7-7x^5+7x^4-7x^3+7x^2+7$
$2^6 7^{10} 23^2$	$x^7-7x^5+7x^4+7x^3-14x^2+7x+13$
$2^6 5^6 7^8$	$x^7-7x^5+7x^4+14x^3-14x^2-14x+6$
$2^6 7^8 17^4$	$x^7-7x^5+7x^4+14x^3-14x^2+14x+2$
$2^6 5^6 7^8 29^2$	$x^7-14x^4-7x^3+14x^2+14$
$2^{16} 5^2 7^8$	$x^7-14x^4+14x^3+4$
$2^8 7^8 643^2$	$x^7-14x^3-14x^2+7x+22$
$7^8 17^2$	$x^7-7x^3+14x^2-7x+1$
$3^8 7^8$	x^7-7x+3 (example of Trinks [TRI])

Table A3.1 (continued)

disc(f)	f(x)
$5^2 7^8 13^2 17^2$	$x^7+7x^4-7x^3-7x^2+14x+3$
$3^6 5^2 7^8 13^2 17^2$	$x^7+14x^4-7x^3-14x^2-14x+13$
$3^4 7^8 13^2 19^2 41^2$	$x^7+14x^5-7x^4-7x^3-7x^2-14x+17$
$2^{12} 5^2 7^8 149^2$	$x^7-28x^3+28x+20$
$3^{12} 7^8 47^2$	$x^7-21x^3+7x+27$
$2^{20} 7^8 457^2$	$x^7-14x^5-28x^3+28x+16$
$2^{12} 7^8 11^2 2699^2$	$x^7-56x^3+28x+44$