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.

© Leonard Soicher, 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

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},
$H \underline{\leq} G$	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,
$stab_G(c)$	the stabilizer in G of c,
$[e_1,...,e_r]$	the multiset of elements $e_1,...,e_r$,
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 <u>acts on</u> 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 <u>orbit</u> containing c (under G) is defined by

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

$|c*G|$ is called the <u>orbit length</u>. 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 orbit length partition of C under G. This partition of |C| consists of the lengths of the distinct orbits of C under G.

The stabilizer of c in G is defined by

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

Let S,T in G, c,d in C and $H = stab_G(c)$. 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 $stab_G(c)$ in G.

(2) $stab_G(c*S) = S^{-1}HS$.

(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):

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

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 $rep(G,\underline{C},*)$ is

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

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

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

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 <u>splitting field</u> 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 <u>zeros</u> 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 <u>the</u>

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

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

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,...,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 conjugate function 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 resolvent polynomial 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 $e_1,\ldots,e_r$ be in K, $0<r\leq n$. Let the multiset $M = [e_1,\ldots,e_r]$. 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 $F = F(x_1,\ldots,x_n) = e_1x_1+\ldots+e_rx_r$.

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 $v_1,\ldots,v_n$. 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]):

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

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 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, Gal(g/Q) = 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 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)≠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 cycle type of a permutation P in S_n to be the partition of n induced by the lengths of the disjoint cycles of P. The factor type 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 $k \to \infty$, the proportion of occurrences of T as the factor type of f(x) mod p_i, i=1,...,k, (p_1,...,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 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 $f(x) = x^6+2x+2$; $disc(f) = -2^6 89.227$. $f(x)$ 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 $Gal(f/Q)$ is transitive and contains permutations with cycle types (3,2,1) and (5,1). This implies that $Gal(f/Q) = S_6$ (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 $f(x) = x^7-14x^5+56x^3-56x+22$; $disc(f) = 2^6 7^{10}$. $f(x)$ 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, $Gal(f/Q) \leq A_7$. 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 $a_i S = a_i$ 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 <u>irreducible</u> 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 $Gal(f/K)$ 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) = $\{F_i : i \text{ in } I\}$ 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) = $\{F_i : i \text{ in } I\}$.

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, $\{F_i(\underline{V}) : i \text{ in } I\}$ = $\{F^*P(\underline{V}) : P \text{ in Gal}(f/K)\}$. 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 $\text{stab}_{S_n}(F)$ in S_n. We see that $\text{Gal}(f/K)$ acts on the zeros of $R(F,f)$ in the same way as it acts by right multiplication on the cosets $\{\text{stab}_{S_n}(F)P_i\}$. $\text{Gal}(R(F,f)/K)$ is the permutation group induced by this action. Note that the orbit length partition of F^*S_n under $\text{Gal}(f/K)$ depends only on $\text{stab}_{S_n}(F)$.

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 $\text{stab}_{\text{Gal}(f/K)}(F_t)$ under $\text{rep}(G(N/K),\underline{V},*)$.

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 $Z[x_1,\ldots,x_n]$, 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 $Z[x_1,\ldots,x_n]$, 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 $G = stab_{S_n}(F)$. 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(V) is a zero of R(F,f). Applying Proposition 2.9, we see that if $Gal(f/K) \leq P^{-1}GP$ 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 Gal(f/K) is contained some conjugate of G.

Resolvents where a linear factor determines if 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 Gal(f/K) among many possible candidates.

2.3.3.1 THE ALTERNATING FUNCTION

Suppose char(K)≠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 $D(\underline{V})^2$ = disc(f) is a square in K. Thus we have proved:

PROPOSITION 2.12. $Gal(f/K) \leq A_n$ 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 $Gal(f/Q) \leq G$. (Initially we know that $Gal(f/Q) \leq S_n$). If G has no transitive proper subgroups, then Gal(f/Q) = G. Otherwise we check to see if $Gal(f/Q) \leq H$, for each maximal transitive subgroup H of G.

For H a maximal transitive subgroup of G, we determine if $Gal(f/Q) \leq P^{-1}HP$ for some P in G. Choose (from a table) a polynomial F in $Z[x_1,\ldots,x_n]$ such that $stab_G(F) = H$ 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,...,k, F_i distinct), $\{P_i\}$ a set of right coset representatives of H in G (obtained from a table). $Gal(f/Q) \leq G$ 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 $R_G(F,f)(round(z)) = 0$. Suppose $R_G(F,f)$ has a non-repeated integral zero, $F*P(\underline{V})$, P in G. Then $Gal(f/Q) \leq P^{-1}HP$. We may reorder the zeros of f(x) by setting $\underline{V}$ to $(v_{1P},\ldots,v_{nP})$, and with repect to this ordering, $Gal(f/Q) \leq H$.

If Gal(f/Q) is contained in no maximal transitive subgroup of G, then Gal(f/Q) = G. Otherwise, we have determined that $Gal(f/Q) \leq H$ 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 $v_1,\ldots,v_n$ and splitting field N. Let the multiset $M = [e_1,\ldots,e_r]$, where e_i in K and $0<r\leq n$. We call r the <u>length</u> of M. We may also write

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

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 $F = e_1x_1+\ldots+e_rx_r$. 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

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

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 $stab_{G(N/K)}(z) = \bigcap_{i=1}^{r} stab_{G(N/K)}(v_{iP})$, 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 $i,j=1,\ldots,n$ 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)≠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)≠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)≠0, then char(K) is a prime, and char(K)>D if and only if char(K)∤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 greatest common divisor 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),

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

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

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

(3) If m = 0, then $\text{res}(f,g) = b^n$. (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 $\text{res}(f,g) = (-1)^{mn} b^{n-\deg(r)} \text{res}(g,r)$.

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

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

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

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

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 char(K)$\nmid$e, 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 $mult(v,f') \geq e-1$. Now if $(x-v)^e \mid f'(x)$, then $(x-v) \mid eh(x)$. This cannot happen as 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 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.

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

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