MATHEMATICS OF COMPUTATION, VOLUME 27, NUMBER 124, OCTOBER 1973

The Determination of Galois Groups

By Richard P. Stauduhar

Abstract. A technique is described for the nontentative computer determination of the Galois groups of irreducible polynomials with integer coefficients. The technique for a given polynomial involves finding high-precision approximations to the roots of the polynomial, and fixing an ordering for these roots. The roots are then used to create resolvent polynomials of relatively small degree, the linear factors of which determine new orderings for the roots. Sequences of these resolvents isolate the Galois group of the polynomial. Machine implementation of the technique requires the use of multiple-precision integer and multiple-precision real and complex floating-point arithmetic. Using this technique, the writer has developed programs for the determination of the Galois groups of polynomials of degree $N \leqq 7$. Two exemplary calculations are given.

Introduction. The existence of an algorithm for the determination of Galois groups is nothing new; indeed, the original definition of the Galois group contained, at least implicitly, a technique for its determination, and this technique has been described explicitly by many authors (cf. van der Waerden [8, p. 189]). These sources show that the problem of finding the Galois group of a polynomial $p(x)$ of degree n over a given field K can be reduced to the problem of factoring over K a polynomial of degree $n!$ whose coefficients are symmetric functions of the roots of $p(x)$.

In principle, therefore, whenever we have a factoring algorithm over K, we also have a Galois group algorithm. In particular, since Kronecker has described a factoring algorithm for polynomials with rational coefficients, the problem of determining the Galois groups of such polynomials is solved in principle. It is obvious, however, that a procedure which requires the factorization of a polynomial of degree $n!$ is not suited to the uses of mortal men.

In the next sections we describe a practical and relatively simple procedure which has been used to develop programs for polynomials of degrees 3 through 7.

Restrictions. The algorithm to be described will apply only to irreducible monic polynomials with integer coefficients. Since any polynomial with rational coefficients can easily be transformed into a monic polynomial with integer coefficients equivalent with respect to its Galois group, these latter two adjectives create no genuine restriction. The irreducibility restriction is genuine, however. For suppose $p(x) = p_1(x) \cdot p_2(x)$, and suppose K_1 and K_2 are the splitting fields of p_1 and p_2, respectively. If $K_1 \cap K_2 =$ the rationals, then the Galois group of $p(x)$ is the direct sum of the Galois groups of $p_1(x)$ and $p_2(x)$, and there is no difficulty. If, on the other hand, $K_1 \cap K_2$ is larger than the rationals, then the group of $p(x)$ is not easily determined from those of $p_1(x)$ and $p_2(x)$ without explicit knowledge of the relations which exist between the roots of p_1 and the roots of p_2.

Received May 21, 1970, revised January 9, 1973.
AMS (MOS) subject classifications (1970). Primary 12-04, 12A20, 12A55; Secondary 12E05.
Key words and phrases. Galois group algorithm, resolvent equations.

As will become clear, the irreducibility restriction is not essential, but it greatly simplifies the work of implementing the algorithm for polynomials of a given degree.

There is another restriction. Application of the algorithm to polynomials of degree n requires knowledge of all transitive permutation groups of that degree. However, the memory size of computers currently available will limit use of the algorithm in the near future to cases for which such knowledge already exists. Consequently, this restriction is not practically important.

Representation of the Galois Group. In the classical development of Galois theory, the Galois group of a polynomial is regarded as a group of permutations on the roots of the polynomial. From the standpoint of computation, this concrete, finite representation of the group seems to offer the best hold on the problem of its determination. Consequently, the Galois group will here be regarded as a group of permutations.

More specifically, let S_n be the symmetric group on n letters and $\pi, \sigma \in S_n$ be maps of $\{1, 2, \cdots, n\}$ onto itself. Multiplication of permutations is composition, so that $(\pi \cdot \sigma)(k) = \pi(\sigma(k))$.*

Let $p(x)$ be a polynomial with rational coefficients and roots $r_1, r_2, \cdots, r_n$. Let K be the splitting field of $p(x)$. Let $\mathcal{G}$ be the group of automorphisms of K. Suppose $s \in \mathcal{G}$. Then s induces a permutation on $r_1, \cdots, r_n$, which can be set forth as follows:

$$\begin{pmatrix} r_1, \cdots, r_n \\ s(r_1), \cdots, s(r_n) \end{pmatrix} \text{ or } \begin{pmatrix} r_1, \cdots, r_n \\ r_{i_1}, \cdots, r_{i_n} \end{pmatrix} \text{ or } \begin{pmatrix} 1, \cdots, n \\ i_1, \cdots, i_n \end{pmatrix}.$$

Letting π_s denote the final expression here, it is clear that the map $s \to \pi_s$ defines an isomorphism from $\mathcal{G}$ onto a subgroup G of S_n. It is important to observe that the group G depends on the chosen labelling of the roots of $p(x)$. For if a new labelling $r_1' = r_{\tau(1)}, \cdots, r_n' = r_{\tau(n)}$ is chosen, then the isomorphism given above will carry $\mathcal{G}$ onto $\tau^{-1}G\tau$. Consequently, when the Galois group of a polynomial is given as a group of permutations, an ordering of the roots of the polynomial must also be given.

The material presented in the following two sections is well known from classical Galois theory. A few of the theorems and definitions are presented in a slightly unusual form, one which has been dictated by the numerical character of their application. The others are set forth simply for completeness and for clarity of exposition of the main algorithm.

Groups and Functions. Let $F(x_1, \cdots, x_n)$ be a polynomial in the indeterminants $x_1, \cdots, x_n$. The course of the Galois algorithm requires that the action of permutations on the arguments of such functions be considered.

Definition. Let $F(x_1, \cdots, x_n)$ be a polynomial in the indeterminants $x_1, \cdots, x_n$. Let $\pi \in S_n$. Then $\pi(F)(x_1, \cdots, x_n) = F(y_1, \cdots, y_n)$ where $y_i = x_{\pi(i)}$.

If two permutations are applied sequentially to a function, we obtain the following:

PROPOSITION. $\sigma(\pi(F))(x_1, \cdots, x_n) = \sigma \cdot \pi(F)(x_1, \cdots, x_n)$.

It may be that a function $F(x_1, \cdots, x_n)$ is left unchanged by the action of certain permutations. For example, $F(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4$ is unchanged by any of the permutations {identity, (1234), (1423), (13)(24), (12)(34), (14)(23), (13), (24)}.

* The order of application, right to left, used here in defining multiplication of permutations, should be carefully noted.

The collection of all permutations on n letters which leave a function $F(x_1, \cdots, x_n)$ unchanged clearly forms a group. (The permutations in the above example form the group of the square.)

Definition. Let $F(x_1, \cdots, x_n)$ be a polynomial with integral coefficients in the indeterminants $x_1, \cdots, x_n$. Let G be a group of permutations on $1, \cdots, n$. If F is left unchanged by precisely the permutations of G, we say that F *belongs to* G.

In this definition we restrict the coefficients of F to be integers for reasons that will be apparent later.

THEOREM 1. *Let G be a subgroup of S_n. Then there is a function $F(x_1, \cdots, x_n)$ which belongs to G.*

Proof. Let $F^*(x_1, \cdots, x_n) = x_1^1 x_2^2 \cdots x_n^n$. Define $F(x_1, \cdots, x_n) = \sum_{\sigma \in G} \sigma(F^*)(x_1, \cdots, x_n)$. Clearly, F belongs to G. For if $\pi \in G$, then the application of π merely permutes the terms of F among themselves, but if $\pi \notin G$, then the terms of F are moved onto terms corresponding to the right coset** πG of G. Q.E.D.

Definition. Given a function $F(x_1, \cdots, x_n)$ and a permutation $\pi \in S_n$, the function $\pi(F)$ is called a *conjugate value* or a *conjugate function* of the function F.

Now we can ask the question: Given a polynomial $F(x_1, \cdots, x_n)$, and a group $H \subset S_n$, how many distinct conjugate values does F take under the permutations of H? This is answered by the following:

THEOREM 2. *Let H be a subgroup of S_n. Suppose $F(x_1, \cdots, x_n)$ belongs to $G \subset S_n$. Then F takes exactly $[H : H \cap G]$ distinct conjugate values under the permutations of H.*

Proof. Suppose $\pi_1, \pi_2 \in H$. We will show that $\pi_1(F) = \pi_2(F)$ iff π_1 and π_2 lie in the same right coset of $H \cap G$.

$$\begin{aligned} & \pi_1(F) = \pi_2(F) \\ \text{iff} \quad & \pi_2^{-1}(\pi_1(F)) = F \\ \text{iff} \quad & \pi_2^{-1} \cdot \pi_1(F) = F \\ \text{iff} \quad & \pi_2^{-1} \cdot \pi_1 \in H \cap G \\ \text{iff} \quad & \pi_1(H \cap G) = \pi_2(H \cap G). \end{aligned}$$

Q.E.D.

Definition. Suppose G and H are subgroups of S_n and $F(x_1, \cdots, x_n)$ belongs to G. Let $G' = G \cap H$. We say then that F *belongs to* G' *in* H. That is, among the permutations in H, exactly those of G' leave F unchanged.

THEOREM 3. *Suppose G and H are subgroups of S_n, with $G \subset H$, and suppose $F(x_1, \cdots, x_n)$ belongs to G in H. If $\pi \in H$, then $\pi(F)$ belongs to $\pi G \pi^{-1}$ in H.*

Proof. Omitted.

Now suppose $F(x_1, \cdots, x_n)$ belongs to G in H, and $[H : G] = k$. Then we can choose permutations $\pi_i \in H$ so that $H = \pi_1 G \cup \cdots \cup \pi_k G$, and hence, as we have shown, so that the functions $F = \pi_1(F), \pi_2(F), \cdots, \pi_k(F)$ are formally distinct. It should be noted, however, that the values of these functions are not necessarily distinct on a fixed n-tuple of numbers. For example, let $F(x_1, x_2, x_3, x_4) = x_1 x_2^2 + x_2 x_3^2 + x_3 x_4^2 + x_4 x_1^2$, so that F belongs to the cyclic group generated by (1234), with right coset representatives {identity, (12), (13), (23), (123), (132)} in S_4. Now if we

** The convention adopted here, following Marshall Hall and some others, is that right cosets of a group G are sets of the form πG.

evaluate F and its conjugates on the four roots of $p(x) = x^4 - 2$, with the ordering

$$(r_1, r_2, r_3, r_4) = (\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}),$$

we observe that $(23)F(r_1, r_2, r_3, r_4) = (123)F(r_1, r_2, r_3, r_4) = 0$.

Functions and the Galois Group. In this section, we consider the relation between the Galois group of an irreducible nth degree polynomial $p(x)$ and the values taken on the roots of $p(x)$ by functions belonging to subgroups of S_n.

THEOREM 4. *Let $p(x)$ be a monic irreducible polynomial of degree n with integer coefficients. Let $r_1, r_2, \cdots, r_n$ be a fixed ordering of the roots of $p(x)$. Suppose H is a transitive subgroup of S_n, and suppose that, with respect to the given ordering of the roots, the Galois group Γ of $p(x)$ is a subgroup of H. Let G be a subgroup of H and $F(x_1, \cdots, x_n)$ a function belonging to G in H. Let $\pi_1, \cdots, \pi_k$ be representative for the right cosets of G in H. Then the resolvent polynomial*

$$Q_{(H,G)}(y) = \prod_{i=1}^{k} (y - \pi_i(F(r_1, \cdots, r_n)))$$

has integer coefficients.

Proof. For each i, $1 \leqq i \leqq k$, $\pi_i(F(r_1, \cdots, r_n))$ is an algebraic integer. Hence, the coefficients of $Q_{(H,G)}(y)$ are algebraic integers. Now suppose $\sigma \in \Gamma$. Then $\sigma \in H$, and hence

$$\sigma(Q(y)) = \prod_{i=1}^{k} (y - \sigma(\pi_i(F(r_1, \cdots, r_n))))$$

$$= \prod_{i=1}^{k} (y - (\sigma \cdot \pi_i)(F(r_1, \cdots, r_n))).$$

But the set $\sigma \cdot \pi_1, \sigma \cdot \pi_2, \cdots, \sigma \cdot \pi_k$ is also a set of right coset representatives for G in H. Thus, the application of σ has merely permuted the roots of $Q_{(H,G)}(y)$, leaving the coefficients fixed. The coefficients of Q are then algebraic integers left fixed by Γ and are therefore rational integers. Q.E.D.

At this point it is worth mentioning that the roots of Q may not be distinct, as the example following Theorem 3 shows.

THEOREM 5. *Let all the assumptions of Theorem 4 hold. $F(r_1, \cdots, r_n)$ is a root of $Q_{(H,G)}(y)$, since one of the coset representatives of G in H lies in G itself. Assume $F(r_1, \cdots, r_n)$ is not a repeated root of $Q_{(H,G)}(y)$. Then $\Gamma \subset G$ iff $F(r_1, \cdots, r_n)$ is a rational integer.*

Proof. First, observe that $F(r_1, \cdots, r_n)$ is an algebraic integer.

Now assume $\Gamma \subset G$. Let $\sigma \in \Gamma$. Then $\sigma \in G$, hence $\sigma(F) = F$. Consequently, $F(r_1, \cdots, r_n)$ is fixed under the action of all elements of the Galois group, hence it is a rational number. Since it is an algebraic integer, it is a rational integer.

Conversely, assume $F(r_1, \cdots, r_n)$ is a rational integer. Then $F(r_1, \cdots, r_n)$ is fixed by the Galois group of $p(x)$. But among the permutations of H only those of G fix $F(r_1, \cdots, r_n)$, since it is not a repeated root of $Q_{(H,G)}$. Hence $(\Gamma \cap H) \subset G$. But by assumption $\Gamma \subset H$. Thus $\Gamma \subset G$. Q.E.D.

COROLLARY. *Assume $\pi_i(F(r_1, \cdots, r_n))$ is not a repeated root of $Q_{(H,G)}(y)$. Then $\Gamma \subset \pi_i G \pi_i^{-1}$ iff $\pi_i(F(r_1, \cdots, r_n))$ is a rational integer.*

COROLLARY. *Suppose $\pi_i(F(r_1, \cdots, r_n))$ is a rational integer, and not a repeated*

root of $Q_{(H,G)}(y)$, *so that* $\Gamma \subset \pi_i G \pi_i^{-1}$. *If the roots of* $p(x)$ *are reordered according to the rule* $r_i' = r_{\pi_i(j)}$, *then* $F(r_1', \cdots, r_n')$ *is a rational integer, and with respect to this new ordering,* $\Gamma \subset G$.

There is a well-known theorem (van der Waerden [8, p. 155, Exercise 4]) which is very useful in trying to determine the Galois group of a polynomial.

THEOREM. *Let* $p(x)$ *be a monic irreducible polynomial of degree* n *with integer coefficients. Then the Galois group of* $p(x)$ *is a subgroup of the alternating group* A_n *iff the discriminant* $D(p(x))$ *is a perfect square.*

The Determination of Galois Groups. Suppose that a monic irreducible polynomial $p(x)$ of degree n with integer coefficients is given. Assume that the discriminant $D(p(x))$ and its square root are known. (There is a simple recursive technique for computing the discriminant of a polynomial, given its coefficients. See Brillhart [0, p. 51].)

Assume further that high-precision approximations to the roots of $p(x)$ are known. Place these roots in an (arbitrary) initial ordering $r_1, \cdots, r_n$. Let Γ denote the Galois group of $p(x)$ with respect to this ordering. Now suppose that M is a *maximal* transitive subgroup of S_n, $M \neq A_n$,*** and $[S_n : M] = k$. We know, *a priori*, that $\Gamma \subset S_n$. To determine if $\Gamma \subset M$, or some conjugate of M, calculate a resolvent polynomial of degree k, $Q_{(S_n,M)}(y)$ numerically, using a function $F(x_1, \cdots, x_n)$ belonging to M in S_n, and a set $\pi_1, \cdots, \pi_k$ of right coset representatives for M in S_n.

According to Theorem 4, this resolvent is monic with integer coefficients. Test the resolvent for integer roots. If it has none, then Γ is not contained in any of the conjugates of M, and similar resolvents may be computed, corresponding to other conjugacy classes of maximal transitive subgroups of S_n.

Suppose, however, that $Q_{(S_n,M)}(y)$ has an integer root. Then this root is $\pi_i(F(r_1, \cdots, r_n))$, where π_i is one of the chosen coset representatives, and in consequence of the first corollary to Theorem 5, $\Gamma \subset \pi_i M \pi_i^{-1}$.

The roots of $p(x)$ must now be reordered, so that $r_j' = r_{\pi_i(j)}$. After the reordering, according to the second corollary to Theorem 5, we have $\Gamma \subset M$.

Now, assuming that $\Gamma \subset M$, suppose M^* is a maximal transitive subgroup of M, and F^* is a function belonging to M^* in M. Then a resolvent polynomial $Q_{(M,M^*)}(y)$ of degree $[M : M^*]$ is calculated, and this new polynomial is tested for integer roots. (This resolvent is, again by Theorem 4, monic with integer coefficients.) If an integer root of $Q_{(M,M^*)}$ is found, the roots of $p(x)$ are again reordered to insure that $\Gamma \subset M^*$.

Searching continues in this way until either none of the resolvents at a given level yield an integer root, or a *minimal* transitive subgroup of S_n is located. We need consider only transitive subgroups of S_n in the course of the search, since $p(x)$ is assumed irreducible. At each level of the search, clearly, only groups not previously eliminated need be considered. Suppose, for example, that S_n has maximal subgroups M_1 and M_2, and it is discovered that $Q_{(S_n,M_1)}(y)$ has no integer roots, but that $Q_{(S_n,M_2)}(y)$ does, so that $\Gamma \not\subset M_1$, and $\Gamma \subset M_2$. Then, for the remainder of the search, groups which lie within $M_1 \cap M_2$ are automatically ruled out as possibilities for Γ.

In the above discussion it is assumed that those integer roots of resolvents with respect to which reordering is taking place are not repeated roots. In the case that all

*** The case $M = A_n$ will be considered later in this section.

the integer roots of a resolvent have multiplicity greater than one, the resolvent can be recalculated with respect to a new function, or the input polynomial can be operated upon with a Tschirnhaus transformation, in order to obtain a resolvent without repeated roots.

We have not yet described how the discriminant is used. It is used in two ways. First, if none of the resolvents associated with the maximal transitive subgroups of S_n yield an integer root, then $\Gamma = A_n$ or $\Gamma = S_n$, depending on whether or not $D(p(x))$ is a perfect square. Second, if $D(p(x))$ is a square, and we have determined that $\Gamma \subset M$, then we know that $\Gamma \subset M \cap A_n$. Use of this fact simplifies the search procedure to some extent.

Something now should be said about how integer roots of resolvent polynomials are identified.

Since at each stage of the search procedure the resolvents being dealt with are known to have integer coefficients, it is only necessary to calculate the coefficients of resolvents to within an accuracy of $\pm\frac{1}{2}$ in order to determine them exactly. To insure this accuracy, the roots of a typical resolvent

$$Q_{(M_1, M_2)}(y) = \prod_{i=1}^{k} (y - \pi_i(F(r_1, \cdots, r_n)))$$

can be calculated to high precision, using the given approximations to $r_1, \cdots, r_n$, and the product can then be expanded to obtain approximations to the coefficients. Multiple-precision complex floating-point arithmetic routines are generally required to obtain the necessary accuracy.

If a given (approximate) root of the resolvent $Q_{(M_1, M_2)}$ seems to be an integer to within some reasonable tolerance, it can be rounded to that integer and a synthetic division can be performed with $Q_{(M_1, M_2)}$ to test whether the integer is indeed a root of the resolvent.

The following tables and diagrams contain the data needed to find the Galois groups of polynomials of degree $N \leqq 7$. The tables contain descriptions of representatives of the conjugacy classes of transitive groups of the various degrees, and, when required, functions belonging to these groups, as well as the necessary coset representatives. The alternating and symmetric groups of the various degrees are not included in the tables. No functions are given belonging to the groups for which no resolvent is computed. For example, in the degree five case, if the Galois group Γ of a polynomial $p(x)$ is a subgroup of G_{20}, and $D(p(x))$ is a perfect square, then $\Gamma \subset G_{10}$, otherwise $\Gamma = G_{20}$. Consequently, it is never necessary to compute a resolvent of the form $Q_{(H, G_{10})}$, when $D(p(x))$ is known.

The groups of degree six have been divided into three categories: the groups imprimitive on two sets of three letters, the groups imprimitive on three sets of two letters but not two sets of three letters, and the primitive groups. They are given in this order in the tables. The diagrams indicate, for each degree, the order in which searching can be carried out (i.e., the order in which resolvents should be computed), so that optimal use is made of accumulated information. For these diagrams, the following conventions have been adopted: (1) at any particular node, searching proceeds from left to right on the branches leaving that node; (2) nodes isolated through examination of the discriminant are identified by a leading "A" (for alternating); an example is the node G_4^2 in the tree for $n = 4$; (3) the alternating group A_n is not shown in tree n.

TABLE 1

Degree	*Group*	*Contained in*	*Function*	*Generators, Description*
4	G_8	S_4	$x_1x_3+x_2x_4$	(1234), (13) group of the square
4	G_4^1	G_8	$x_1x_2^2+x_2x_3^2+x_3x_4^2+x_4x_1^2$	(1234) cyclic four group
4	G_4^2			(12)(34), (13)(24) Klein 4-group
5	G_{20}	S_5	$[x_1x_2+x_2x_3+x_3x_4+x_4x_5+x_5x_1 -x_1x_3-x_2x_5-x_5x_2-x_2x_4-x_4x_1]^2$	(12345), (2354) metacyclic five group
5	G_{10}			(12345), (25)(34)
5	G_5	G_{10}	$x_1x_2^2+x_2x_3^2+x_3x_4^2+x_4x_5^2+x_5x_1^2$	(12345) cyclic five group
6	G_{72}	S_6	$x_1x_2x_3+x_4x_5x_6$	(123), (456), (12), (45), (14)(25)(36) maximal group imprimitive on two sets of three letters
6	G_{36}^1			(123), (456), (12)(45), (1425)(36) $G_{72} \cap A_6$
6	G_{36}^2	G_{72}	$(x_1-x_2)(x_2-x_3)(x_3-x_1)(x_4-x_5) \cdot (x_5-x_6)(x_6-x_4)$	(123), (456), (12)(45), (14)(25)(36)

TABLE 1 (*continued*)

Degree	*Group*	*Contained in*	*Function*	*Generators, Description*
6	G_{18}	G_{36}^{2}	$(x_1-x_2)(x_2-x_3)(x_3-x_1)$ $+ (x_4-x_5)(x_5-x_6)(x_6-x_4)$	(123), (456), (14)(25)(36)
6	G_{12}^{1}	G_{36}^{2}	$x_1x_4+x_2x_5+x_3x_6$	(123)(456), (12)(45), (14)(25)(36) metacyclic six group
6	G_{6}^{1}	G_{18}	$x_1x_4+x_2x_6+x_3x_5$	(123)(465), (14)(25)(36) isomorphic to S_3
6	G_{6}^{2}	G_{18}	$x_1x_6^2+x_2x_4^2+x_3x_5^2+x_4x_2^2+x_5x_1^2$ $+x_6x_2^2$	(123)(456), (14)(25)(36) cyclic six group
6	G_{48}	S_6	$x_1x_2+x_3x_4+x_5x_6$	(12), (34), (56), (135)(246), (13)(24) maximal group imprimitive on three sets of two letters
6	G_{24}^{1}	G_{48}	$(x_1+x_2-x_3-x_4)(x_3+x_4-x_5-x_6)$ $\cdot(x_5-x_6-x_1-x_6)(x_1-x_2)$ $\cdot(x_3-x_4)(x_5-x_6)$	(12)(34), (34)(56), (12)(56), (135)(246), (14)(23)(56)
6	G_{24}^{2}	G_{48}	$(x_1+x_2-x_3-x_4)(x_3+x_4-x_5-x_6)$ $\cdot(x_5+x_6-x_1-x_2)$	(12)(34)(56), (34)(56), (56), (135)(246)

TABLE 1 (*continued*)

Degree	*Group*	*Contained in*	*Function*	*Generators, Description*
6	G_{24}^{3}			(135)(246), (13)(24), (12)(34), (34)(56) $G_{48} \cap A_6$ isomorphic to S_4
6	G_{12}^{2}	G_{24}^{3}	see G_{24}^{2}	(12)(34), (34)(56), (12)(56), (135)(246) isomorphic to A_4
6	G_{120}	S_6	$[x_1x_2+x_3x_5+x_4x_6]\cdot[x_1x_3+x_4x_5+x_2x_6]\cdot[x_3x_4+x_1x_6+x_2x_5]\cdot[x_1x_5+x_2x_4+x_3x_6]\cdot[x_1x_4+x_2x_3+x_5x_6]$	(126)(354), (12345), (2354) isomorphic to S_5
6	G_{60}			(126)(354), (12345), (25)(34) $G_{120} \cap A_6$ isomorphic to A_5
7	G_{168}	S_7	$x_1x_2x_4+x_1x_3x_7+x_1x_5x_6+x_2x_3x_5+x_2x_6x_7+x_3x_4x_6+x_4x_5x_7$	(1234567), (235)(476), (2743)(56)
7	G_{42}	S_7	$x_1x_2x_4+x_1x_2x_6+x_1x_3x_4+x_1x_3x_7+x_1x_5x_6+x_1x_5x_7+x_2x_3x_5+x_2x_3x_7+x_2x_4x_5+x_2x_6x_7+x_3x_4x_6+x_3x_5x_6+x_4x_5x_7+x_4x_6x_7$	(1234567), (243756) metacyclic seven group

TABLE 1 (*continued*)

Degree	*Group*	*Contained in*	*Function*	*Generators, Description*
7	G_{21}	G_{168}	See $G_{42} \subset S_7$	(1234567), (235)(476)
7	G_{14}	G_{42}	$x_1x_2+x_2x_3+\ldots+x_6x_7+x_7x_1$	(1234567), (27)(45)(36)
7	G_7	G_{21}	See $G_{14} \subset G_{42}$	(1234567) cyclic 7 group

For $n = 3$, the only transitive groups are S_3 and A_3. Hence the Galois group of an irreducible polynomial of this degree is determined entirely by the value of the discriminant of the polynomial. Consequently, no tree is shown for this degree.

Table 2 gives right coset representatives for the groups of the various degrees, as indicated.

Remark. Information used in constructing the tables and trees presented here has been gleaned from [1], [2], [3], [4]. The author has constructed a similar table and tree for the degree-eight case, using, in addition to the above sources, [5], [6], [7].

TABLE 2

Degree 4	
$G_8 \subset S_4$	I, (23), (34)
$G_4 \subset O_8$	I, (12)(34)
Degree 5	
$G_{20} \subset S_5$	I, (12)(34), (12435), (15243) (12453), (12543)
$G_5 \subset G_{10}$	I, (12)(35)
Degree 6	
$G_{72} \subset S_6$	I, (2543), (236)(45), (25436) (25)(34), (2453), (25), (2345) (24536), (3645)
$G_{36}^2 \subset G_{72}$	I, (56)
$G_{18} \subset G_{72}$	I, (12)(45), (56), (12)(465)
$G_6^1 \subset G_{18}$	I, (123), (132)
$G_6^2 \subset G_{18}$	I, (123), (132)
$G_{12} \subset G_{72}$	I, (123), (132), (56), (123)(56) (132)(56)
$G_{48} \subset S_6$	I, (24635), (26)(35), (354), (2345) (253), (345), (256)(34), (26435) (2346), (234), (25)(36), (2435) (24)(35), (26543)
$G_{24}^1 \subset G_{48}$	I, (12)
$G_{24}^2 \subset G_{48}$	I, (13)(24)
$G_{12}^2 \subset G_{24}^3$	I, (13)(24)
$G_{120} \subset S_6$	I, (13), (23), (123), (132), (12)

Degree 7

$G_{168} \subset S_7$	I, (356), (365), (34)(56),(354), (364), (456), (345), (36)(45), (465), (35)(46), (346), (47)(56), (35)(47), (36)(47), (243756), (243675), (243)(57), (2475), (247536), (247563), (246375), (246)(57), (246753), (24)(375), (24)(36)(57), (24)(567), (245)(37), (245736), (245673)
$G_{42} \subset S_7$	Let A be the set consisting of the even coset representatives for G_{168} in S_7. Let B be the set of all coset representatives for G_{21} in G_{168}. Then the required 120 coset representatives here are given by $A \cdot B$.
$G_{21} \subset G_{168}$	I, (37)(56), (23)(74), (2347)(56), (24)(56), (24)(37), (2743)(56), (27)(34)
$G_{14} \subset G_{42}$	I, (235)(476), (253)(467)
$G_7 \subset G_{21}$	I, (235)(476), (253)(467)

The degree-eight information is not given in this paper, since it has not been checked by actual computation.

Example 1. Let $p(x) = x^6 - 42x^4 + 80x^3 + 441x^2 - 1680x + 4516$. $p(x)$ can be shown to be irreducible over the rationals. Let Γ denote the Galois group of $p(x)$.

$$D(p(x)) = -2994775465327199186944,$$

clearly not a perfect square.

The roots of $p(x)$ are (approximately)

$$r_1 = 4.392 - 1.570i; \qquad r_2 = \bar{r}_1,$$
$$r_3 = -5.490 - 0.780i; \qquad r_4 = \bar{r}_3,$$
$$r_5 = 1.098 - 2.355i; \qquad r_6 = \bar{r}_5.$$

Let this be the initial ordering of the roots. The maximal subgroup G_{72} of S_6 has the ten right coset representatives

$$\pi_1 = \text{identity}, \qquad \pi_6 = (2453),$$
$$\pi_2 = (2543), \qquad \pi_7 = (25),$$
$$\pi_3 = (236)(45), \qquad \pi_8 = (2345),$$
$$\pi_4 = (25436), \qquad \pi_9 = (24536),$$
$$\pi_5 = (25)(34), \qquad \pi_{10} = (3645).$$

When the resolvent $Q_{(S_6, G_{72})}(y)$ is computed using the above data and the function $F(x_1, \cdots, x_6) = x_1x_2x_3 + x_4x_5x_6$ given in Table 1, we obtain

$$\begin{aligned} Q_{(S_6,\ G_{72})}(u) = {} & y^{10} + 80y^9 - 59166y^8 - 4390320y^7 \\ & + 1200615393y^6 + 88076918880y^5 \\ & - 7198940057856y^4 - 388801984512000y^3 \\ & + 20193311991398400y^2 \\ & + 595967000182784000y \\ & - 4689149328097280000. \end{aligned}$$

[The actual calculation of the resolvent was made carrying 192 bits of precision. With this precision, the coefficients of the resolvent were integers to within 2^{-96}.] The resolvent has a single integer root, -80, corresponding to the conjugate value $\pi_3(F)$, and no repeated roots. Consequently, $\Gamma \subset \pi_3 G_{72} \pi_3^{-1}$ and, after reordering the roots of $p(x)$ according to the rule $r_j' = r_{\pi_3(j)}$, we know that $\Gamma \subset G_{72}$. G_{72} has two maximal subgroups of order 36, G_{36}^1 and G_{36}^2. Since $G_{36}^1 \subset A_6$, and since we know that $D(p(x))$ is not a perfect square, $\Gamma \not\subset G_{36}^1$. Computing the resolvent $Q_{(G_{72}, G_{36}^2)}(y)$, we find

$$Q_{(G_{72}, G_{36}^2)}(y) = (y + 137376)(y - 137376)$$

and therefore $\Gamma \subset G_{36}^2$. Now, G_{36}^2 contains two isomorphic versions of G_{18} which are conjugate in G_{72} but not in G_{36}^2. Therefore, to test whether Γ is contained in some conjugate of G_{18}, one can either compute a single quartic resolvent, $Q_{(G_{72}, G_{18})}$, or a pair of quadratic resolvents $Q_{(G_{36}^2, G_{18})}$. Adopting the first course, G_{18} has the four right coset representatives {identity, (12)(45), (56), (12)(465)} in G_{72}. We then find

$$Q_{(G_{72}, G_{18})}(y) = (y + 360i)(y - 360i)(y + 648)(y - 648)$$

and we have $\Gamma \subset (56)G_{18}(56)$.

Reordering the roots of $p(x)$ again, using the interchange (56), we have $\Gamma \subset G_{18}$. Finally, G_{18} has the transitive subgroup G_6^1, and the resolvent associated with this subgroup turns out to be

$$G_{(G_{18}, G_6^1)}(y) = y^3 - 1323y + 7722 = (y - 33)(y - 6)(y + 39).$$

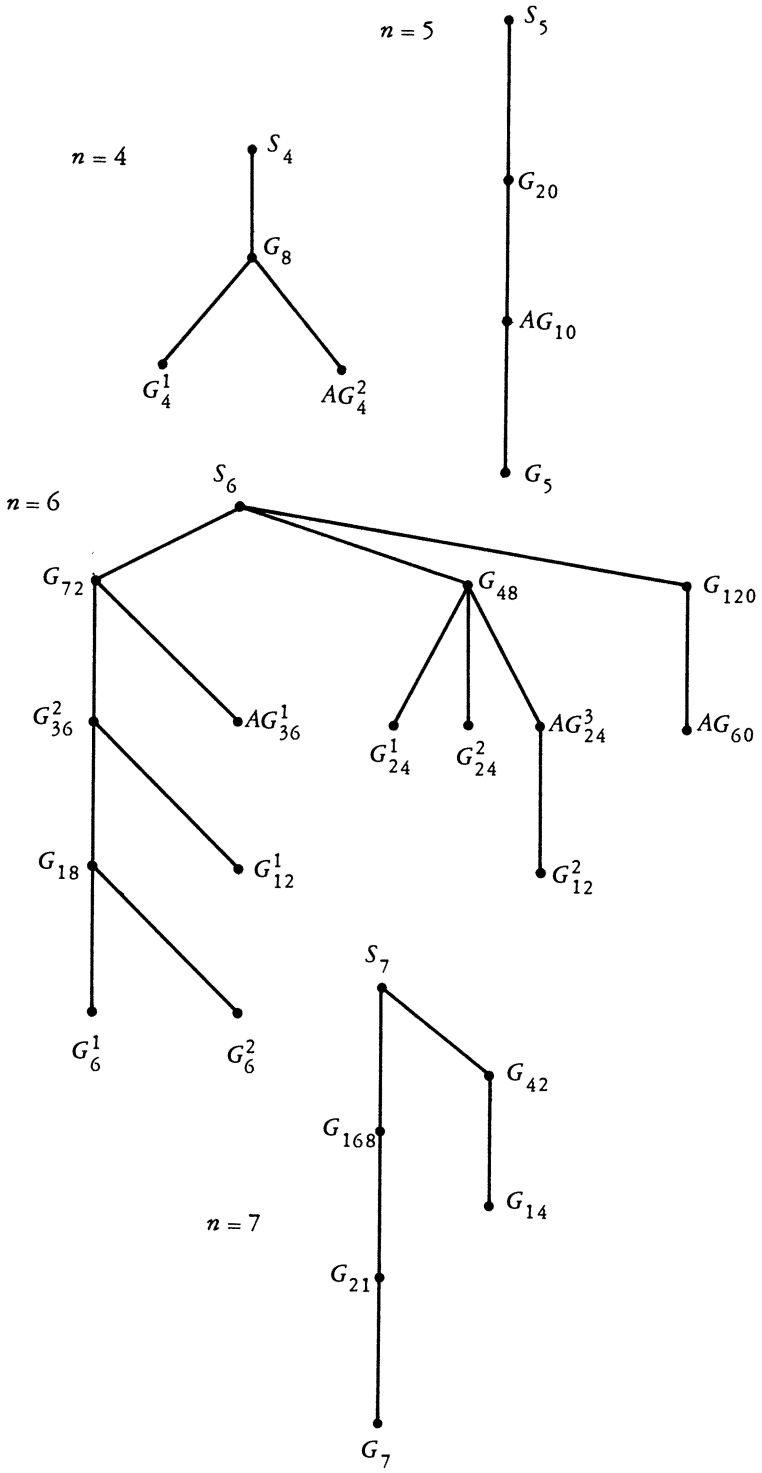
Thus, $\Gamma \subset G_6^1$, and since G_6^1 is a minimal transitive subgroup of S_6, $\Gamma = G_6^1$. Therefore, with respect to the final ordering

$$\begin{aligned} r_1 &= 4.392 - 1.570i; & r_2 &= -5.490 - 0.780i; \\ r_3 &= 1.098 + 2.355i; & r_4 &= 1.098 - 2.355i; \\ r_5 &= 4.392 + 1.570i; & r_6 &= -5.490 + 0.780; \end{aligned}$$

the Galois group of $p(x)$ is

identity
(123)(465)
(132)(456)
(14)(25)(36)
(15)(26)(34)
(16)(24)(35),

a group isomorphic to S_3.


n = 5
S5
G20
AG10
G5
n = 4
S4
G8
G4^1
AG4^2
n = 6
S6
G72
G48
G120
G36^2
AG36^1
G24^1
G24^2
AG24^3
AG60
G18
G12^1
G12^2
G6^1
G6^2
S7
G42
G168
G14
n = 7
G21
G7

Example 2. Let $p(x) = x^6 - 32x^4 + 160x^3 - 320x^2 + 384x - 256$. Again, $p(x)$ is irreducible over the rationals, and again we let Γ denote the Galois group of $p(x)$.

$$D(p(x)) = 403780252137947136 = (635437056)^2.$$

An initial ordering for the roots of $p(x)$ is

$$r_1 = 1.587; \qquad r_2 = 0.517 - 1.342i;$$
$$r_3 = \bar{r}_2; \qquad r_4 = 2.534 + 1.927i;$$
$$r_5 = \bar{r}_4; \qquad r_6 = -7.690.$$

This time, we obtain the resolvent

$$\begin{aligned} Q_{(S_6, G_{72})}(y) = {} & y^{10} + 160y^9 + 12544y^8 + 761856y^7 + 35586048y^6 \\ & + 1375731712y^5 + 39845888000y^4 \\ & + 935765999616y^3 + 15169824489472y^2 \\ & + 172073569746944y - 30786325577728 \end{aligned}$$

which proves to have no integer roots. Hence Γ is not contained in any of the conjugates of G_{72}.

We next compute a resolvent with respect to the maximal subgroup G_{48} of index 15 in S_6,

$$\begin{aligned} Q_{(S_6, G_{48})}(y) = {} & y^{15} + 96y^{14} + 4992y^{13} + 171520y^{12} \\ & + 4546560y^{11} + 99237888y^{10} \\ & + 1895104512y^9 + 31195136000y^8 \\ & + 448874414080y^7 + 5653059376768y^6 \\ & + 63843346677760y^5 + 606767209775104y^4 \\ & + 4504321181876224y^3 + 28162341078040576y^2 \\ & + 71405583642656768y + 0. \end{aligned}$$

This resolvent has the single integer root 0 corresponding to the conjugate value (23456)(F) of the function $F(x_1, \cdots, x_6) = x_1x_2 + x_3x_4 + x_5x_6$. After reordering the roots of $p(x)$ according to (23456), we have $\Gamma \subset G_{48}$. Since $D(p(x))$ is a perfect square, $\Gamma \subset G_{48} \cap A_6 = G_{24}^3$.

There is only one transitive subgroup of G_{24}^3 which is not also a subgroup of G_{72}. This group is G_{12}^2, and computing the resolvent $Q_{(G_{24}^3, G_{12}^2)}(y) = y^2 - 103424$, we find that $\Gamma = G_{24}^3$, since this resolvent has no integer roots. Thus, with respect to the final ordering

$$r_1 = 1.587, \qquad r_2 = -7.690,$$
$$r_3 = 0.517 - 1.342i, \qquad r_4 = \bar{r}_3,$$
$$r_5 = 2.534 + 1.927i, \qquad r_6 = \bar{r}_5$$

of the roots of $p(x)$, the Galois group Γ of $p(x)$ is a group of 24 even permutations, isomorphic to S_4. Generators for this group are given in Table 1.

Quadratic Factors of Resolvents. Suppose M_1 and M_2 are nonconjugate maximal transitive subgroups of S_n, and $p(x)$ is an irreducible polynomial of degree n with Galois group Γ. It has been shown, above, that a resolvent polynomial $Q_{(S_n, M_1)}(y)$ can be used to determine if Γ is a subgroup of some conjugate of M_1. This is done by searching, in effect, for linear factors of $Q_{(S_n, M_1)}$. It is sometimes possible to determine if Γ is a subgroup of another maximal transitive subgroup M_2 by searching for higher degree factors of $Q_{(S_n, M_1)}$. There are obvious practical advantages to this approach if $[S_n : M_1]$ is substantially smaller than $[S_n : M_2]$. For example, S_7 has two maximal transitive subgroups: G_{168}, of index 30, and G_{42}, of index 120. It turns out that by looking for quadratic factors of the resolvent $Q_{(S_7, G_{168})}$ of degree 30, one can avoid ever dealing with a resolvent of degree 120. (A similar situation occurs in the degree eight case.) A difficulty is encountered, however, in using quadratic factors of resolvents. Under certain circumstances a quadratic factor of $Q_{(S_n, M_1)}$ will guarantee that Γ is a subgroup of *some* conjugate of M_2, but will fail to specify exactly *which* conjugate. To put it another way, it is sometimes impossible to extract from the quadratic factor the information necessary to reorder the roots of $p(x)$. As it turns out, this unpleasant situation can always be avoided in the degree seven and degree eight cases. Even so, the procedure for obtaining reordering information from a quadratic factor is somewhat complicated and will not be discussed here.

2802 Webster
Berkeley, California 94705

0. J. BRILLHART, "On the Euler and Bernoulli polynomials," *J. Reine Angew. Math.*, v. 234, 1969, pp. 45–64.
1. W. BURNSIDE, *Theory of Groups of Finite Order*, Cambridge Univ. Press, London, 1897.
2. A. CAYLEY, "On the substitution groups for two, three,. . ., eight letters," *Quart. J. Pure Appl. Math.*, v. 25, 1891, pp. 71–88, 137–155.
3. F. N. COLE, "Note on the substitution groups of six, seven and eight letters," *Bull. New York Math. Soc.*, v. 2, 1893, pp. 184–190.
4. E. DEHN, *Algebraic Equations*, Columbia Univ. Press, New York; reprint, Dover, New York, 1960.
5. G. A. MILLER, "Note on substitution groups of eight letters," *Bull. New York Math. Soc.*, v. 3, 1894, pp. 168–169.
6. G. A. MILLER, "Note on the substitution groups of eight and nine letters," *Bull. New York Math. Soc.*, v. 3, 1894, pp. 242–245.
7. G. A. MILLER, "Note on Burnside's theory of groups," *Bull. Amer. Math. Soc.*, v. 5, 1899, pp. 249–251.
8. B. VAN DER WAERDEN, *Modern Algebra*. Vol. I, Ungar, New York, 1953.