MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 178
APRIL 1987, PAGES 781–797

On Invariant Polynomials and Their Application in Field Theory

By Kurt Girstmair

Abstract. Certain polynomials invariant under a permutation group G (so called G-polynomials) play an important role in several computational methods of Galois theory. Since their practical value depends on the degree, it is important to know G-polynomials of smallest possible degree. A reasonable technique to find such G-polynomials is presented, and for certain classes of groups an explicit description is obtained. The list of G-polynomials given by Stauduhar in vol. 27 of this journal is thereby enlarged and improved. As an application of G-polynomials, three important resolvents of quintic and sextic algebraic equations are computed and a parametric family of sextic equations with given Galois group is exhibited.

Introduction. Let K be a field and $X_1, \ldots, X_m$ indeterminates. Let S_m be the group of all permutations of $1, \ldots, m$, which acts on the polynomial ring $K[X_1, \ldots, X_m]$ by $s \circ X_i = X_{s(i)}$, $s \in S_m$, $i = 1, \ldots, m$. Let G be a subgroup of S_m. Several problems in field theory—e.g., the determination of the Galois group or the computation of a Galois resolvent of a given algebraic equation—can be solved explicitly, if one can do the following (see [7, p. 276], [16], [11], [2], [3] and references in the last paper):

I. *Find* a polynomial P *belonging to* G (also called a *G-polynomial*), i.e., a polynomial P in $K[X_1, \ldots, X_m]$ whose stabilizer $\{s \in S_m \mid s \circ P = P\}$ is *equal* to G.

II. Let Z be an additional indeterminate and $\sigma_1, \ldots, \sigma_m$ the elementary symmetric functions defined by $(Z - X_1) \cdots (Z - X_m) = Z^m + \sigma_1 Z^{m-1} + \cdots + \sigma_m$. Let $R \in K[X_1, \ldots, X_m][Z]$ be the polynomial of Z-degree $[S_m : G]$ whose zeros in $K[X_1, \ldots, X_m]$ are the elements of $\{s \circ P \mid s \in S_m\}$. *Find* the unique polynomial $R^+ \in K[X_1, \ldots, X_m][Z]$ such that $R = R^+(\sigma_1, \ldots, \sigma_m, Z)$.

Suppose that Problems I and II have been solved for $G \subseteq S_m$. If $f = Z^m + a_1 Z^{m-1} + \cdots + a_m \in K[Z]$ is a polynomial with coefficients in K and splitting field $K(f)$, then $R^+(a_1, \ldots, a_m, Z)$ is a certain *resolvent* of f, i.e., its splitting field is a subfield of $K(f)$. The prime factor decomposition of $R^+(a_1, \ldots, a_m, Z)$ in $K[Z]$, for example, gives insight into the relation between G and the Galois group $G(f) = \mathrm{Gal}(K(f)/K)$ of f. By this method one can determine the group $G(f)$ (loc. cit.).

Up to now, actual solutions of Problem II exist only in very few cases: If G is the alternating group A_m, take $R^+ = Z^2 - D$, where D is the discriminant of $Z^m + X_1 Z^{m-1} + \cdots + X_m$. For subgroups G of S_m, $m \leqslant 4$, see [10, p. 72 ff]. If $m = 5$ and

Received September 16, 1982.
1980 *Mathematics Subject Classification.* Primary 12-04, 12F10, 20B99.

0025-5718/87 $1.00 + $.25 per page

G is a maximal solvable transitive subgroup of S_5, a polynomial R^+ could be derived from a general resolvent given by Cayley [1] in the way described in [18, p. 674].

Note that for $K = \mathbf{Q}$ one can evade the explicit computation of R^+, because P and a given $f \in \mathbf{Q}[Z]$ can be supposed to have *integral* coefficients. They allow us to obtain a numerical approximation of $R^+(a_1, \ldots, a_m, Z) \in \mathbf{Z}[Z]$, and thus $R^+(a_1, \ldots, a_m, Z)$ itself (see [16]). However, for several reasons it is desirable to know R^+ *itself*: The method becomes applicable to *arbitrary* fields K, the computation of $R^+(a_1, \ldots, a_m, Z)$ is considerably simplified, and sometimes R^+ is useful in the construction of parametric families of polynomials with a given Galois group (an example for this is Proposition 6).

In Section 3 we consider three especially important groups G_n, $n \in \{20, 72, 120\}$, where the subscript denotes the order of the group. Let R_n^+ be the polynomial R^+ corresponding to G_n. We describe the computation of $R_n^* = R_n^+(0, X_2, \ldots, X_m, Z)$ and give the result in Table 2. Since the coefficient a_1 of a given f can be easily removed, there is no loss of generality in taking R_n^* instead of R_n^+. Let us outline the import of the polynomials R_n^*.

The group G_{20} is the maximal solvable transitive subgroup of S_5 mentioned above (it is unique up to conjugation). Suppose that $f = Z^5 + a_2Z^3 + a_3Z^2 + a_4Z + a_5 \in K[Z]$ is irreducible. If $R_{20}^*(a_2, \ldots, a_5, Z)$ has no multiple roots (for infinite ground fields K this can always be attained, cf. [3]), then f is solvable if and only if $R_{20}^*(a_2, \ldots, a_5, Z)$ has a zero in K. One can decide the latter property in many fields K, so we may say that R_{20}^* *decides the solvability of irreducible quintic equations*. The groups G_{72} and G_{120} are maximal transitive subgroups of S_6. In [3] it has been shown that R_{120}^* (whose Z-degree is 6), together with some discriminants, allows us to find the Galois group of an irreducible sextic polynomial in *most cases*. The remaining cases are settled by R_{72}^* (of Z-degree 10).

In principle, it is easy to solve Problem I, if the group G in question is sufficiently well known (cf. [7, p. 54], [16, Theorem 1]). But in many applications the G-polynomial is a crucial point. Most of all, its *degree* strongly influences further calculations and can make them impracticable. For example, the only G_{120}-polynomial known in the literature is of degree 10 (it goes back to the paper [14] of Serret in 1850, cf. also [16]; in [18, p. 679] Weber wrongly claims the existence of such a polynomial of degree 4). The computation of the corresponding polynomial R_{120}^* requires the solution of a system of linear equations in 758 unknowns. This is hard to do for a computer, chiefly for reasons of memory capacity. However, the lowest possible degree of a G_{120}-polynomial P is 6. Our polynomial R_{120}^* is based on a sextic P; the number of unknowns is thereby reduced to 177, a problem we could manage much better (the memory capacity needed amounts to 5% of the degree 10 case).

Stauduhar [16] gives a useful list of G-polynomials of low degrees for most of the transitive subgroups of S_m, $m \leqslant 7$, which he has partially collected from the literature. The groups omitted are not of interest from his point of view. But like his G_{120}-polynomial, his G_{72}-polynomial is not of lowest possible degree, and two other polynomials (cf. the remark in Section 2) in his list do not belong to the group they should (however, they fulfil their purpose within the scope of [16]). Most of his G-polynomials seem to be *ad hoc* constructions.

The above discussion will show that it is desirable *to get some insight into the constitution of G-polynomials.* This problem is the subject of the largest part of the present paper. It dates back to C. Jordan and contemporaries. Following their ideas, we give a methodical framework for the treatment of this question (Section 1). We thereby obtain a practicable algorithm to find the lowest possible degree of a G-polynomial, as well as G-polynomials of this degree. A refined version of this procedure has been used to establish Table 1 (Section 2), a supplement to the list of [16]. Combined with recent theorems on permutation groups, our method yields an explicit description of all types of G-polynomials (and the degrees they can take) for the class of groups $G \subseteq S_m$ such that each larger group is either S_m or A_m (Section 2, Theorem 1). Furthermore, the possible types of lowest degree are given for the solvable transitive subgroups of S_m, m prime (Theorem 2).

1. Invariants, Essential Sets, and a Problem of Jordan. For the time being, it suffices to assume that K is a commutative ring with identity 1 ($\neq 0$). We continue to use the notations of the Introduction. We write $K[X] = K[X_1, \ldots, X_m]$. A *partition* of $\{1, \ldots, m\}$ is a tuple $T = (T_1, \ldots, T_r)$ of sets $T_j \subseteq \{1, \ldots, m\}$ such that $\dot{\bigcup}_{j=1}^{r} T_j = \{1, \ldots, m\}$ and $|T_1| \geqslant \cdots \geqslant |T_r| \geqslant 1$ ("$\dot{\cup}$" denotes the disjoint union, "$|\ |$" the number of elements of the corresponding set). The tuple $(|T_1|, \ldots, |T_r|)$ is called the *type* of T; more generally, a tuple $t = (t_1, \ldots, t_r)$ of integers with $t_1 \geqslant \cdots \geqslant t_r \geqslant 1$ and $t_1 + \cdots + t_r = m$ is called a *type for* m. By $\mathscr{T}$ we denote the set of all partitions of $\{1, \ldots, m\}$ and by $\mathscr{T}(t)$ the set of partitions of type $t = (t_1, \ldots, t_r)$.

Now fix a monomial $Q = X_1^{n_1} \cdots X_m^{n_m}$ in $K[X]$. For $k \in \mathbf{N}_0$ (= set of nonnegative integers) we put $T(k) = \{ j \in \{1, \ldots, m\} \mid n_j = k \}$. Starting with the largest set $T(k)$, we arrange all nonempty sets $T(k)$, $k \in \mathbf{N}_0$, *descending* with their cardinality; whenever in this process we arrive at two or more sets $T(k)$ of equal size, we order them *ascending* with the size of k. We thereby obtain a partition T of $\{1, \ldots, m\}$ uniquely determined by Q. (It will be seen later [Proposition 4 and corollary] why T is arranged in *this* way.) For example, if $m = 6$ and $Q = X_1^3 X_4^2 X_5^2 X_6$, T is $(\{2, 3\}, \{4, 5\}, \{6\}, \{1\})$. Moreover, the assignment $Q \mapsto T = (T_1, \ldots, T_r)$ yields a unique tuple $i = (i_1, \ldots, i_r) \in \mathbf{N}_0^r$, which is defined by the property

$$Q = \Big(\prod_{j \in T_1} X_j \Big)^{i_1} \cdots \Big(\prod_{j \in T_r} X_j \Big)^{i_r}.$$

For the right side of this equation we write T^i. Note that i is in the set $I_T = \{(i_1, \ldots, i_r) \in \mathbf{N}_0^r \mid i_j \text{ all distinct}, i_j < i_{j+1} \text{ if } |T_j| = |T_{j+1}|\}$. We obtain

PROPOSITION 1. $K[X_1, \ldots, X_m] = \oplus_{T \in \mathscr{T}} (\oplus_{i \in I_T} K T^i)$.

As usual, $\oplus$ denotes the direct sum of K-modules. Observe that the set I_T only depends on the type of T. We call I_T the set of exponents for T.

In the sequel let G be a *fixed* subgroup of S_m. The group S_m acts in a natural way on the set $\mathscr{T}$ of partitions of $\{1, \ldots, m\}$; namely, for $T = (T_1, \ldots, T_r) \in \mathscr{T}$ one defines $s \circ T = (s(T_1), \ldots, s(T_r))$, $s \in S_m$. By $\mathscr{T}/G$ we denote the set of *orbits* $\{ G \circ T \mid T \in \mathscr{T} \}$ of G in $\mathscr{T}$, and by $\mathscr{T}//G$ a *system of representatives* of these orbits (i.e., a subset $\mathscr{U} \subseteq \mathscr{T}$ which contains exactly one element from each orbit). We fix

$\mathscr{T}//G$ in what follows. Let $T \in \mathscr{T}$ and $i \in I_T$. Then $N_G(T^i) := \Sigma(T''^i \mid T' \in G \circ T)$ is called the *reduced norm* of T^i under G. It is an element of the *G-invariant ring* ${}^GK[X] = \{Q \in K[X] \mid s \circ Q = Q \text{ for all } s \in G\}$. ${}^GK[X]$ contains all G-polynomials, and Proposition 1 implies

PROPOSITION 2. ${}^GK[X] = \oplus_{T \in \mathscr{T}//G}(\oplus_{i \in I_T} KN_G(T^i))$.

Let $\mathscr{U}$ be a subset of $\mathscr{T}//G$. We consider $\underline{P}(\mathscr{U}) = \{\Sigma_{T \in \mathscr{U}} \Sigma_{i \in I_T} a_{T,i} N_G(T^i) \mid \text{for each } T \in \mathscr{U} \text{ there is an } i \in I_T \text{ such that } a_{T,i} \neq 0\} \subseteq {}^GK[X]$. By Proposition 2,

$$ {}^GK[X] = \dot{\cup}(\underline{P}(\mathscr{U}) \mid \mathscr{U} \subseteq \mathscr{T}//G). $$

Thus we have divided ${}^GK[X]$ into a finite number of subsets, which we shall investigate more closely. Consider the action of S_m on the *subsets* $\mathscr{U}$ of $\mathscr{T}$, defined by $s \circ \mathscr{U} = \{s \circ T \mid T \in \mathscr{U}\}$, $s \in S_m$. Let $\mathrm{Stab}(\mathscr{U})$ be the *stabilizer* of $\mathscr{U}$ in S_m, $\mathrm{Stab}(\mathscr{U}) = \{s \in S_m \mid s \circ T \in \mathscr{U} \text{ for all } T \in \mathscr{U}\}$. Of particular interest are the stabilizers $\mathrm{Stab}(G \circ T)$ of the orbits $G \circ T$ of G (obviously, they contain G). For $\mathscr{U} \subseteq \mathscr{T}$ we define an *exponent distribution* $(J_T)_{T \in \mathscr{U}}$ as a family of nonempty finite subsets $J_T \subseteq I_T$, $T \in \mathscr{U}$. If $\mathscr{U} \subseteq \mathscr{T}//G$ and $P \in \underline{P}(\mathscr{U})$, we write $P = \Sigma_{T \in \mathscr{U}} \Sigma_{i \in J_T} a_{T,i} N_G(T^i)$, with J_T such that $a_{T,i} \neq 0$ for all $i \in J_T$. The family $(J_T)_{T \in \mathscr{U}}$ is called *the exponent distribution of* P.

PROPOSITION 3. *Let $\mathscr{U}$ be a subset of $\mathscr{T}//G$, and let $P \in \underline{P}(\mathscr{U})$ have the above shape. Put $G(\mathscr{U}) = \bigcap_{T \in \mathscr{U}} \mathrm{Stab}(G \circ T)$. Then P belongs to a group H that contains $G(\mathscr{U})$. H is equal to $G(\mathscr{U})$, provided there are no partitions $T \neq T'$ in $\mathscr{U}$ of the same type with $J_T = J_{T'}$ and $a_{T,i} = a_{T',i}$ for all $i \in J_T$. In particular, if K has infinitely many elements, $\underline{P}(\mathscr{U})$ always contains $G(\mathscr{U})$-polynomials.*

The proof is based on Propositions 1, 2 and is left to the reader. A set $\mathscr{U} \subseteq \mathscr{T}//G$ will be called *essential* if $G(\mathscr{U}) = G$. It follows from Proposition 3 that G-polynomials in $K[X]$ can be found only in sets $\underline{P}(\mathscr{U})$ for *essential* $\mathscr{U}$'s. If K is infinite, such sets $\underline{P}(\mathscr{U})$ actually contain G-polynomials; one can even prescribe their exponent distribution. If $\mathscr{U} \subseteq \mathscr{T}//G$ is essential, every set $\mathscr{V}$ with $\mathscr{U} \subseteq \mathscr{V} \subseteq \mathscr{T}//G$ is essential, too. Therefore we get a good overview over all G-polynomials, if we can solve

Problem III. Determine all *minimal essential sets* $\mathscr{U} \subseteq \mathscr{T}//G$.

In his "Traité" C. Jordan proved the existence of essential sets consisting of *one* partition (cf. Section 2). He raised several problems concerning G-polynomials. One of them can be reformulated in the following way (cf. [7, p. 54]): Determine all sets $\underline{P}(\{T\})$ with $\{T\} \subseteq \mathscr{T}//G$ essential (such a $\underline{P}(\{T\})$ he calls "family of elementary functions belonging to G"). This is an important special case of Problem III. It is clear that one can solve Problem III for each individual permutation group G in finitely many steps. In most cases, however, this is not an easy task. Theorem 1 will give the solution for a large class of groups that admit a relatively simple answer.

PROPOSITION 4. *Let $T = (T_1, \ldots, T_r)$ be a partition of $\{1, \ldots, m\}$. Among all polynomials T^i, $i \in I_T$, there is exactly one of smallest degree, namely $T^{(0,1,\ldots,r-1)}$; its degree is $w(T) = |T_2| + 2|T_3| + \cdots + (r-1)|T_r|$.*

The proof is omitted. We call $i_0(T) = (0, 1, \ldots, r-1) \in I_T$ the *minimal exponent* of T, and $w(T)$ the *weight* of T. Both minimal exponent and weight depend only on the *type* of T. For $\mathscr{U} \subseteq \mathscr{T}$ we define the *weight* of $\mathscr{U}$ as $w(\mathscr{U}) = \max\{w(T) \mid T \in \mathscr{U}\}$

if $\mathcal{U} \neq \emptyset$, and $w(\emptyset) = -\infty$. One obtains the important

COROLLARY. *Let $\mathcal{U} \subseteq \mathcal{T}//G$. Then $\deg(P) \geqslant w(\mathcal{U})$ for all $P \in \underline{P}(\mathcal{U})$. The degree $w(\mathcal{U})$ is taken by each polynomial in $\underline{P}(\mathcal{U})$ whose exponent distribution is the family $(i_0(T))_{T \in \mathcal{U}}$ of minimal exponents.*

Let K be *infinite*. In view of Propositions 3, 4 and the corollary, all G-polynomials of smallest possible degree can be formed if we know $d = \min\{w(\mathcal{U}) \mid \mathcal{U} \subseteq \mathcal{T}//G, \mathcal{U}$ essential$\}$ and all minimal essential sets of weight d (call them $\mathcal{V}_1, \ldots, \mathcal{V}_k$). In the sequel we describe the main features of an *algorithm* to find d and one set $\mathcal{V}_l$, $l \in \{1, \ldots, k\}$. It may happen, however, that the (always existing) G-polynomials in $\underline{P}(\mathcal{V}_l)$ are not yet best possible for applications. By means of some modifications, which are not difficult but tedious, the algorithm produces a subsystem of $\mathcal{V}_1, \ldots, \mathcal{V}_k$ that meets most practical requirements (for a short discussion, see explanations to Table 1 and Section 3). Table 1 is based on this enlarged version.

ALGORITHM. Compute all types for the number m and order them in some way, ascending with their weight. Let $w_1 < w_2 < \cdots$ be the set of all weights occurring. Construct in every step a group G_j and a set $\mathcal{U}_j$ in the following way:

Put $G_0 = S_m$, $\mathcal{U}_0 \neq \emptyset$. Stop if $G = S_m$; otherwise, put $j = 1$.

(*) Take all types $t = (t_1, \ldots, t_r)$ of weight $w(t) = w_j$. Establish for these t a system of representatives $\mathcal{T}(t)//G$ of the orbits of G in $\mathcal{T}(t)$ (note that $|\mathcal{T}(t)| = m!/(t_1! \cdots t_r!)$). Put $\mathcal{T}_j = \bigcup(\mathcal{T}(t)//G \mid w(t) = w_j)$. Compute $G(\mathcal{T}_j)$ (notation of Proposition 3), and put $G_j = G(\mathcal{T}_j) \cap G_{j-1}$. If $G_j = G_{j-1}$, put $\mathcal{U}_j = \mathcal{U}_{j-1}$, increase j by 1 and go to (*); otherwise, *minimize* $\mathcal{T}_j$, i.e., replace $\mathcal{T}_j$ by a minimal subset $\mathcal{T}_j'$ of $\mathcal{T}_j$ with $G(\mathcal{T}_j') = G(\mathcal{T}_j)$. If $G_{j-1} \supseteq G(\mathcal{T}_j)$ put $\mathcal{U}_j = \mathcal{T}_j$; otherwise, put $\mathcal{U}_j = \mathcal{U}_{j-1} \cup \mathcal{T}_j$ and minimize $\mathcal{U}_j$. Stop when $G_j = G$; otherwise, increase j by 1 and go to (*). The final set $\mathcal{U}_j$ has the desired property.

2. Explicit Description of G-Polynomials for Certain Classes of Groups. We adopt the notations above (K a commutative ring with $1 \neq 0$). Let $G \subseteq S_m$ be a subgroup, $T \in \mathcal{T}//G$. In [7, p. 54], Jordan has shown that $\{T\}$ is essential if the type of T is $(1, \ldots, 1)$. Moreover, he showed

PROPOSITION 5. *Let G be a k-fold transitive proper subgroup of S_m, $T = (T_1, \ldots, T_r) \in \mathcal{T}//G$. Suppose that $\{T\}$ is essential. Then $|T_1| \leqslant m - (k+1)$.*

Indeed, it is easy to see that otherwise $G \circ T = S_m \circ T$, i.e., $\mathrm{Stab}(G \circ T) = S_m$. The $(m-2)$-fold transitivity of A_m and the corollary of Proposition 4 yield

COROLLARY. *A subset $\mathcal{U} \subseteq \mathcal{T}//A_m$ is essential if and only if $\mathcal{U}$ contains a T of type $(1, \ldots, 1)$. In particular, the minimal degree d of an A_m-polynomial is $m(m-1)/2$ (which is assumed by $\prod_{j<k}(X_j - X_k)$, the root of the discriminant of $Z^m + \sigma_1 Z^{m-1} + \cdots + \sigma_m$).*

In what follows we say that a subgroup of S_m is *A_m-maximal* if it is $\neq S_m$, A_m and maximal in the set $\{G \subseteq S_m \mid G \neq S_m, A_m\}$. The A_m-maximal groups play an important role in the computation of Galois groups, cf. [16]. For most of them, Problem III is solved simply by the converse of Proposition 5, namely

THEOREM 1. *Let $G \subseteq S_m$ be a k-fold, but not $(k+1)$-fold transitive A_m-maximal subgroup of S_m ($k = 0$, if G is intransitive).*

1. *A subset* $\mathscr{U} \subseteq \mathscr{T}//G$ *is essential if and only if it contains a partition* $T = (T_1, \ldots, T_r)$ *with*

(a) $|T_1| \leqslant m - (k+1)$, *if* G *is none of the groups* $P\Gamma L(2,8)$ $(\subseteq S_9)$, $P\Gamma L(2,32)$ $(\subseteq S_{33})$,

(b) $|T_1| \leqslant m - (k+2)$, *or* $|T_1| = m - (k+1)$ *and* $|T_2| = 1$, *if* $G = P\Gamma L(2,8)$ $(m = 9,\ k = 3)$,

(c) $|T_1| \leqslant m - (k+2)$, *or* $|T_1| = m - (k+1)$ *and* $|T_2| \leqslant 2$, *if* $G = P\Gamma L(2,32)$ $(m = 33,\ k = 3)$.

2. *The smallest degree* d *of a* G*-polynomial is* $d = k + 1$, *except in the cases*

$$G = \begin{cases} AGL(1,5) \subseteq S_5, & d = 4\ (k = 2), \\ PGL(2,5) \subseteq S_6, & d = 6\ (k = 3), \\ P\Gamma L(2,8) \subseteq S_9, & d = 6\ (k = 3), \\ P\Gamma L(2,32) \subseteq S_{33}, & d = 5\ (k = 3). \end{cases}$$

Remark. The notation of groups in Theorem 1 is that of [8] (cf. also [6] and the introductory remarks to Theorem 2). The groups $AGL(1,5)$ and $PGL(2,5)$ are the groups G_{20} and G_{120} of [16] and the Introduction. All groups are uniquely determined up to conjugation only. They are actually A_m-maximal, as one can see from the table in [15] and Corollary 4.4 in [13]. It is very likely that each 6-fold transitive subgroup of S_m contains A_m (cf. [17], [5, p. 55]). Then the number d would be $\leqslant 6$, for all A_m-maximal groups G.

Proof of Theorem 1. The proof of assertion 1 is based on some results which have been used to prove Theorem 4 in [3]. We note that $\mathscr{U} \subseteq \mathscr{T}//G$ is essential if and only if there is a $T = (T_1, \ldots, T_r) \in \mathscr{U}$ such that $G \circ T$ is *not* the whole set $\mathscr{T}(t)$, where $t = (t_1, \ldots, t_r)$ is the type of T. The necessity of this condition is clear, since $\mathrm{Stab}(\mathscr{T}(t)) = S_m$. The sufficiency follows from $A_m \circ T = S_m \circ T = \mathscr{T}(t)$ for $t_1 \geqslant 2$, resp. $|A_m \circ T| = |A_m| > |G| = |G \circ T|$ for $t_1 = 1$, and the A_m-maximality of G.

Now let $T \in \mathscr{T}$ be of type $t = (t_1, \ldots, t_r)$ with $t_1 \leqslant m - (k+1)$. Suppose that $G \circ T = \mathscr{T}(t)$. We distinguish two cases:

(i) $t_1 \geqslant m/2$. Since $m - t_1 \leqslant t_1$, $(t_1, m - t_1)$ is a *type* for m and, by assumption, G acts transitively on $\mathscr{T}(t_1, m - t_1)$. A theorem of Livingstone, Wagner, and Kantor [8, Theorem 1] implies that G is $(m - t_1)$-fold transitive or $m = 9$, $G = P\Gamma L(2,8)$, $m = 33$, $G = P\Gamma L(2,32)$. Since $m - t_1 \geqslant k + 1$, only the latter two cases are possible.

(ii) $t_1 < m/2$. There is a subset $M \subseteq \{1, \ldots, r\}$ such that $t_2' := \Sigma(t_j \mid j \in M)$ fulfils $m/3 \leqslant t_2' \leqslant m/2$. This is elementary (cf. Lemma 4 in [3]). Since G is transitive on $\mathscr{T}(m - t_2', t_2')$, Theorem 1 in [8] yields $k \geqslant m/3$. However, A_m-maximal groups with $k \geqslant m/3$ can occur only for $m \leqslant 12$ (this follows, e.g., from Lemmas 1, 2 in [3] and the table in [15]), namely: $AGL(1,5)$, $PGL(2,5)$, $PGL(2,7)$ $(\subseteq S_8)$; the holomorph of the group $(\mathbf{Z}/2\mathbf{Z})^3$ $(\subseteq S_8)$, $P\Gamma L(2,8)$, and the Mathieu groups M_{11} $(\subseteq S_{11})$, M_{12} $(\subseteq S_{12})$.

Thus we have proved assertion 1 up to the exceptional groups in (i) and (ii), which require separate considerations. In most cases one can work with divisibility properties, as we exemplify for the group $PGL(2,5)$. By (ii) we have to treat the types $(2,2,2)$, $(2,2,1,1)$, $(2,1,1,1,1)$, and $(1,1,1,1,1,1)$. It suffices to show that G cannot be transitive on $\mathscr{T}(2,2,2)$. If this were not true, $|\mathscr{T}(2,2,2)| = 6!/(2!)^3 = 90$ would

divide $|G| = 120$, a contradiction. Observe also that $P\Gamma L(2,8)$ (resp. $P\Gamma L(2,32)$) is a *regular* permutation group on $\mathcal{T}(5,2,1,1)$ (resp. $\mathcal{T}(29,3,1)$).

As to assertion 2, consider the types $t = (t_1, \ldots, t_r)$ with $t_1 \leqslant m - (k+1)$. Among them, $(m-(k+1), k+1)$ has smallest weight and is unique with this property, except when $k+1 > m-(k+1)$, i.e., $k > m/2 - 1$. This can happen only for $m = 5, 6$. The exceptional cases are easy. □

Let p be a prime number and $\mathbf{F}_p$ the field with p elements. Consider $AGL(1,p) = \{l_{a,b} \mid a \in \mathbf{F}_p \setminus \{0\},\ b \in \mathbf{F}_p\}$, the group of maps $l_{a,b}: \mathbf{F}_p \to \mathbf{F}_p$: $c \mapsto ac + b$. A *transitive solvable subgroup* $G \subseteq S_p$ is isomorphic to a subgroup of $AGL(1,p)$. In particular, $|G|$ divides $p(p-1)$. Using theorems of P. M. Neumann [12], [13], we give a rather complete description of minimal essential sets of smallest weight for these groups G.

THEOREM 2. *Let G be a transitive solvable subgroup of S_p, p prime. Let $\mathcal{T}//G = \bigcup(\mathcal{T}(t)//G \mid t$ a type for $p)$ be a system of representatives of $\mathcal{T}/G$ and $d = \min\{w(\mathcal{U}) \mid \mathcal{U} \subseteq \mathcal{T}//G,\ \mathcal{U}$ essential$\}$.*

1. Let $|G|$ be even. The minimal essential sets of weight d are all subsets $\mathcal{U} \subseteq \mathcal{T}(t)//G$ with $|\mathcal{U}| = 1$, where

(a) *$d = 2$ and $t = (p-2, 2)$ if $|G| < p(p-1)$,*

(b) *$d = 3$ and $t = (p-3, 3)$ if $|G| = p(p-1)$ and $p \geqslant 7$,*

(c) *$d = 4$ and $t = (2,2,1)$ if $|G| = p(p-1)$ and $p = 5$,*

(d) *$d = -\infty$ if $p = 2, 3$.*

2. If G is odd, d is equal to 3. There exist the following categories of essential sets of weight 3:

(a) *All subsets $\mathcal{U} \subseteq \mathcal{T}(p-2,1,1)//G$ with $|\mathcal{U}| = 1$.*

(b) *If $p \geqslant 7$, the set $\mathcal{T}(p-3,3)//G$.*

(c) *If $p \geqslant 7$ and $|G| < p(p-1)/2$, certain sets $\{T, T'\}$ with $T \in \mathcal{T}(p-2,2)//G$, $T' \in \mathcal{T}(p-3,3)//G$.*

Every minimal essential set is contained in a set (a), (b) *or* (c).

Remark. If $|G|$ is odd and $p \geqslant 7$, there are always nonempty subsets $\mathcal{U} \subseteq \mathcal{T}(p-3,3)//G$ that are *not* essential. If, in addition, $p \equiv 1 \bmod 3$, there always exist *minimal* essential sets of category 2(c). Both assertions become clear from the proof. Recall that a good knowledge of all minimal essential sets of weight d can be of advantage in applications (cf. Section 3).

Proof of Theorem 2. We identify S_p with the symmetric group of $\mathbf{F}_p$ in such a way that $G \subseteq AGL(1,p) = \{l_{a,b} \mid a \in \mathbf{F}_p \setminus \{0\},\ b \in \mathbf{F}_p\}$. The types of weight $\leqslant 3$ are: (p) of weight 0, $(p-1,1)$ of weight 1, $(p-2,2)$ of weight 2, and $(p-3,3)$ and $(p-2,1,1)$ of weight 3.

If T is a partition of weight $\leqslant 1$, $G \circ T = S_p \circ T$. Thus d is $\leqslant 1$ only if $G = S_p$. This is case 1(d). Let $T \in \mathcal{T}(p-2,2)$ and $H \subseteq S_p$ be a group containing G. If H is *not* solvable, it is doubly transitive (by a theorem of Burnside), hence $H \circ T = \mathcal{T}(p-2,2)$. For solvable H, $|H \circ T| = |H|$ if $|H|$ is odd, and $|H \circ T| = |H|/2$, otherwise. Therefore, if $|G|$ is even and $< p(p-1)$, we have always $|H \circ T| > |G \circ T|$ for $H \supseteq G$, $H \neq G$. Hence 1(a) follows.

Next let $|G| = p(p-1)$, i.e., $G = AGL(1,p)$. The case 1(c) being contained in Theorem 1, we may assume $p \geqslant 7$. Because of the transitivity of G on $\mathcal{T}(p-2,2)$ and $\mathcal{T}(p-1,1,1)$, d must be $\geqslant 3$, and a minimal essential set of weight 3 is in

$\mathscr{T}(p-3,3)$ (if there is any). Let $T \in \mathscr{T}(p-3,3)$. Every group $H \supseteq G$, $H \neq G$, is triply transitive, by [12]; thus $H \circ T = \mathscr{T}(p-3,3)$. On the other hand, $G \circ T \neq \mathscr{T}(p-3,3)$, for otherwise, $|\mathscr{T}(p-3,3)|$ would divide $p(p-1)$. This proves 1(b).

Now suppose that $|G|$ is *odd*. Let G' be the group generated by G and $l_{-1,0} \in AGL(1,p)$ (G' is the unique subgroup of $AGL(1,p)$ of order $2|G|$). For $T \in \mathscr{T}(p-2,2)$ the arguments in the proof of 1(a) yield

$$(*) \qquad \operatorname{Stab}(G \circ T) = \begin{cases} S_p & \text{if } |G| = p(p-1)/2, \\ G' & \text{if } |G| < p(p-1)/2. \end{cases}$$

Therefore $d \geqslant 3$. For $T \in \mathscr{T}(p-2,1,1)$ and $H \supseteq G$ we obtain $|H \circ T| = |H|$ if H is solvable, and $|H \circ T| = p(p-1)$, otherwise. This implies 2(a).

In the sequel, let $p \geqslant 7$. Let u, v, w be distinct elements of $\mathbf{F}_p$ and $T_{uvw} = (\mathbf{F}_p \setminus \{u,v,w\}, \{u,v,w\}) \in \mathscr{T}(p-3,3)$. By $G(u,v,w)$ we denote the stabilizer of T_{uvw} in $AGL(1,p)$, i.e., $G(u,v,w) = \{s \in AGL(1,p) \mid s \circ T_{uvw} = T_{uvw}\}$. Some calculations show that

$$|G(u,v,w)| = \begin{cases} 3 & \text{if } p \equiv 1 \bmod 3 \text{ and } w \in \{(u+v \pm \sqrt{-3}(u-v))/2\}, \\ 2 & \text{if } w \in \{(u+v)/2, 2u-v, 2v-u\}, \\ 1 & \text{otherwise,} \end{cases}$$

where $\sqrt{-3}$ is in $\mathbf{F}_p$. Let $|G| < p(p-1)/2$. By (*), $\operatorname{Stab}(G \circ T) = G'$ for each $T \in \mathscr{T}(p-2,2)$; moreover, $|G' \circ T_{uvw}| > |G \circ T_{uvw}|$ if and only if $|G(u,v,w)| \neq 2$. Hence a subset $\mathscr{U} \subseteq \mathscr{T}(p-2,2)//G \cup \mathscr{T}(p-3,3)//G$ with at least one element in $\mathscr{T}(p-2,2)//G$ is essential if and only if it contains a T_{uvw} with $|G(u,v,w)| \neq 2$. This shows 2(c).

Finally, we exhibit an essential subset of $\mathscr{T}(p-3,3)//G$. If $H \supseteq G$ and H is not solvable, it has at most $1 + p(p-1)/(2|G|)$ orbits on $\mathscr{T}(p-3,3)$. This follows easily from Theorem 5.2, (ii) in [13]. Thus there is a $T_H \in \mathscr{T}(p-3,3)//G$ with

$$(**) \qquad |H \circ T_H| \geqslant 2|G|\,|\mathscr{T}(p-3,3)|/(2|G| + p(p-1)) \geqslant |G|(p-2)/6.$$

Let $p > 7$ and $G_0 = \bigcap(\operatorname{Stab}(G \circ T_H) \mid H \supseteq G,\ H \text{ not solvable})$. If G_0 is *not* solvable, G_0 stabilizes $G \circ T_{G_0}$, so $G_0 \circ T_{G_0} = G \circ T_{G_0}$. Therefore, $|G_0 \circ T_{G_0}| \leqslant |G|$, a contradiction to (**). We obtain $G \subseteq G_0 \subseteq AGL(1,p)$. Now choose $T_{uvw} \in \mathscr{T}(p-3,3)//G$ such that $|G(u,v,w)| = 1$. Then G is the largest subgroup of $AGL(1,p)$ that stabilizes $G \circ T_{uvw}$, which shows that $\{T_H \mid H \supseteq G,\ H \text{ not solvable}\} \cup \{T_{uvw}\}$ is essential.

We mention briefly the result for $p = 7$. If $|G| = 7$, $|\mathscr{T}(4,3)//G| = 5$, and each minimal essential subset of $\mathscr{T}(4,3)//G$ has two elements; there are exactly six such sets. If $|G| = 21$, $|\mathscr{T}(4,3)//G| = 3$. The minimal essential subsets $\mathscr{U} \subseteq \mathscr{T}(4,3)//G$ are those with two elements. This completes the proof of the theorem. □

Next we consider the transitive groups $G \subseteq S_m$ for $m \leqslant 7$. They are the subject of several tables ([16], [15], [11]). With the exception of most subgroups of S_6, all of them are covered by Theorems 1 or 2. So we know the essential sets of smallest weight explicitly, and it is easy to establish the corresponding G-polynomials. As an example, take $G = G_{20} = AGL(1,5) \subseteq S_5$, with generators (12345), (1243). This group is doubly transitive, and by Theorem 1 the minimal essential sets of smallest weight $d = 4$ have the shape $\{T\}$, $T \in \mathscr{T}(2,2,1)$. Each $T \in \mathscr{T}(2,2,1)$ is stabilized by at most 1 or 2 elements of G, hence $|G \circ T| = 20$ or 10. The latter case holds for

$T = (\{1,4\},\{2,3\},\{5\})$; we obtain the G-polynomial

$$N_G(T^{i_0(T)}) = X_1^2(X_2X_5 + X_3X_4) + X_2^2(X_1X_3 + X_4X_5) + X_3^2(X_1X_5 + X_2X_4)$$
$$+ X_4^2(X_1X_2 + X_3X_5) + X_5^2(X_1X_4 + X_2X_3).$$

This polynomial has been found by Serret [14] in 1850. We have used it to compute R^*_{20} (Section 3).

For reasons discussed in the Introduction, we give a new table for $m = 6$. Since it is a supplement to [16, Table 1], we adopt the notation of the article cited. This means that the groups in our list are equal to those of [16] *in the strict set-theoretical sense*. This is important, because conjugate groups lead to permuted G-polynomials. Generators of the groups can be found in [16].

TABLE 1

Essential sets and G-polynomials for groups of degree six

Nr.	name	structure	imp.	d	essent. set	G-polynomial
1.	G_{120}	$PGL(2,5)$	—	6	$\{12\|35\|46\}$	$\begin{pmatrix}1&5\\2&4\\3&6\end{pmatrix}+\begin{pmatrix}1&6\\2&5\\3&4\end{pmatrix}+\begin{pmatrix}1&3\\2&6\\4&5\end{pmatrix}+\begin{pmatrix}1&4\\2&3\\5&6\end{pmatrix}+\begin{pmatrix}1&2\\3&5\\4&6\end{pmatrix}$
2.	G_{72}	$S_3 \wr S_2$	A	2	$\{1234\|56\}$	$12 + 23 + 31 + 45 + 56 + 64$
3.	G_{60}	$PSL(2,5)$	—	3	$\{123\|456\}$	$124 + 126 + 134 + 135 + 156$ $+235 + 236 + 245 + 346 + 456$
4.	G_{48}	$S_2 \wr S_3$	B	2	$\{1234\|56\}$	$12 + 34 + 56$
5.	G^1_{36}	$(S_3 \wr S_2) \cap A_6$	A	7	$\{14\|25\|3\|6\}$	$\frac{123}{465}+\frac{123}{546}+\frac{123}{654}+\frac{456}{123}+\frac{456}{231}+\frac{456}{312}$
6.	G^2_{36}	$\simeq S_3 \times S_3$	A	6	$\{14\|25\|36\}$	$\begin{pmatrix}1&4\\2&5\\3&6\end{pmatrix}+\begin{pmatrix}1&5\\2&6\\3&4\end{pmatrix}+\begin{pmatrix}1&6\\2&4\\3&5\end{pmatrix}$
7.	G^1_{24}	$\simeq S_4$	B	6	$\{135\|2\|4\|6\}$	$[153] + [246] + [136] + [254]$ $+[145] + [263] + [164] + [235]$
					$\{13\|25\|46\}$	$\begin{pmatrix}1&4\\2&6\\3&5\end{pmatrix}+\begin{pmatrix}1&5\\2&4\\3&6\end{pmatrix}+\begin{pmatrix}1&3\\2&5\\4&6\end{pmatrix}+\begin{pmatrix}1&6\\2&3\\4&5\end{pmatrix}$
8.	G^2_{24}	$\cong A_4 \times S_2$	B	3	$\{123\|456\}$	$125 + 126 + 134 + 234 + 356 + 456$
					$\{1235\|4\|6\}$	$13^2 + 35^2 + 51^2 + 14^2 + 46^2 + 61^2$ $+24^2 + 45^2 + 52^2 + 23^2 + 36^2 + 62^2$
9.	G^3_{24}	$(S_2 \wr S_3) \cap A_6$	B	3	$\{135\|246\}$	$136 + 235 + 246 + 145$
10.	G_{18}	$A_3 \wr S_2$	A	3	$\{1234\|5\|6\}$	$12^2 + 23^2 + 31^2 + 45^2 + 56^2 + 64^2$
11.	G^1_{12}	dihedral	A, C	2	$\{2346\|15\}$	$15 + 53 + 34 + 42 + 26 + 61$
12.	G^2_{12}	$\cong A_4$	B	3	$\{135\|246,$ $123\|456\}$	$aP(G^3_{24}) + bP(G^2_{24})$
13.	G^1_6	$\cong S_3$	A, D E, F	3	$\{1234\|5\|6,$ $1246\|35\}$	$aP(G_{18}) + b(14 + 26 + 35)$
14.	G^2_6	cyclic	A, C	3	$\{2346\|1\|5\}$	$15^2 + 53^2 + 34^2 + 42^2 + 26^2 + 61^2$

$A = \{\{123\},\{456\}\}$, $B = \{\{12\},\{34\},\{56\}\}$, $C = \{\{14\},\{25\},\{36\}\}$,
$D = \{\{14\},\{26\},\{35\}\}$, $E = \{\{16\},\{25\},\{34\}\}$, $F = \{\{15\},\{24\},\{36\}\}$.

Explanations to Table 1. 1. In Column 3 "$\wr$" denotes the wreath-product of groups (cf. [6, p. 94]). Column 4 gives the imprimitive systems of the group; e.g., group nr. 11 permutes the sets in A and C. Column 5 contains the smallest degree d of a polynomial belonging to the group, and Column 6 gives minimal essential sets of weight d. The notation of these sets has been reduced. So $\{135|246, 123|456\}$ stands for the set consisting of the partitions $(\{1,3,5\}, \{2,4,6\})$ and $(\{1,2,3\}, \{4,5,6\})$. Column 7 gives the G-polynomials derived from the essential sets in Column 6. Most essential sets consist of only one element T; then the corresponding G-polynomial is simply $N_G(T^{i_0(T)})$. Only for groups nr. 12, 13 has the set the shape $\{T, T'\}$, and the G-polynomial is $aN_G(T^{i_0(T)}) + bN_G(T'^{i_0(T')})$, with $a, b \in K \setminus \{0\}$ distinct; the reduced norms coincide with the polynomials belonging to the groups in brackets. All polynomials are written in an abbreviated way. Instead of X_i^j we write i^j, so that $ij^2 + kl^2 + \cdots$ denotes the polynomial $X_iX_j^2 + X_kX_l^2 + \cdots$. The expression

$$\begin{pmatrix} i & r \\ j & s \\ k & t \end{pmatrix}$$

(groups nr. 1, 6, 7) is defined as $i^2r^2(js + kt) + j^2s^2(ir + kt) + k^2t^2(ir + js)$. The symbol $\frac{ijk}{rst}$ (nr. 5) stands for $i^3r^2(js + kt) + j^3s^2(ir + kt) + k^2t^2(ir + js)$. Finally, $[ijk] = ij^2k^3 + jk^2i^3 + ki^2j^3$ (nr. 7).

2. The sets of Column 6 have been selected according to the following principles: Two minimal essential sets of weight d are considered *equivalent* if the types occurring in them are the same. We take only *one* representative from each equivalence class, in such a way that the number of monomials in the corresponding G-polynomial is the smallest possible. However, an equivalence class is omitted *altogether* if there is another one whose types form a strict subset of the types of the class in question. This is the case only for groups nr. 12 and 14. Up to these reductions, our list of minimal essential sets of smallest weight is intended to be complete.

Remark. The polynomials of [16, Table 1] professedly belonging to G_{12}^1 and G_6^1, actually are G_{48}-polynomials, where the groups G_{48} are defined by their imprimitive systems C (in case of G_{12}^1) and D (in case of G_6^1).

3. Computation of Resolvents for Degrees Five and Six. Let the notations of the Introduction hold, in particular, let K be a field. The polynomial $R \in K[X_1, \ldots, X_m, Z]$ connected with the group G has the shape $R = \prod(Z - s \circ P)$, s running through a system of representatives of S_m/G, the left cosets modulo G (cf. Introduction). The coefficients b_i of $R = Z^l + b_1Z^{l-1} + \cdots + b_l$ are symmetric in $X_1, \ldots, X_m$, so $R^+ = Z^l + b_1^+Z^{l-1} + \cdots + b_l^+ \in K[X, Z]$ exists with $R = R^+(\sigma_1, \ldots, \sigma_m, Z)$. The coefficients $b_i^+ = \sum c_{n_1 \cdots n_m}^{(i)} X_1^{n_1} \cdots X_m^{n_m}$ can be determined by interpolation, as described, e.g., in [4]. For each $i = 1, \ldots, l$ this method leads to a system of linear equations in the unknowns $c_{n_1 \cdots n_m}^{(i)}$. The number of unknowns depends on the knowledge of finite sets $M_i \subseteq \mathbf{N}_0^m$ such that each exponent $(n_1, \ldots, n_m)$ with nonvanishing $c_{n_1 \cdots n_m}^{(i)}$ is in M_i. In order to get a feasible procedure, one has to make M_i small. A first step is to work with $R^* = R^+(0, X_2, \ldots, X_m, Z)$ instead of R^+. In the case of R_{20}^+, for example, the set M_6 (computed by the method below) has 173 elements, whereas the respective set for R_{20}^* has cardinality 35. The degrees of b_i in each set of variables $\{X_1, \ldots, X_k\}$,

$k \leqslant m$, determine a system of linear inequalities for the tuples in M_i. The *full system* (which seems not to be generally known, though one or two inequalities are given in several algebra books) is due to [9]. It is very advantageous, since the sets M_i thereby found are, as a rule, rather close to the sets of actually occurring exponents. For instance, in the case of R^*_{120} one gets $|M_i| = 2, 9, 23, 51, 99, 177$, $i = 1, \ldots, 6$, and 2, 9, 23, 45, 86, 146 actual exponents in $b^*_1, \ldots, b^*_6$, respectively. In the last analysis, the size of M_i depends on the *types* constituting the G-polynomial P, because they determine the various degrees of b_i. It is advisable to select candidates for P according to the principles described in the explanations to Table 1. Sometimes the very best P can be found only by trial.

Table 2 contains the polynomials R^*_n for the groups $G = G_n$, $n = 20, 72, 120$. They have been computed by a mod p-version of the method just described. The underlying G_n-polynomials are those of Section 2. The information given for each coefficient b^*_i consists of the list of exponents $(n_1, \ldots, n_m)$ (written without commas, since all n_j are $\leqslant 9$) and the list of numerical coefficients $c^{(i)}_{n_1 \cdots n_m}$, in the respective order. The R^*_n are defined over arbitrary fields K. Obviously, it is tedious to copy the *whole* polynomial R^*_{120}, say, from Table 2 by hand. However, polynomials in $K[Z]$ of interest often have two or more vanishing coefficients, and then only a small part of R^* is needed, which can be found very quickly.

We give an illustration both of this fact and the import of R^*_{120}. Let $f = Z^6 + aZ + b \in K[Z]$. By Table 2, $R[a, b] := R^+_{120}(0, 0, 0, 0, a, b, Z)$ has the shape

$$R[a,b] = Z^6 + 18bZ^5 - 135b^2Z^4 - 3240b^3Z^3 + (93312b^5 + 3125a^6)Z - 186624b^6 + 40625a^6b.$$

This polynomial can be written as

$$R[a,b] = (Z - 3b)^2(Z - 12b)(Z + 12b)^3 + 5^5a^6(Z + 13b);$$

we obtain an analogue of a theorem of Weber on solvable quintic trinomials [18, p. 676], namely

PROPOSITION 6. *Let K be a field of characteristic > 5, $f = Z^6 + aZ + b \in K[Z]$ irreducible, $a \neq 0$. Consider the Galois group $G(f)$ as a subgroup of S_6, according to its action on the roots of f. Then $G(f)$ is contained in a group $PGL(2,5)$ ($\cong S_5$) if and only if there exist $u, v \in K$ such that*

$$(*) \qquad a = -(u - 3v)^2(u - 12v)(u + 12v)^3/(5^5(u + 13v)), \qquad b = av.$$

Proof. Suppose that $G(f) \subseteq PGL(2,5)$. Then $R[a, b]$ has a zero in K (cf. [16], [2]), say x. Put $x = au$, $b = av$, $u, v \in K$. $R[a, b](x) = 0$ implies $u \neq -1 - 13v$, and $(*)$ follows as in [18]. Conversely, let a, b be defined by $(*)$, $a \neq 0$, and f irreducible. Then au is a root of $R[a, b]$. One must show that $R[a, b]$ has no multiple zero y in any extension of K. Suppose y exists. Since

$$0 = \frac{dR[a,b]}{dZ}(y) = 6(y - 3b)(y + 12b)^2(y^2 - 6by - 36b^2) + 5^5a^6,$$

we can eliminate 5^5a^6 in the equation $R[a, b](y) = 0$, and obtain

$$0 = -5(y - 3b)(y + 12b)^2g(y),$$

with $g = Z^3 + 9bZ^2 - 108b^2Z - 648b^3$. Obviously, $g(y) = 0$, and reduction of $dR[a, b]/dZ$ modulo g yields $0 = -6^6b^5 + 5^5a^6$. This means $a = 6^6v^5/5^5$, $b = 6^6v^6/5^5$, and f has the (double) root $-6v/5$ in K, a contradiction. □

Remarks. 1. For $K = \mathbf{Q}$ the polynomials f defined by (*) in general have $G(f) = PGL(2,5)$.

2. The author has computed some other polynomials R^* for subgroups of S_5 and S_6, among them one belonging to the intransitive group $S_3 \subseteq S_5$. This R^* yields a *Galois resolvent* (i.e., the minimal polynomial of a generator of the splitting field of f) for each f with $G(f) = AGL(1,5)$. It should be noted that also for degrees higher than six such computations are feasible, at least when two or more variables X_i in R^+ are specialized to zero.

3. All polynomials R_n^* given in Table 2 have been tested in various *relevant* numerical examples. In particular, the (a priori known) Galois groups of several polynomials in $\mathbf{Q}[Z]$ have been verified in this way. Therefore, the author is convinced of the accuracy of Table 2.

TABLE 2

Resolvents belonging to groups of degree six

1. $R_{20}^* = Z^6 + b_1^* Z^5 + \ldots + b_6^* \in K[X_1, \ldots, X_5, Z]$.

b_1^*:

(00010)
-8

b_2^*:

(00101)	(00020)	(02010)	(01200)
-50	40	-6	2

b_3^*:

(01002)	(00111)	(02101)	(00030)	(02020)	(01210)	(00400)
-125	400	15	-160	40	-21	2

b_4^*:

(01012)	(00202)	(00121)	(02111)	(01301)	(00040)	(02030)
(01220)	(04020)	(00410)	(03210)	(02400)		
500	625	-1400	90	-50	400	-136
76	9	-8	-6	1		

b_5^*:

(00004)	(01103)	(01022)	(00212)	(03012)	(02202)	(05002)
(00131)	(02121)	(01311)	(04111)	(00501)	(03301)	(00050)
(02040)	(01230)	(04030)	(00420)	(03220)	(02410)	(01600)
3125	-625	500	-2750	-525	325	108
2400	-260	-105	-117	58	31	-512
256	-76	-32	-3	51	-19	2

b_6^*:

(00014)	(02004)	(01113)	(01032)	(00222)	(03022)	(02212)
(05012)	(01402)	(04202)	(07002)	(00141)	(02131)	(01321)
(04121)	(00511)	(03311)	(06111)	(02501)	(05301)	(00060)
(02050)	(01240)	(04040)	(00430)	(03230)	(06030)	(02420)
(05220)	(01610)	(00800)				
-9375	3125	-1250	-2000	3250	1200	-725
-99	-125	-150	-27	-1600	-160	590
196	-124	12	18	-12	-4	256
-192	-16	48	17	-128	-4	65
1	-13	1				

TABLE 2 (*continued*)

2. $R^*_{72} = Z^{10} + b^*_1 Z^9 + \ldots + b^*_{10} \in K[X_1, \ldots, X_6, Z]$.

b^*_1: (010000)

4

b^*_2: (000100) (020000)

-6 6

b^*_3: (000001) (010100) (002000) (030000)

-66 -26 3 4

b^*_4: (010001) (001010) (000200) (020100) (012000) (040000)

-324 36 1 -42 9 1

b^*_5: (000101) (020001) (000020) (011010) (010200) (002100) (030100) (022000)

-114 -642 123 120 18 -12 -30
9

b^*_6: (000002) (010101) (002001) (030001) (010020) (001110) (021010) (000300) (020200) (012100) (040100) (004000) (032000)

129 -482 138 -640 521 -138 148
24 49 -40 -8 3 3

b^*_7: (010002) (001011) (000201) (020101) (012001) (040001) (000120) (020020) (011110) (003010) (031010) (010300) (002200) (030200) (022100) (014000)

384 342 -80 -752 366 -320 -94
898 -470 36 80 80 2 48
-44 6

b^*_8: (000102) (020002) (000021) (011011) (010201) (002101) (030101) (022001) (050001) (010120) (002020) (030020) (001210) (021110) (013010) (041010) (000400) (020300) (012200) (040200) (004100) (032100) (024000)

120 384 66 852 -240 -6 -512
324 -64 -246 51 788 -24 -568
84 16 16 88 18 16 -6
-16 3

b^*_9: (000003) (010102) (002002) (030002) (010021) (001111) (021011) (000301) (020201) (012101) (040101) (004001) (032001) (001030) (000220) (020120) (012020) (040020) (011210) (003110) (031110) (023010) (010400) (002300) (030300) (022200) (014100) (006000)

-64 256 48 128 112 -24 704
-32 -224 -8 -128 -12 96 14
8 -216 86 352 -40 6 -320
64 32 -8 32 32 -14 1

TABLE 2 (*continued*)

R^*_{72} (continued)

b^*_{10}: (010003) (000202) (020102) (012002) (000121) (020021) (011111)
(031011) (010301) (002201) (030201) (014001) (000040) (011030)
(010220) (002120) (030120) (022020) (050020) (021210) (013110)
(041110) (033010) (020400) (012300) (004200) (032200) (024100)
(016000)

-64	16	128	48	-8	48	-16
192	-32	-8	-64	-12	1	12
8	2	-64	36	64	-16	4
-64	16	16	-8	1	16	-8
1						

3. $R^*_{120} = Z^6 + b^*_1 Z^5 + \ldots + b^*_6 \in K[X_1, \ldots, X_6, Z]$.

b^*_1: (000001) (010100)

18	2

b^*_2: (000002) (010101) (002001) (030001) (010020) (001110) (021010)
(000300) (020200)

-135	114	-54	-8	-50	30	2
-8	1					

b^*_3: (000003) (010102) (002002) (030002) (010021) (001111) (021011)
(000301) (020201) (012101) (040101) (004001) (032001) (001030)
(000220) (020120) (012020) (040020) (011210) (003110) (031110)
(010400) (002300)

-3240	1440	-1350	-304	-900	990	126
-304	232	-198	-16	27	2	-125
50	-120	15	2	66	-9	2
-16	2					

b^*_4: (010103) (002003) (030003) (010022) (001112) (021012) (000302)
(020202) (012102) (040102) (004002) (032002) (060002) (001031)
(000221) (020121) (012021) (040021) (011211) (003111) (031111)
(023011) (051011) (010401) (002301) (030301) (022201) (050201)
(014101) (042101) (020040) (011130) (031030) (010320) (002220)
(030220) (022120) (050120) (042020) (001410) (021310) (013210)
(000600) (020500) (012400)

-4536	-1944	-1224	1350	3240	756	-1224
4320	-4752	-688	972	234	16	-1125
450	-3480	1485	218	2484	-891	84
-54	-8	-688	234	168	-144	-8
27	2	625	-875	-50	250	225
-70	45	2	1	-120	28	-9
16	-8	2				

TABLE 2 (*continued*)

R^*_{120} (continued)

b^*_5: (000005) (010104) (002004) (030004) (010023) (001113) (021013)
(000303) (020203) (012103) (040103) (004003) (032003) (060003)
(001032) (000222) (020122) (012022) (040022) (011212) (003112)
(031112) (023012) (051012) (010402) (002302) (030302) (022202)
(050202) (014102) (042102) (070102) (034002) (062002) (000141)
(020041) (011131) (003031) (031031) (010321) (002221) (030221)
(022121) (014021) (042021) (070021) (001411) (021311) (013211)
(041211) (005111) (033111) (061111) (025011) (053011) (000601)
(020501) (012401) (004301) (000060) (011050) (010240) (002140)
(030140) (022040) (050040) (001330) (021230) (013130) (041130)
(005030) (033030) (061030) (000520) (020420) (012320) (040320)
(004220) (032220) (024120) (011510) (003410) (031410) (023310)
(010700) (002600)

93312	-85536	163296	16416	48600	-174960	33696
16416	6048	-43416	-4224	11664	864	-96
40500	37800	-40320	4590	7192	39096	-10044
-6144	2052	104	-4224	864	4032	-2376
-416	324	312	32	-54	-8	-22500
12750	-10950	2025	-2770	-560	-270	-2144
4014	-918	-32	-8	552	608	-756
192	162	-150	-8	27	2	-96
-416	312	-54	3125	-625	750	375
850	325	58	-350	-1340	-180	-112
108	31	2	56	352	574	8
-162	32	-9	-264	66	-8	2
32	-8					

b^*_6: (000006) (010105) (002005) (030005) (010024) (001114) (021014)
(000304) (020204) (012104) (040104) (004004) (032004) (060004)
(001033) (000223) (020123) (012023) (040023) (011213) (003113)
(031113) (023013) (051013) (010403) (002303) (030303) (022203)
(050203) (042103) (070103) (034003) (062003) (000142) (020042)
(011132) (003032) (031032) (010322) (002222) (030222) (022122)
(050122) (014022) (042022) (070022) (001412) (021312) (013212)
(041212) (005112) (033112) (061112) (053012) (000602) (020502)
(012402) (040402) (004302) (032302) (060302) (024202) (052202)
(080202) (072102) (064002) (000061) (011051) (010241) (002141)
(030141) (022041) (050041) (001331) (021231) (013131) (041131)
(005031) (033031) (061031) (000521) (020421) (012321) (040321)
(004221) (032221) (060221) (024121) (052121) (080121) (016021)
(044021) (072021) (011511) (003411) (031411) (023311) (051311)
(015211) (043211) (035111) (010701) (002601) (030601) (022501)
(050501) (042401) (034301) (010160) (002060) (001250) (021150)
(041050) (000440) (020340) (012240) (040240) (032140) (060140)
(024040) (052040) (080040) (011430) (003330) (031330) (023230)
(051230) (015130) (043130) (007030) (035030) (010620) (002520)
(030520) (022420) (050420) (014320) (042320) (006220) (034220)
(021610) (013510) (005410) (020800) (012700) (004600)

TABLE 2 (*continued*)

-186624	248832	1026432	-29376	-129600	-1477440	536544
-29376	-93744	-178848	19296	46656	-9936	144
432000	529200	-249480	-165240	48408	139104	-7776
-68976	17496	-2544	19296	-9936	6912	-864
-3072	2520	-96	-432	24	-292500	70125
72900	29700	-11360	-22080	-29160	-7992	22572
3032	-3564	222	-232	6336	14784	-12204
-1312	1944	324	336	-84	144	-3072
2520	1296	-432	-752	-32	108	8
16	-8	1	40625	-20625	-7750	-10125
5550	225	954	11700	-12020	1935	-3616
54	923	108	-2472	1096	1962	-168
-486	2262	-160	-1215	-106	-8	162
36	2	-144	36	-480	336	176
-54	-80	9	-96	24	-32	8
-32	16	-2	3125	3125	-3125	625
-125	625	250	-125	375	525	38
-150	-12	1	-200	50	-700	-185
-36	198	25	-27	-4	56	-14
152	370	8	-210	-6	27	1
-144	72	-9	16	-8	1	

Acknowledgment. Most of this work was done while the author had a Humboldt research fellowship at the University of Karlsruhe. Computer calculations were carried out at the computer center of this university. The author thanks Professor H. W. Leopoldt and his research group for their hospitality and kind permission to use their program library. His special thanks are due to W. Happle for his valuable help in programming questions.

Institut für Mathematik der Universität Innsbruck
Technikerstrasse 15
A-6020 Innsbruck, Austria

1. A. CAYLEY, *On a New Auxiliary Equation in the Theory of Equations of the Fifth Order*, Collected Papers of A. Cayley, vol. 4, pp. 309–324.

2. K. GIRSTMAIR, "Über konstruktive Methoden der Galoistheorie," *Manuscripta Math.*, v. 26, 1979, pp. 423–441.

3. K. GIRSTMAIR, "On the computation of resolvents and Galois groups," *Manuscripta Math.*, v. 43, 1983, pp. 289–307.

4. K. GIRSTMAIR & U. OBERST, "Ein Verfahren zur konstruktiven Bestimmung von Galoisgruppen," in *Jahrbuch Überblicke Mathematik*, Bibliographisches Institut, Mannheim, 1976.

5. D. GORENSTEIN, *Finite Simple Groups*, Plenum Press, New York and London, 1982.

6. B. HUPPERT, *Endliche Gruppen* I, Springer-Verlag, Berlin and New York, 1967.

7. C. JORDAN, *Traité des Substitutions et des Équations Algébriques*, Gauthier-Villars, Paris, 1870.

8. W. M. KANTOR, "k-homogeneous groups," *Math. Z.*, v. 124, 1972, pp. 261–265.

9. G. KOHN, "Über symmetrische Funktionen der Wurzeln einer algebraischen Gleichung," *Sitzungsber. Kaiserl. Akad. Wiss. Math. Nat. Classe Wien*, 1893, pp. 199–214.

10. W. KRULL, *Elementare und klassische Algebra* II, de Gruyter, Berlin, 1959.

11. J. MCKAY, "Some remarks on computing Galois groups," *SIAM J. Comput.*, v. 8, 1979, pp. 344–347.

12. P. M. NEUMANN, "Transitive permutation groups of prime degree," *J. London Math. Soc.* (2), v. 5, 1972, pp. 202–208.

13. P. M. NEUMANN, "Transitive permutation groups of prime degree III," *Proc. London Math. Soc.* (3), v. 31, 1975, pp. 482–494.

14. A. SERRET, "Mémoirs sur les fonctions de quatre, cinq et six lettres," *J. Math. Pures Appl.* (1), v. 15, 1850, pp. 45–70.

15. C. SIMS, "Computational methods in the study of permutation groups," *Computational Problems in Abstract Algebra* (Proc. Oxford Conf., 1967), Pergamon Press, Oxford, 1970.

16. R. P. STAUDUHAR, "The determination of Galois groups," *Math. Comp.* v. 27, 1973, pp. 981–996.

17. M. SUZUKI, "Transitive extensions of a class of doubly transitive groups," *Nagoya Math. J.*, v. 27, 1966, pp. 159–169.

18. H. WEBER, *Lehrbuch der Algebra* I, Vieweg, Braunschweig, 1895, ^{2}1898; reprinted, Chelsea, New York.