MATHEMATICS OF COMPUTATION
Volume 66, Number 218, April 1997, Pages 823–831
S 0025-5718(97)00831-4

COMPUTATION OF GALOIS GROUPS OVER FUNCTION FIELDS

THOMAS MATTMAN AND JOHN MCKAY

Abstract. Symmetric function theory provides a basis for computing Galois groups which is largely independent of the coefficient ring. An exact algorithm has been implemented over $\mathbb{Q}(t_1, t_2, \ldots, t_m)$ in Maple for degree up to 8. A table of polynomials realizing each transitive permutation group of degree 8 as a Galois group over the rationals is included.

Introduction

There are currently three techniques used for computing the Galois group, $\mathrm{Gal}_{\mathbb{Q}}(f)$, of an irreducible polynomial f over the rationals. First there is the method of Stauduhar [22, 12], described in his thesis [21] for polynomials of degree up to 8, which uses approximations to the roots of f. He forms resolvent polynomials with roots which are polynomial invariants of potential Galois groups, working down the upper semi-lattice of transitive subgroups of the symmetric group. The resolvent roots are evaluated on permutations of roots of the original polynomial given by some coset transversal. The resolvents are computed from approximate values of the roots of f, and factors (often linear) sought.

This method appears in Cohen [4] and has been used by Olivier [15] for degree up to 11. It is generally fast but has exponential complexity in groups such as $PSL(2, q)$ in its natural representation, see McKay [12]. It has the disadvantage of needing a complicated data structure for traversing the upper semi-lattice of transitive groups of a given degree, and requires storing (or generating) many coset transversals and polynomial invariants; careful control of rounding errors is needed for the result to constitute a proof.

Second is the method of Darmon and Ford [7] in which they prove directly from p-adic approximations to the roots that the value of a polynomial invariant evaluated on the roots of f is a rational integer.

The third method, which we use, is the method of symmetric functions. This is a refinement of that described for Galois groups over $\mathbb{Q}$ of degree up to 7 in Soicher and McKay [19], with which we assume familiarity. It is exact and, unlike the first two methods, has the advantage of being largely independent of the coefficient ring which may, for example, be a number field, K, a function field, $K(t_1, t_2, \ldots, t_m)$, or a p-adic field extension. Here we compute $\mathrm{Gal}_K(f)$, $K = \mathbb{Q}(t_1, t_2, \ldots, t_m)$ for

Received by the editor June 12, 1995 and, in revised form, December 7, 1995.
1991 *Mathematics Subject Classification.* Primary 12F10, 12Y05.
Key words and phrases. Galois groups, polynomials, computation.
Research supported by NSERC and FCAR of Québec.

$f \in K[x]$. In Mattman [10] (supervised by the second author), this is implemented in Maple for polynomials of degree up to 8.

The method

As an example of our method we discuss the degree 8 case in detail. Let f be an irreducible polynomial of degree δf in $K[x]$ where $K = \mathbb{Q}(t_1, \dots, t_m)$. The Galois group $\mathrm{Gal}_K(f)$ is realisable as the group of permutations of the roots of f induced by the automorphisms of the splitting field $spl(f)$ of f. Since we require f to be irreducible, $\mathrm{Gal}_K(f)$ is one of the 50 transitive groups, $T_1, T_2, \dots, T_{50}$, of degree 8 in Butler and McKay [1]. (In our tables these names are correlated with the more informative inherently meaningful names of [5].) It is determined up to relabelling of the roots, that is, up to conjugacy in the symmetric group, S_8. Our aim is to determine sufficient properties to identify $\mathrm{Gal}_K(f)$ among these candidates.

By multiplication, if necessary, we may assume that $f \in \mathbb{Z}[t_1, \dots, t_m][x]$ so that we can construct cycle types of $\mathrm{Gal}_K(f)$ by factoring f modulo maximal ideals $\mathfrak{p}$ of $\mathbb{Z}[t_1, \dots, t_m]$. If f has no repeated roots in an algebraic closure of $\mathbb{Z}[t_1, \dots, t_m]/\mathfrak{p}$, the partition of δf formed by the degrees of the irreducible factors of $f \bmod \mathfrak{p}$ is the shape (cycle type) of a permutation in $\mathrm{Gal}_K(f)$ (see [24]). After factoring f modulo various maximal ideals, we may eliminate those candidate groups lacking elements of the shapes found.

When $K = \mathbb{Q}$, the algorithm of Casperson and McKay [3] can be used to construct non-trivial decompositions $f(x) \mid g(h(x))$. Such a decomposition exists whenever $\mathrm{Gal}_K(f)$ has a block system with δg blocks of imprimitivity. Once a decomposition is found, we may eliminate all groups which do not admit such a block system.

Neither shapes nor decompositions are required to determine $\mathrm{Gal}_K(f)$; both are useful to reduce the list of candidate Galois groups but these methods do not usually suffice to specify the group. Degree 8 is the smallest degree for which there are pairs of groups,

$$[2^2]4 = \langle (1,3,5,7)(2,4,6,8), (1,6)(2,5)(3,7)(4,8) \rangle \quad \text{and}$$

$$Q_8 : 2 = \langle (1,6,2,5)(3,7,4,8), (1,5)(2,6)(3,7)(4,8), (1,3)(2,4)(5,8)(6,7) \rangle$$

of order 16, $[2^3]A(4)$ & $[\frac{1}{3}A(4)^2]2$ (order 96) and $[2^3]S(4)$ & $\frac{1}{2}[2^4]S(4)$ (order 192), with the same frequency of elements of each shape and thus Čebotarev's density theorem cannot be used to separate the groups within these pairs.

Resolvent polynomials

We adopt the notation for resolvents in [19]. The action of $\mathrm{Gal}_K(f)$ on r-sets (sets of r roots) may be realised in terms of polynomials with roots which are sums or products of r-sets of the roots of f. Casperson and McKay [2] discuss efficient methods for constructing such polynomials. To construct the 2-sequence resolvent

$$R = R(x_1 + cx_2, f), \quad c \neq 0, 1,$$

of degree $n^2 - n$, $n = \delta f$, we make use of the relation (compare [23]):

$$\mathcal{P}_k(R) = \sum_{i=0}^{k} c^i \binom{k}{i} (\mathcal{P}_i(f)\mathcal{P}_{k-i}(f) - \mathcal{P}_k(f)), \quad k \geq 1,$$

between the power-sum symmetric functions of f and R.

TABLE 1. These groups (see [1, 5]) are distinguished by testing the underlined factors of the resolvents; '+/–' indicates reducible/irreducible over $K(\sqrt{\Delta})$

Group	T_{16}- $\frac{1}{2}[2^4]4$	T_{27}- $[2^4]4$	T_{21}- $\frac{1}{2}[2^4]E(4)$	T_{31}- $[2^4]E(4)$	T_{46}- $\frac{1}{2}[S(4)^2]2$	T_{47}- $[S(4)^2]2$
2-set	$\underline{+4}, 8, 16$	$\underline{-4}, 8, 16$	$\underline{+4}, 8^3$	$\underline{-4}, 8^3$	$\underline{+12}, 16$	$\underline{-12}, 16$

Group	T_{26}-$\frac{1}{2}[2^4]eD(4)$	T_{28}-$\frac{1}{2}[2^4]dD(4)$	T_{30}-$\frac{1}{2}[2^4]cD(4)$	T_{35}-$[2^4]D(4)$
2-set	$\underline{-4}, 8, \underline{+16}$	$\underline{+4}, 8, \underline{-16}$	$\underline{-4}, 8, \underline{-16}$	$\underline{-4}, 8, \underline{-16}$
3-set	$8, \underline{+16}, 32$	$8, \underline{+16}, 32$	$8, \underline{+16}, 32$	$8, \underline{-16}, 32$

We define a Tschirnhaus transformation (over K) on a polynomial f to be an invertible map: $x \mapsto N(x)/D(x) \equiv P(x) \bmod f$, $P(x) \in K[x]$. If K is omitted, it is assumed that $K = \mathbb{Q}$.

The orbit-length partition of the action of $\mathrm{Gal}_K(f)$ on F^{S_8} (the orbit of F under S_8, see [19]) is given by the factorization of the resolvent $R(F, f)$, provided it has no repeated roots. Although polynomials with repeated roots are theoretically rare, being a set of measure zero, they may occur when simple polynomials are chosen for f. To eliminate repeated roots, we apply a Tschirnhaus transformation to f. It is not simple to program choices for an appropriate Tschirnhaus transformation. We need to ensure that the coefficients do not become unwieldy. One suggestion is to generate them using $x \mapsto x + 1$ and $x \mapsto -1/x$ which generate the modular group; it may be better to let the user choose a Tschirnhaus transformation interactively.

The discriminant and orbit-length partitions (see [13]) of the r-set and 2-sequence resolvent polynomials suffice to identify twenty-four of the fifty transitive groups of degree 8. Of the remaining thirteen groups with non-square discriminant, Δ, ten may be distinguished by testing whether factors of the resolvents are reducible over $K(\sqrt{\Delta})$ (see Table 1). As noted in [19], the reducibility of resolvent factors is an invariant of the Galois group.

The remaining sixteen groups are identified by calculating the Galois group of a factor h of a resolvent polynomial as indicated in the last column of Tables 2 and 3 by resolvent type over the degree of h. That these groups are invariants of $\mathrm{Gal}_K(f)$ is an immediate consequence of the fundamental theorem of Galois theory. For $\delta h \leq 8$ we can use either the techniques of [19] or those presented here to find $\mathrm{Gal}_K(h)$; however, to distinguish between $[A(4)^2]2$ and $[\frac{1}{2}S(4)^2]2$ we make use of a factor h of degree 12. In this case, we define two degree 12 groups G_{288} and G_{576} isomorphic to the degree 8 groups $[A(4)^2]2$ and $[\frac{1}{2}S(4)^2]2$ respectively. They may be represented as

$$G_{288} = \langle (1,5,4)(2,6,3)(9,10)(11,12), (1,8)(2,7)(3,11,4,12)(5,9,6,10) \rangle$$

and

$$G_{576} = \langle (1,9,5,7,3,12)(2,10,6,8,4,11), (1,11,4,10,5,8)(2,12,3,9,6,7) \rangle.$$

As indicated in Table 3, G_{288} and G_{576} (and consequently $[A(4)^2]2$ and $[\frac{1}{2}S(4)^2]2$) are distinguished by the Galois group of the degree 6 factor of the 2-set resolvent; they have the same orbit-length partition for the 2-set resolvent.

TABLE 2. Distinguishing Galois groups for $G \not\subseteq A_8$

Group ($G \not\subseteq A_8$) (see [1, 5])	Orbit-Length Partition 2 set	3 set	4 set	2 seq	Factorization over $K(\sqrt{\Delta})$ (see Table 1)	Galois Group of deg. 8 factor of 4-diff resolvent
T_1-C_8		8^7				
T_6-$D(8)$	$4, 8^3$	$8^3 16^2$				
T_7-$\frac{1}{2}[2^3]4$				$8^3 16^2$		
T_8-$2D_8(8)$	$4, 8, 16$	$8^3 16^2$		$8, 16^3$		
T_{15}-$[\frac{1}{4}cD(4)^2]2$		$8, 16^3$				
T_{16}-$\frac{1}{2}[2^4]4$	$\underline{+4}, 8, 16$	$8^3 32$			Needed	
T_{17}-$[4^2]2$				$8^3 32$		
T_{21}-$\frac{1}{2}[2^4]E(4)$	$\underline{+4}, 8^3$	$8^3 32$			Needed	
T_{23}-$GL(2,3)$	$4, 24$	$8, 24^2$				
T_{26}-$\frac{1}{2}[2^4]eD(4)$	$\underline{-4}, 8, \underline{+16}$	$8, \underline{+16}, 32$		$8, 16, 32$	Needed	
T_{27}-$[2^4]4$	$\underline{-4}, 8, 16$	$8^3 32$			Needed	
T_{28}-$\frac{1}{2}[2^4]dD(4)$	$\underline{+4}, 8, \underline{-16}$	$8, \underline{+16}, 32$		$8, 16, 32$	Needed	
T_{30}-$\frac{1}{2}[2^4]cD(4)$	$\underline{-4}, 8, \underline{-16}$	$8, \underline{+16}, 32$		$8, 16, 32$	Needed	
T_{31}-$[2^4]E(4)$	$\underline{-4}, 8^3$	$8^3 32$			Needed	
T_{35}-$[2^4]D(4)$	$\underline{-4}, 8, \underline{-16}$	$8, \underline{-16}, 32$		$8, 16, 32$	Needed	
T_{38}-$[2^4]A(4)$		$24, 32$				T_{33}-$[\frac{1}{3}A(4)^2]2$
T_{40}-$\frac{1}{2}[2^4]S(4)$		$24, 32$				T_{34}-$E(4)^2{:}D_6$
T_{43}-$PGL(2,7)$			$28, 42$			
T_{44}-$[2^4]S(4)$		$24, 32$				T_{41}-$E(4)^2{:}D_{12}$
T_{46}-$\frac{1}{2}[S(4)^2]2$	$\underline{+12}, 16$				Needed	
T_{47}-$[S(4)^2]2$	$\underline{-12}, 16$				Needed	
T_{50}-S_8			70			

The '4-diff' resolvent of Tables 3 and 2 is $R(F^2, f)$ where

$$F = x_1 + x_2 + x_3 + x_4 - x_5 - x_6 - x_7 - x_8.$$

As shown in [19], the existence of $\sigma \in S_8$ such that $F^\sigma = -F$ implies that $R(F, f)(x) = R(F^2, f)(x^2)$. When the sum of the roots of $f(x)$ is zero we have $R(F, f) = R(2(x_1 + x_2 + x_3 + x_4), f)$ and so the 4-diff resolvent may be derived from the 4-set resolvent after applying an appropriate linear Tschirnhaus transformation to f.

Tables 2 and 3 summarize how to distinguish the fifty transitive groups of degree 8. Where factorization over $K(\sqrt{\Delta})$ is needed, certain factors of the resolvents are underlined in Table 2. A '+/–' means the factor is reducible/irreducible over $K(\sqrt{\Delta})$.

For each group G, we indicate orbit-length partitions for a set S of resolvent polynomials. If G and H are groups of the same parity having the same orbit-length partition for each resolvent in S, then G and H have the same partition for the remaining r-set ($r = 2, 3, 4$) and 2-sequence resolvents. With the exception of four groups in Table 2, S is chosen such that no proper subset of S has this property.

The groups $\frac{1}{2}[2^4]eD(4)$, $\frac{1}{2}[2^4]dD(4)$, $\frac{1}{2}[2^4]cD(4)$ and $[2^4]D(4)$ are distinguished amongst themselves by testing if factors of the 2- and 3-set resolvents are reducible over $K(\sqrt{\Delta})$, so the 2-set orbit-length partition is included in the table even though it is unnecessary to include it in S.

TABLE 3. Distinguishing Galois groups for $G \subseteq A_8$

Group ($G \subseteq A_8$) (see [1, 5])	Orbit-Length Partition 2 set	3 set	4 set	2 seq	Galois Groups of Resolvent Factors
T_2-$4[\times]2$	$4^3 8^2$	8^7			
T_3-$E(8)$	4^7				
T_4-$D_8(8)$	$4^5 8$				
T_5-$Q_8(8)$	$4, 8^3$	8^7			
T_9-$D(4)[\times]2$	$4^3 8^2$	$8^3 16^2$			
T_{10}-$[2^2]4$	$4^3 16$	$8^3 16^2$			
T_{11}-Q_8:2	$4, 8^3$	$8^3 16^2$			
T_{12}-$SL(2,3)$	$4, 24$	$8, 24^2$			
T_{13}-$A(4)[\times]2$			$2, 6^2 8, 24^2$		Gal(2-set/4) $= A_4$
T_{14}-$S(4)[\frac{1}{2}]2$			$2, 6^2 8, 12^2 24$		
T_{18}-$[2^2]D(4)$				$8^3 32$	
T_{19}-$E(8)$:4				$8, 16, 32$	Gal(2-set/8) = T_{21}-$\frac{1}{2}[2^4]E(4)$
T_{20}-$[2^3]4$	$4, 8, 16$	$8^3 32$			
T_{22}-$[2^3]2^2$	$4, 8^3$	$8^3 32$			
T_{24}-$S(4)[\times]2$			$2, 6^2 8, 24^2$		Gal(2-set/4) $= S_4$
T_{25}-$E(8)$:7			$14, 56$		Gal(4-diff/7) $= C_7$
T_{29}-$[2^3]D(4)$				$8, 16, 32$	Gal(2-set/8) = T_{31}-$[2^4]E(4)$
T_{32}-$[2^3]A(4)$				$8, 48$	Gal(2-set/4) $= A_4$
T_{33}-$[\frac{1}{3}A(4)^2]2$			$2, 12, 24, 32$		Gal(4-diff/6) $= A_4$
T_{34}-$E(4)^2$:D_6			$2, 12^3 32$		
T_{36}-$E(8)$:F_{21}			$14, 56$		Gal(4-diff/7) $= C_7.C_3$
T_{37}-$PSL(2,7)$			$14^2 42$		
T_{39}-$[2^3]S(4)$				$8, 48$	Gal(2-set/4) $= S_4$
T_{41}-$E(4)^2$:D_{12}			$2, 12, 24, 32$		Gal(4-diff/6) $= S_4/V_4$
T_{42}-$[A(4)^2]2$			$2, 32, 36$		Gal(2-set/12) $= G_{288}$
				(For G_{288}:	Gal(2-set/6) $= C_3.S_3$)
T_{45}-$[\frac{1}{2}S(4)^2]2$			$2, 32, 36$		Gal(2-set/12) $= G_{576}$
				(For G_{576}:	Gal(2-set/6) $= 3^2.2^2$)
T_{48}-$E(8)$:L_7			$14, 56$		Gal(4-diff/7) = $PSL(3,2)$
T_{49}-A_8			70		

POLYNOMIALS WITH GIVEN GALOIS GROUPS

For each transitive group G of degree 8, Tables 4 and 5 contain a representative polynomial $f \in \mathbb{Q}[x]$ such that $\mathrm{Gal}_{\mathbb{Q}}(f) = G$. In the tables, ζ_k denotes a primitive kth root of unity.

Many of these polynomials were suggested to us in earlier work by Darmon [6]. Examples for $SL(2,3)$, $PSL(2,7)$ and $PGL(2,7)$ are drawn from [8] and [11].

In [18], Soicher constructs a polynomial for $E(8)$:L_7 and mentions that the same method may be used for $E(8)$:7 and $E(8)$:F_{21}. For $[\frac{1}{3}A(4)^2]2$ and $E(4)^2$:D_6, we use

TABLE 4. Rational polynomials with Galois groups for $G \not\subseteq A_8$

Group ($G \not\subseteq A_8$)	$f(x)$	Remarks
T_1-C_8	$x^8 - 68x^6 + 918x^4$ $-612x^2 + 17$	$spl(f) = \mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$ [6]
T_6-$D(8)$	$x^8 - 8x^4 - 2$	$f = (x^4 - (2^{1/4} + 2^{3/4})^2)\times$ $(x^4 + (2^{1/4} - 2^{3/4})^2)$ [6]
T_7-$\frac{1}{2}[2^3]4$	$x^8 - 20x^6 + 100x^4$ $-160x^2 + 80$	$f = \prod_{\sigma\in C_4}(x^2 - \sigma(\alpha + \sqrt{2\alpha} + \sqrt{2\beta}))$ $\alpha = 5 + \sqrt{5}$, $\beta = 5 - \sqrt{5}$ [6]
T_8-$2D_8(8)$	$x^8 - 2$	[6]
T_{15}-$[\frac{1}{4}cD(4)^2]2$	$x^8 - 16x^4 - 98$	$f = (x^4 - (2^{1/4} + 2(2)^{3/4})^2)\times$ $(x^4 + (2^{1/4} - 2(2)^{3/4})^2)$ [6]
T_{16}-$\frac{1}{2}[2^4]4$	$x^8 - 5x^4 + 5$	$\mathrm{Gal}(x^4 - 5x^2 + 5) = C_4$ [6]
T_{17}-$[4^2]2$	$x^8 + 2x^4 + 2$	
T_{21}-$\frac{1}{2}[2^4]E(4)$	$x^8 + 8x^6 + 31x^4 + 60x^2 + 45$	$f = (x^2 + 2)^4 + 7(x^2 + 2)^2 + 4$ [6]
T_{23}-$GL(2,3)$	$x^8 - 44x^2 - 44$	
T_{26}-$\frac{1}{2}[2^4]eD(4)$	$x^8 + x^4 + 2$	$\mathrm{Gal}(x^4 + x^2 + 2) = D_4$ [6]
T_{27}-$[2^4]4$	$x^8 + 4x^6 + 10x^4 + 12x^2 + 7$	$\mathrm{Gal}(x^4 + 4x^3 + 10x^2 + 12x + 7) = C_4$ [6]
T_{28}-$\frac{1}{2}[2^4]dD(4)$	$x^8 + 4x^6 + 8x^4 + 8x^2 + 2$	$\mathrm{Gal}(x^4 + 4x^3 + 8x^2 + 8x + 2) = D_4$ [6]
T_{30}-$\frac{1}{2}[2^4]cD(4)$	$x^8 - 4x^6 + 4x^4 - 2$	
T_{31}-$[2^4]E(4)$	$x^8 + 4x^6 + 7x^4 + 6x^2 + 6$	$\mathrm{Gal}(x^4 + 4x^3 + 7x^2 + 6x + 6) = V_4$ [6]
T_{35}-$[2^4]D(4)$	$x^8 + 4x^6 + 7x^4 + 6x^2 + 5$	$\mathrm{Gal}(x^4 + 4x^3 + 7x^2 + 6x + 5) = D_4$ [6]
T_{38}-$[2^4]A(4)$	$x^8 + 8x^2 + 12$	
T_{40}-$\frac{1}{2}[2^4]S(4)$	$x^8 + 12x^2 - 9$	
T_{43}-$PGL(2,7)$	$x^8 + x^7 + 7x^6 + x + 1$	[11]
T_{44}-$[2^4]S(4)$	$x^8 + x^2 + 2$	
T_{46}-$\frac{1}{2}[S(4)^2]2$	$x^8 - 4x^6 + x^4 - 4x^3$ $+2x^2 + 4x + 2$	
T_{47}-$[S(4)^2]2$	$x^8 + 4x^5 + 8$	
T_{50}-S_8	$x^8 + x + 2$	

a method derived from Soicher's: let H be a subgroup of index s in G_1 such that $G_2 \cong G_1/(\bigcap_{\sigma\in G_1} \sigma^{-1}H\sigma)$ and suppose h is a polynomial with roots $\gamma = \gamma_1, \ldots, \gamma_r$ such that $\mathrm{Gal}(h) = G_1$; then we may construct $F \in K[x_1, \ldots, x_r]$ with $stab_{G_1}(F) = H$ (see [22] for example). Using the notation of [19], $F^{G_1} = \{F_1, \ldots, F_s\}$ where the F_i are distinct functions. Provided it has no repeated roots, the polynomial $R_F = \prod_{i=1}^{s}(x - F_i(\gamma)) \in K[x]$ is of degree s with $\mathrm{Gal}(R_F) = G_2$. To remove repeated roots, we apply a Tschirnhaus transformation to h. In this way we arrive at polynomials for $[\frac{1}{3}A(4)^2]2$ (a quotient of $G_1 = [2^4]A(4)$) and $E(4)^2{:}D_6$ ($G_1 = [2^3]S(4)$).

The remaining polynomials are found by computer searching. We were guided in our searches by Soicher [17, pp.85-87]. In particular, we use his ideas for generating polynomials with square discriminant.

TABLE 5. Rational polynomials with Galois groups for $G \subseteq A_8$

Group ($G \subseteq A_8$)	$f(x)$	Remarks
T_2-4[×]2	$x^8 + 2x^6 + 4x^4 + 8x^2 + 16$	$spl(f) = \mathbb{Q}(\zeta_5, \sqrt{2})$ [6]
T_3-$E(8)$	$x^8 - 12x^6 + 23x^4 - 12x^2 + 1$	$spl(f) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ [6]
T_4-$D_8(8)$	$x^8 + 4x^6 + 8x^4 + 4x^2 + 1$	$spl(f) = spl(x^4 - 2)$ [6]
T_5-$Q_8(8)$	$x^8 - 24x^6 + 144x^4 - 288x^2 + 144$	$spl(f) =$ $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})})$ [6]
T_9-$D(4)$[×]2	$x^8 - 10x^4 + 1$	$f = \prod(x \pm \sqrt{\pm\sqrt{2} \pm \sqrt{3}})$ [6]
T_{10}-[2^2]4	$x^8 - 3x^6 + 9x^4 - 12x^2 + 16$	$f = \prod_{i=1}^{i=4}(x^2 - \zeta_5^i x - 2)$ [6]
T_{11}-Q_8:2	$x^8 - 18x^4 + 9$	$spl(f) =$ normal closure of $\mathbb{Q}(\sqrt{12 + 7\sqrt{6} + 12\sqrt{2} + 7\sqrt{3}})$ [6]
T_{12}-$SL(2,3)$	$x^8 + 9x^6 + 23x^4 + 14x^2 + 1$	[8]
T_{13}-$A(4)$[×]2	$x^8 + 24x^4 + 64x^2 + 144$	$spl(f) = \mathbb{Q}(spl(x^4 + 8x + 12), i)$
T_{14}-$S(4)[\frac{1}{2}]2$	$x^8 + 150x^4 - 500x^2 + 5625$	$spl(f) = spl(x^4 + 2x + 3)$
T_{18}-[2^2]$D(4)$	$x^8 + 8x^2 + 9$	
T_{19}-$E(8)$:4	$x^8 - 4x^6 + 12x^4 - 8x^2 + 4$	[6]
T_{20}-[2^3]4	$x^8 + 4x^6 + x^4 - 6x^2 + 1$	$f = (x^2+1)^4 - 5(x^2+1)^2 + 5$ [6]
T_{22}-[2^3]2^2	$x^8 - 28x^4 + 100$	$f = \prod(x^2 - (\pm 2\sqrt{3} \pm \sqrt{2}))$ [6]
T_{24}-$S(4)$[×]2	$x^8 - 4x^2 + 4$	
T_{25}-$E(8)$:7	$x^8 - x^7 + 2x^6 + 2x^5 + 7x^4$ $+3x^3 + 4x^2 + 3x + 5$	See accompanying text
T_{29}-[2^3]$D(4)$	$x^8 + 4x^6 + 7x^4 + 6x^2 + 4$	$\mathrm{Gal}(x^4 + 4x^3 + 7x^2 + 6x + 4) = D_4$ [6]
T_{32}-[2^3]$A(4)$	$x^8 - x^6 - 3x^2 + 4$	
T_{33}-[$\frac{1}{3}A(4)^2$]2	$x^8 - 4x^7 - 8x^6 + 24x^5 + 36x^4$ $-24x^3 - 48x^2 + 48x - 12$	See text
T_{34}-$E(4)^2$:D_6	$x^8 - 6x^6 - 4x^5 + 24x^4 - 28x^2 + 18$	See text
T_{36}-$E(8)$:F_{21}	$x^8 + 2x^7 + 28x^6 + 84x^5 + 224x^4$ $+392x^3 - 336x + 112$	See text
T_{37}-$PSL(2,7)$	$x^8 + 2x^7 + 28x^6 + 1728x + 3456$	[11]
T_{39}-[2^3]$S(4)$	$x^8 + x^2 + 1$	
T_{41}-$E(4)^2$:D_{12}	$x^8 + 16x^4 + 16x^3 + 8$	
T_{42}-[$A(4)^2$]2	$x^8 + 7x^4 + 8x^3 + 9$	
T_{45}-[$\frac{1}{2}S(4)^2$]2	$x^8 - 8x^6 - 8x^5 + 8$	
T_{48}-$E(8)$:L_7	$x^8 + 14x^5 + 7x^4 - 14x^3 + 4x + 14$	[18]
T_{49}-A_8	$x^8 + 8x^3 + 10$	

Note that $\mathrm{Gal}_K(f)$ has a system of imprimitivity consisting of blocks of size two if f is even, and conversely, given f such that $\mathrm{Gal}(f)$ is imprimitive with blocks of size two, we may construct an even $\tilde{f}$ as follows:

From degree considerations, $f(x)$ with roots $\{\alpha_i\}$, has a quadratic factor ϕ in $\mathbb{Q}(\beta)[x]$ where $f(x) \mid g(h(x))$, β a root of g. The discriminant of ϕ, Δ_ϕ, lies in $\mathbb{Q}(\beta)$

so by eliminating β we obtain

$$\tilde{f} = resultant(x^2 - \Delta_\phi, g(\beta), \beta).$$

Indexing the roots so that

$$\{\alpha_1, \alpha_2 : \alpha_3, \alpha_4 : \ldots : \alpha_{n-1}, \alpha_n\}$$

partitions them into blocks of size two, we find the roots of $\tilde{f}$ are

$$\{\alpha_1 - \alpha_2, \alpha_2 - \alpha_1, \ldots, \alpha_{n-1} - \alpha_n, \alpha_n - \alpha_{n-1}\},$$

so that $\mathrm{Gal}(\tilde{f}) = \mathrm{Gal}(f)$ (provided $\tilde{f}$ has no repeated roots).

For each group in Tables 4 and 5 with such a system of imprimitivity, we give the associated polynomial in x^2.

Gene Smith [20] has provided test polynomials over $\mathbb{Q}(t)$ for all Galois groups of degree ≤ 8.

Remark

We have described techniques which, together, are designed to reduce the potential Galois groups to a single group, $\mathrm{Gal}(f)$. These techniques, when combined with an ad hoc approach to a small proportion of intransigent groups, are practicable and adequate up to degree 8 and, no doubt, further. For example, Hulpke [9] has recently completed an enumeration of permutation groups up to degree 31. However this may be a bound to the degree of f for which we can, in practice, find $\mathrm{Gal}(f)$. In higher degrees there exist pairs of groups [16] which are likely to be extremely hard to separate, having identical irreducible representations and isomorphic proper subgroup structure. The smallest such groups appear to be of order 256 but they have a minimal transitive faithful permutation degree of 32. One such pair is indexed (3678,3679) in O'Brien's [14] 2-group list accessible in GAP and elsewhere. It is true, however, that as a last resort the polynomial invariants of a group identify it uniquely even though they may be unwieldy to work with.

References

[1] G. Butler and J. McKay, 'The transitive groups of degree up to 11', *Comm. Algebra* **11** (1983), 863-911. MR **84f:**20005

[2] D. Casperson and J. McKay, 'Symmetric functions, m-sets, and Galois groups', *Math. Comp.* Vol. 63, No. 208 (1994), 749-757. MR **95a:**12001

[3] ———, 'An ideal decomposition algorithm', preliminary report, *AMS Abstracts* **13** (1992) 405.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993 (ISBN 3-540-55640-0). MR **94i:**11105

[5] J. Conway, A. Hulpke, J. McKay, ' On transitive permutation groups' (to appear).

[6] H. Darmon, private communication (1986).

[7] H. Darmon and D. Ford, 'Computational verification of M_{11} and M_{12} as Galois groups over $\mathbb{Q}$', *Comm. Alg.* **17** (1989), 2941-2943. MR **91b:**11146

[8] F-P. Heider and P. Kolvenbach, 'The construction of SL(2,3)-polynomials', *J. Number Theory* **19** (1984) 392-411. MR **86g:**11063

[9] A. Hulpke, *Konstruktion transitiver Permutationsgruppen*. PhD. thesis, RWTH-Aachen, Aachen, Germany, 1996.

[10] T. W. Mattman, *The computation of Galois groups over function fields*. Master's thesis, McGill University, Montréal, Québec, Canada, December 1992.

[11] B. H. Matzat, 'Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe', *J. Reine und Angew. Math.* **349** (1984), 179-220. MR **85j:**11164

[12] J. McKay, 'Advances in computational Galois theory', in *Computers in algebra*, (Martin C. Tangora, Ed.), *Lecture notes in pure and applied mathematics.*, vol. 111, pp.99-101, (1988). CMP 90:14
[13] J. McKay and E. Regener, 'Actions of permutation groups on r-sets', *Comm. Algebra* **13** (1985) 619-630. MR **86j:**20004
[14] E.A. O'Brien, 'The groups of order 256', *J. Algebra* **143** (1991) 219-235. MR **93e:**20029
[15] M. Olivier, Calcul des groupes de Galois de degré 8,9,10, et 11. Université Bordeaux I, 12 Oct. 1991 et 12 Fev. 1993.
[16] E. Skrzipczyk, *Charaktertafeln von p-Gruppen*. Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule Aachen, Aachen, Germany, 1992.
[17] L. Soicher, *The computation of Galois groups*. Master's thesis, University of Concordia, Montréal, Québec, Canada, April 1981.
[18] ———, 'An Algorithm for Computing Galois Groups', in *Computational Group Theory* (M. D. Atkinson, Ed.), pp. 291-296, Academic Press, 1984. MR **86d:**12002b
[19] L. Soicher and J. McKay, 'Computing Galois groups over the rationals', *J. Number Theory* **20** (1985), 273-281. MR **87a:**12002
[20] Gene W. Smith, 'Some Polynomials over $\mathbb{Q}(t)$ and their Galois groups.' (to appear in *Math. Comp.*).
[21] R. P. Stauduhar, *The automatic determination of Galois groups*. Ph. D. Dissertation, University of California, Berkeley, 1969.
[22] ———, 'The determination of Galois groups', *Math. Comp.* **27** (1973) 981-996. MR **48:**6054
[23] S. Strelitz, 'On the Routh-Hurwitz Problem', *Amer. Math. Monthly* **8** (1977) 542-544. MR **57:**288
[24] B. van der Waerden, *Modern Algebra*. Vol. I, Ungar, (1949) Chapter 7.61. MR **10:**587b

Mathematics Department, McGill University, Montréal, H3A 2K6, Canada
E-mail address: mattman@math.mcgill.ca

Centre Interuniversitaire en Calcul Mathématique Algébrique, Concordia University, Montréal, H3G 1M8, Canada
E-mail address: mckay@cs.concordia.ca