DETERMINING GALOIS GROUPS OF REDUCIBLE POLYNOMIALS VIA DISCRIMINANTS AND LINEAR RESOLVENTS

CHAD AWTREY, TAYLOR CESARSKI, AND PETER JAKES

Abstract. Let $f(x)$ be a polynomial with integer coefficients of degree less than or equal to 7, and assume f is reducible over the rational numbers. We show how to compute the Galois group of f. The main tools we employ are composita of irreducible factors, discriminants, and in the case when f is a degree 7 polynomial, two linear resolvents. For each possible Galois group G, we provide a reducible polynomial whose Galois group over the rationals is G.

1. Introduction

Let $f(x)$ be a polynomial with integer coefficients. A fundamental task in computational number theory is the determination of the Galois group G of f over the rational numbers. When f is irreducible, then many algorithms for determining G appear in the literature, most of which are based on either the relative resolvent method [8] or the absolute resolvent method [7]. For example, the implementation in Magma [1] is based on the relative resolvent method, as described in [10]. The implementation Pari/GP [5] is based on the absolute resolvent method, as described in [2].

Less well studied is the case when f is reducible. Magma's implementation for computing Galois groups is able to accept reducible polynomials as inputs; the approach for reducible polynomials is essentially the same as for irreducible polynomials. See [9] for more details. An alternate approach to computing Galois groups of reducible polynomials is described in [4]; this method also uses relative resolvents.

The purpose of this paper is to introduce a method for computing Galois groups of reducible polynomials that uses linear resolvents [6] (which are absolute resolvents) instead of relative resolvents. Therefore, our approach is suitable for implementation in Pari/GP. Such an implementation is available by contacting the first author.

The remainder of the paper is organized as follows. Section 2 gives an overview of the tools we wlll use; namely, discriminants, polynomial composita, and linear resolvent. Sections 3–6 discuss algorithms for computing Galois groups of reducible polynomials of degrees 4–7, respectively. The final section lists sample reducible polynomials for each possible Galois group.

2010 *Mathematics Subject Classification.* 11R32, 12Y05.

Key words and phrases. reducible polynomials; Galois groups; discriminants; linear resolvents.

2. Preliminaries

Throughout the rest of the paper, we will assume that $f(x)$ is a reducible polynomial of degree less than or equal to 7 with integer coefficients, defined over the rational numbers. Let $f_1, \ldots, f_k$ denote the nonlinear irreducible factors of f, and let G_i denote the Galois group of f_i over the rational numbers. Note that each G_i is a transitive subgroup of S_{n_i} (the symmetric group) where $n_i = \text{degree}(f_i)$, and therefore the Galois group G of f is a subgroup of $\prod_{i=1}^{k} G_i$. If $k = 1$, then this reduces to the case of computing the Galois group of an irreducible polynomial.

For $i, j \in \{1, \ldots, k\}$, we can consider the compositum $\text{comp}(f_i, f_j)$; that is, a polynomial defining the field extension obtained by adjoining a root of both f_i and f_j to the rationals. One way to obtain such a polynomial is to compute the characteristic polynomial of $\alpha + \beta$ where $f_i(\alpha) = f_j(\beta) = 0$. Using resultants, this can be realized as:

$$\text{comp}(f_i, f_j) = \text{Resultant}_y(f_i(y), f_j(x - y)).$$

If the resultant is squarefree, we factor it and choose an irreducible factor of largest degree. Otherwise, we perform a tschirnhaus transformation (see Algorithm 3.6.4 in [2]) on f_i until the resultant is squarefree. Note, only finitely many transformations will yield a resultant that is not squarefree. Note, the Galois group of the compositum is a subgroup of G. In the case where f factors into two irreducible polynomials, the compositum of these two factors gives an irreducible polynomial that defines the splitting field of f. Thus the Galois group of the compositum is isomorphic to the Galois group of f. The Galois groups of these two factors are an invariant of G, as the next proposition shows.

Proposition 2.1. *Suppose $f = f_1 f_2$ where each f_i is irreducible. Let $g = comp(f_1, f_2)$ and let G, G_1, and G_2 denote the Galois groups of g, f_1, and f_2 respectively. Then G_1 and G_2 are invariants of G. In other words, any irreducible polynomial whose degree equals that of g and whose Galois group is G must define a field that contains subfields of the same degrees as f_1 and f_2 such that the Galois groups of the normal closures of these subfields are G_1 and G_2.*

Proof. Let K denote the splitting field of g and F its stem field (obtained by adjoining one root of g to the rationals). By the Galois correspondence, F corresponds to a subgroup H which is the point stabilizer of 1 in G. Since f_1 and f_2 define subfields of K, there exist subgroups H_1 and H_2 of G such that $H \leq H_1, H_2 \leq G$. For $i = 1, 2$, the Galois group of f_i is therefore isomorphic to the image of the permutation representation of G acting on the cosets G/H_i. □

Let $d_i = \text{disc}(f_i)$ denote the discriminant of f_i. Then d_i is a perfect square if and only if G_i is a subgroup of A_{n_i} (the alternating group). For each subset S of $\{1, \ldots, k\}$, we can consider the integer $d_S = \prod_{i \in S} d_i$, which is a product of discriminants of some collection of irreducible factors of f. It follows from the Galois correspondence that the parity of d_S (i.e., whether or not it is a perfect square) is an invariant of G. We can also utilize the product of d_S with various composita to yield additional invariants of G. Clearly we can simply take the composita of all f_i to obtain an irreducible polynomial of degree $1 + \cdots + k$. One drawback of this approach is that the degree can be greater than 11, which is beyond the capability of PARI/GP (but not for Magma). Another drawback is that it is sometimes not

necessary to compute the Galois group of such a large degree polynomial, since we can leverage discriminant data and other information instead.

In Section 6, we will make use of two linear resolvent polynomials (as defined in [7]). In this case, we need an irreducible polynomial $g(x)$ of degree n. For us, n will be 12. For now, we describe how to compute these resolvents in general.

$$dp(x^2) = \frac{\mathrm{comp}(g, g)}{2^n \cdot g(x/2)}$$
$$tp(x^3) = \frac{\mathrm{comp}(dp(g), g) \cdot 3^n \cdot g(x/3)}{\mathrm{comp}(g, 2^n \cdot g(x/2))}$$

The degree of $dp(x)$ is $\binom{n}{2} = n(n-1)/2$ while the degree of $tp(x)$ is $\binom{n}{3} = n(n-1)(n-2)/6$. In the language of [2, §6.3], $dp(x)$ is the linear resolvent of g associated to the multivariable function $T = x_1 + x_2$ that is stabilized by a subgroup of S_n that is isomorphic to $S_2 \times S_{n-2}$. Similary, $tp(x)$ is the linear resolvent of g associated to the function $T = x_1 + x_2 + x_3$ that is stabilized by a subgroup isomorphic to $S_3 \times S_{n-3}$. If the resolvent is squarefree, the degrees of the irreducible factors correspond to orbit lengths of the Galois group of G acting on the cosets of the associated subgroup (see [7] for a proof).

In the remaining sections, we reference Table 1, which gives all possible Galois groups of reducible polynomials up to degree 7. Our notation is of the form $n\mathrm{R}j$ where n is the degree of f and j is an integer. We note that our numbering system is not standard, as there is no standard numbering system for reducible Galois groups. Consequently, we also give a structural description of each Galois group as well as an identification of the group in GAP's [3] SmallGroups library; the notation $[s, k]$ means `SmallGroup(s,k)` in GAP. The structural descriptions are standard; C_n denotes the cyclic group of order n, E_n the elementary abelian group of order n, S_n the symmetric group of order $n!$, A_n the alternating group of order $n!/2$, D_n the dihedral group of order $2n$, $F_p = C_p : C_{p-1}$ the Frobenius group of order $p(p-1)$ for primes p, $\times$ a direct product, and : a semi-direct product.

3. Degree 4

The algorithm for reducible quartic polynomials is straightforward. The only case we consider is when f factors as two quadratics f_1, f_2 and the compositum of f_1 and f_2 has degree 4. Otherwise, f is irreducible (once linear factors are removed and redundant factors are eliminated). In this case, the Galois group G must be isomorphic to a transitive subgroup of S_4 that is itself a subgroup of E_4. Thus $G = E_4$.

4. Degree 5

For reducible quintic polynomials, we only consider the case where f factors as the product of an irreducible quadratic and an irreducible cubic. Otherwise, we can use Section 3 or irreducible algorithms. In this case, the compositum of the two factors will be a degree 6 polynomial whose Galois group is isomorphic to a transitive subgroup G of S_6 that is a subgroup of $S_3 \times C_2 = D_6$. Thus there are three possible Galois groups; namely, C_6, S_3, and D_6. Among these 3, only C_6 has a cyclic cubic subfield; which will occur precisely when the discriminant of the cubic is a perfect square. Otherwise, we can consider the discriminants of the quadratic and cubic polynomials (which are necessarily not perfect squares). Thus each discriminant

TABLE 1. Possible Galois groups of reducible polynomials up to degree 7. Column **R** gives the R number of the group, **Name** gives a structural description of the group, **Size** gives the order of the group, and **GAP** gives a pair [s,k] such that the group is `SmallGroup`(s,k) in GAP's SmallGroups library.

R	**Name**	**Size**	**GAP**
4R1	E_4	2	(4,2)
5R1	S_3	6	(6,1)
5R2	C_6	6	(6,2)
5R3	D_6	12	(12,4)
6R1	$C_4 \times C_2$	8	(8,2)
6R2	D_4	8	(8,3)
6R3	E_8	8	(8,5)
6R4	$D_4 \times C_2$	16	(16,11)
6R5	S_4	24	(24,12)
6R6	$A_4 \times C_2$	24	(24,13)
6R7	$S_4 \times C_2$	48	(48,48)
6R8	E_9	9	(9,2)
6R9	$S_3 \times C_3$	18	(18,3)
6R10	$E_9 : C_2$	18	(18,4)
6R11	$S_3 \times S_3$	36	(36,10)
7R1	D_5	10	(10,1)
7R2	C_{10}	10	(10,2)
7R3	F_5	20	(20,3)
7R4	D_{10}	20	(20,4)
7R5	$F_5 \times C_2$	40	(40,12)
7R6	S_5	120	(120,34)
7R7	$A_5 \times C_2$	120	(120,35)
7R8	$S_5 \times C_2$	240	(240,189)
7R9	$C_3 : C_4$	12	(12,1)
7R10	C_{12}	12	(12,2)
7R11	A_4	12	(12,3)
7R12	D_6	12	(12,4)
7R13	$C_6 \times C_2$	12	(12,5)
7R14	$C_4 \times S_3$	24	(24,5)
7R15	D_{12}	24	(24,60)
7R16	$(C_6 \times C_2) : C_2$	24	(24,8)
7R17	$C_3 \times D_4$	24	(24,10)
7R18	S_4	24	(24,12)
7R19	$E_4 \times S_3$	24	(24,14)
7R20	$A_4 \times C_3$	36	(36,11)
7R21	$D_4 \times S_3$	48	(48,38)
7R22	$S_4 \times C_3$	72	(72,42)
7R23	$(A_4 \times C_3) : C_2$	72	(72,43)
7R24	$A_4 \times S_3$	72	(72,44)
7R25	$S_4 \times S_3$	144	(144,183)

defines a quadratic subfield of the splitting field of the compositum. By the Galois correspondence, these two quadratic subfields correspond to index 2 subgroups of G. Direct computation shows that these two subgroups are the same when $G = S_3$ and they are not equal when $G = D_6$.

Algorithm 4.1 (Reducible Quintics)**.** *Let $f(x) = f_1 f_2$ be a reducible quintic polynomial where f_1 is an irreducible quadratic and f_2 is an irreducible cubic. This algorithm returns the Galois group of f.*

1. *Set $d_1 = disc(f_1)$ and $d_2 = disc(f_2)$.*
2. *If d_2 is a perfect square, return 5R2 and terminate.*
3. *Else, if $d_1 d_2$ is a perfect square, return 5R1 and terminate. Otherwise return 5R3 and terminate.*

5. Degree 6

For reducible sextic polynomials, we consider three cases: where f factors as (1) three irreducible quadratics; (2) two irreducible cubics; (3) and the product of an irreducible quadratic and an irreducible quartic.

5.1. **Three Quadratics.** This case is similar to Section 3. In particular, we will assume that the compositum of all three quadratics has degree 8. Otherwise, we can reduce down to either a quartic polynomial (in which case the Galois group is E_4) or a quadratic. In this case, the Galois group must be a transitive subgroup G of S_8 that is itself a subgroup of E_8. Thus $G = E_8$.

5.2. **A Quadratic and a Quartic.** If f factors as the product of an irreducible quadratic f_1 and an irreducible quartic f_2, we will assume the compositum g of f_1 and f_2 has degree 8. Otherwise, this reduces to the case of an irreducible quartic. Thus the Galois group G must be a transitive subgroup of S_8 that is itself a subgroup of $S_2 \times S_4$. Furthermore, G contains at least one quadratic subfield and at least one quartic subfield. There are exactly 7 possibilities for G; namely, $C_4 \times C_2$, D_4, E_8, $D_4 \times C_2$, S_4, $A_4 \times C_4$, or $S_4 \times C_4$. If the Galois group H of f_2 is either C_4, E_4, or A_4, then $G = H \times C_2$. Otherwise, G is determined by whether or not $d_1 d_2$ is a perfect square. As before, all statements follow from Proposition 2.1 and direct computation on the possible Galois groups.

Algorithm 5.1 (Reducible Sextics (An Irreducible Quadratic and Irreducible Quartic))**.** *Let $f(x) = f_1 f_2$ be a reducible sextic polynomial where f_1 is an irreducible quadratic and f_2 is an irreducible quartic. Let $g(x) = comp(f_1, f_2)$ and assume $degree(g) = 8$. This algorithm returns the Galois group of f.*

1. *Set H equal to the Galois group of f_2.*
2. *Partial answer.*
   (a) *If $H = C_4$, return 6R1 and terminate.*
   (b) *If $H = E_4$, return 6R3 and terminate.*
   (c) *If $H = A_4$, return 6R5 and terminate.*
3. *Set $d_1 = disc(f_1)$ and $d_2 = disc(f_2)$.*
4. *If $H = D_4$, then*
   (a) *If $d_1 d_2$ is a perfect square, return 6R2 and terminate.*
   (b) *Otherwise return 6R4 and terminate.*
5. *If $H = S_4$, then*
   (a) *If $d_1 d_2$ is a perfect square, return 6R6 and terminate.*

(b) *Otherwise return 6R7 and terminate.*

5.3. **Two Cubics.** If f factors as two irreducible cubics f_1 and f_2, we will assume that f_1 and f_2 do not define the same extension (i.e., their compositum has degree 9). Otherwise, this reduces to the case of an irreducible cubic polynomial. Thus the Galois group G must be a transitive subgroup of S_9 that is itself a subgroup of $S_3 \times S_3$. Furthermore, G contains either two cyclic cubic subfields, two S_3 cubic subfields, or one of each. There are only 4 possibilities: E_9, $S_3 \times C_3$, $E_9 : C_2$, and $S_3 \times S_3$. If there are two cyclic cubic subfields, the $G = E_9$. If there is only one cyclic cubic subfield, G is $S_3 \times C_3$. Otherwise, G is determined by the parity of the discriminant of the compositum of the two cubic subfields. If the discriminant is a perfect square, $G = E_9 : C_2$; otherwise, $G = S_3 \times S_3$. All statements follow by direct computation on the four possibilities, utilizing Proposition 2.1.

Algorithm 5.2 (Reducible Sextics (2 Irreducible Cubics))**.** *Let $f(x) = f_1 f_2$ be a reducible sextic polynomial where each f_i is an irreducible cubic polynomial. Let $g(x) = comp(f_1, f_2)$ and assume degree$(g) = 9$. This algorithm returns the Galois group of f.*

1. *Set $d_1 = disc(f_1)$ and $d_2 = disc(f_2)$.*
2. *If both d_1 and d_2 are perfect squares, return 6R8 and terminate.*
3. *If exactly one of d_1 and d_2 is a perfect square, return 6R9 and terminate.*
4. *Set $g = comp(f_1, f_2)$ and $d_3 = disc(g)$.*
5. *If d_3 is a perfect square, return 6R10 and terminate. Otherwise return 6R11 and terminate.*

6. Degree 7

For reducible septic polynomials, we again consider three cases: where f factors as the product of (1) an irreducible quadratic and an irreducible quintic; (2) two irreducible quadratics and an irreducible cubic; (3) and an irreducible cubic and an irreducible quartic.

6.1. **A Quadratic and a Quintic.** If f factors as the product of an irreducible quadratic f_1 and an irreducible quintic f_2, then the compositum g of f_1 and f_2 has degree 10. Thus the Galois group G must be a transitive subgroup of S_{10} that is itself a subgroup of $S_2 \times S_5$. Furthermore, G contains at least one quadratic subfield and at least one quintic subfield. There are 8 possibilities for G; namely, C_{10}, D_5, F_5, D_{10}, $F_5 \times C_2$, S_5, $A_5 \times C_2$, and $S_5 \times C_2$. If the Galois group H of f_2 is either C_5 or A_5, then $G = H \times C_2$. When H is either F_5 or S_5, then G is determined by whether or not $d_1 d_2$ is a perfect square. When $H = D_5$, then G is determined by the degree of comp(g, g).

Algorithm 6.1 (Reducible Septics (An Irreducible Quadratic and Irreducible Quintic))**.** *Let $f(x) = f_1 f_2$ be a reducible septic polynomial where f_1 is an irreducible quadratic and f_2 is an irreducible quintic. Let $g(x) = comp(f_1, f_2)$. This algorithm returns the Galois group of f.*

1. *Set H equal to the Galois group of f_2.*
2. *Partial answer.*
   (a) *If $H = C_5$, return 7R2 and terminate.*
   (b) *If $H = A_5$, return 7R7 and terminate.*
3. *Set $d_1 = disc(f_1)$ and $d_2 = disc(f_2)$.*

(4) *If $H = F_5$, then*
   (a) *If $d_1 d_2$ is a perfect square, return 7R3 and terminate.*
   (b) *Otherwise return 7R5 and terminate.*
(5) *If $H = S_5$, then*
   (a) *If $d_1 d_2$ is a perfect square, return 7R6 and terminate.*
   (b) *Otherwise return 7R8 and terminate.*
(6) *Set $h = comp(g, g)$.*
(7) *If the degree of h is 10, return 7R1 and terminate. Otherwise return 7R4 and terminate.*

6.2. **Two Quadratics and a Cubic.** If f factors as the product of two irreducible quadratics f_1, f_2 and an irreducible cubic f_3, we will assume the compositum g of f_1, f_2, and f_3 has degree 12. Otherwise, this reduces to the case of a reducible quintic. Thus the Galois group G must be a transitive subgroup of S_{12} that is itself a subgroup of $E_4 \times S_3$. Furthermore, G contains at least two quadratic subfields and at least one cubic subfield. There are 3 possibilities for G; namely, D_6, $C_6 \times C_2$, and $E_4 \times S_3$. If the Galois group of f_3 is C_3, then $G = C_6 \times C_2$. Otherwise, G has three quadratic subfields whose discriminants are d_1, d_2, and $d_1 d_2$. If one of these fields defines the same field as $x^2 - \mathrm{disc}(f_3)$, then $G = D_6$. Otherwise $G = E_4 \times S_3$.

Algorithm 6.2 (Reducible Septics (Two Irreducible Quadratics and an Irreducible Cubic))**.** *Let $f(x) = f_1 f_2 f_3$ be a reducible septic polynomial where f_1 and f_2 are irreducible quadratics and f_3 is an irreducible cubic. Let $g(x) = comp(comp(f_1, f_2), f_3)$ and assume degree$(g) = 12$. This algorithm returns the Galois group of f.*

(1) *Set d_1, d_2, and d_3 equal to the discriminant of f_1, f_2, and f_3 respectively.*
(2) *If d_3 is a perfect square, return 7R13 and terminate.*
(3) *Set $c_1 = d_1 d_3$, $c_2 = d_2 d_3$, and $c_3 = d_1 d_2 d_3$.*
(4) *If none of c_1, c_2, c_3 are perfect squares, return 7R20 and terminate. Otherwise return 7R12 and terminate.*

6.3. **A Cubic and a Quartic.** If f factors as the product of an irreducible cubic f_1 and an irreducible quarticf_2, then their compositum g has degree 12. Then the Galois group G of f is isomorphic to the Galois group of g. Thus G must be a transitive subgroup of S_{12} that is itself a subgroup of $S_3 \times S_4$. Furthermore, G contains a cubic subfield and a quartic subfield. This is the most difficult case considered in this paper, as there are 17 possibilities for G. These are $C_3 : C_4$, C_{12}, A_4, D_6, $C_6 \times C_2$, $C_4 \times S_3$, D_{12}, $(C_6 \times C_2) : C_2$, $C_3 \times D_4$, S_4, $E_4 \times S_3$, $A_4 \times C_3$, $D_4 \times S_3$, $S_4 \times C_3$, $(A_4 \times C_3) : C_2$, $A_4 \times S_3$, and $S_4 \times S_3$. If H_1 is the Galois group of f_1 and H_2 is the Galois group of f_2, then H_1 and H_2 determine G in 5 cases. If degree(comp$(g, g)) = 12$, then H_1 and H_2 determine G in 6 additional cases. The remaining cases require the absolute resolvents $tp(x)$ and $dp(x)$ referenced in Section 2.

Algorithm 6.3 (Reducible Septics (Irreducible Cubic and Irreducible Quartic))**.** *Let $f(x) = f_1 f_2$ be a reducible septic polynomial where f_i is an irreducible cubic polynomial and f_2 is an irreducible quartic polynomial. Let $g(x) = comp(f_1, f_2)$. This algorithm returns the Galois group of f.*

(1) *Set $d_1 = disc(f_1)$, $d_2 = disc(f_2)$, H_1 the Galois group of f_1, and H_2 the Galois group of f_2.*
(2) *Partial answer.*

(a) *If* $(H_1, H_2) = (C_3, C_4)$*, return 7R10 and terminate.*
(b) *If* $(H_1, H_2) = (C_3, E_4)$*, return 7R13 and terminate.*
(c) *If* $(H_1, H_2) = (C_3, D_4)$*, return 7R17 and terminate.*
(d) *If* $(H_1, H_2) = (C_3, S_4)$*, return 7R22 and terminate.*
(e) *If* $(H_1, H_2) = (S_3, A_4)$*, return 7R24 and terminate.*

(3) *Set* $h = comp(g, g)$.
(4) *If* $(H_1, H_2) = (C_3, A_4)$*, then*
   (a) *If* $degree(h) = 12$*, return 7R11 and terminate.*
   (b) *Otherwise return 7R20 and terminate.*
(5) *If* $(H_1, H_2) = (S_3, C_4)$*, then*
   (a) *If* $degree(h) = 12$*, return 7R9 and terminate.*
   (b) *Otherwise return 7R14 and terminate.*
(6) *If* $(H_1, H_2) = (S_3, E_4)$*, then*
   (a) *If* $degree(h) = 12$*, return 7R12 and terminate.*
   (b) *Otherwise return 7R19 and terminate.*
(7) *Set* t *equal to the list of degrees of irreducible factors of* $tp(g)$.
(8) *If* $(H_1, H_2) = (S_3, S_5)$*, then*
   (a) *If* $t = [4, 4, 8, 12, 12, 12, 24, 24, 24, 24, 24, 24, 24]$*, return 7R18 and terminate.*
   (b) *If* $t = [4, 12, 12, 12, 36, 72, 72]$*, return 7R23 and terminate.*
   (c) *If* $t = [4, 12, 24, 36, 72, 72]$*, return 7R25 and terminate.*
(9) *If* $t = [4, 12, 12, 24, 24, 24, 24, 48, 48]$*, return 7R21 and terminate.*
(10) *If* $t = [4, 12, 12, 12, 12, 12, 12, 24, 24, 24, 24, 24, 24]$*, return 7R16 and terminate.*
(11) *Set* d *equal to the list of degrees of irreducible factors of* $dp(g)$.
(12) *If* $d = [6, 12, 12, 12, 12, 12]$*, return 7R15 and terminate. Otherwise return 7R16 and terminate.*

We note that in Steps (10) and (12) of Algorithm 6.3, a Galois group of 7R16 $= (C_6 \times C_2) : C_2$ is returned. The reason why the Galois group occurs twice here is because as a transitive subgroup of S_{12}, the group 7R16 occurs as two non-conjugate representations. Using GAP's transitive group library, Step (10) returns `TransitiveGroup(12,15)` while Step (12) returns `TransitiveGroup(12,13)`.

7. Polynomial List

In this section we list reducible polynomials for each possible Galois group appearing in Table 1. Table 2 lists the polynomials (in factored form). Column headers are the same as in Table 1.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.
[3] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.
[4] Sébastien Orange, Guenaël Renault, and Annick Valibouze. Note sur les relations entre les racines d'un polynôme réductible. *Theor. Inform. Appl.*, 39(4):651–659, 2005.
[5] PARI Group, The. *PARI/GP – Computational Number Theory, version 2.5.3*, 2013. available from `http://pari.math.u-bordeaux.fr/`.

TABLE 2. Sample polynomials for each possible Galois group appearing in Table 1.

R	**Name**	**Size**	**Polynomial**
4R1	E_4	2	$(x^2+1)(x^2+2)$
5R1	S_3	6	$(x^2+3)(x^3+2)$
5R2	C_6	6	$(x^2+1)(x^3-3x+1)$
5R3	D_6	12	$(x^2+1)(x^3+2)$
6R1	$C_4 \times C_2$	8	$(x^2+1)(x^4+4x^2+2)$
6R2	D_4	8	$(x^2-2)(x^4+2)$
6R3	E_8	8	$(x^2+2)(x^4+1)$
6R4	$D_4 \times C_2$	16	$(x^2+1)(x^4+2)$
6R5	S_4	24	$(x^2-229)(x^4+x+1)$
6R6	$A_4 \times C_2$	24	$(x^2+1)(x^4-7x^2-3x+1)$
6R7	$S_4 \times C_2$	48	$(x^2+1)(x^4+x+1)$
6R8	E_9	9	$(x^3-3x+1)(x^3-x^2-2x+1)$
6R9	$S_3 \times C_3$	18	$(x^3-3x+1)(x^3+2)$
6R10	$E_9 : C_2$	18	$(x^3+2)(x^3+3)$
6R11	$S_3 \times S_3$	36	$(x^3+2)(x^3+4)$
7R1	D_5	10	$(x^2-x+12)(x^5-2x^4+2x^3-x^2+1)$
7R2	C_{10}	10	$(x^2+1)(x^5-x^4-4x^3+3x^2+3x-1)$
7R3	F_5	20	$(x^2-2x-12)(x^5-x^4+2x^3-4x^2+x-1)$
7R4	D_{10}	20	$(x^2+1)(x^5-2x^4+2x^3-x^2+1)$
7R5	$F_5 \times C_2$	40	$(x^2+1)(x^5-x^4+2x^3-4x^2+x-1)$
7R6	S_5	120	$(x^2+1)(x^5-x^4+3x^2-6x+2)$
7R7	$A_5 \times C_2$	120	$(x^2+1)(x^5-x^4+2x^2-2x+2)$
7R8	$S_5 \times C_2$	240	$(x^2+1)(x^5-x^4-x^3+x^2-1)$
7R9	$C_3 : C_4$	12	$(x^3-12x-14)(x^4-x^3+x^2-x+1)$
7R10	C_{12}	12	$(x^3-3x+1)(x^4+4x^2+2)$
7R11	A_4	12	$(x^3-x^2-20x+9)(x^4-7x^2-3x+1)$
7R12	D_6	12	$(x^3-3)(x^4-2x^2+4)$
7R13	$C_6 \times C_2$	12	$(x^3-3x+1)(x^4+1)$
7R14	$C_4 \times S_3$	24	$(x^3+2)(x^4+4x^2+2)$
7R15	D_{12}	24	$(x^3+3x-3)(x^4-x^3-x^2-x+1)$
7R16	$(C_6 \times C_2) : C_2$	24	$(x^3-x^2-3x+1)(x^4-x^3-2x^2+3)$ $(x^3-x^2+x+1)(x^4-x^3+x^2+x+1)$
7R17	$C_3 \times D_4$	24	$(x^3-3x+1)(x^4+2)$
7R18	S_4	24	$(x^3-4x-1)(x^4-x+1)$
7R19	$E_4 \times S_3$	24	$(x^3+2)(x^4+1)$
7R20	$A_4 \times C_3$	36	$(x^3-3x+1)(x^4-7x^2-3x+1)$
7R21	$D_4 \times S_3$	48	$(x^3+2)(x^4+2)$
7R22	$S_4 \times C_3$	72	$(x^3-3x+1)(x^4+x+1)$
7R23	$(A_4 \times C_3) : C_2$	72	$(x^3-2)(x^4-2x^3-6x+3)$
7R24	$A_4 \times S_3$	72	$(x^3+2)(x^4-7x^2-3x+1)$
7R25	$S_4 \times S_3$	144	$(x^3+2)(x^4+x+1)$

[6] Leonard Soicher. The computation of Galois groups. Master's thesis, Concordia University, Montreal, 1981.
[7] Leonard Soicher and John McKay. Computing Galois groups over the rationals. *J. Number Theory*, 20(3):273–281, 1985.
[8] Richard P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.
[9] Nicole Sutherland. Computing Galois groups of polynomials (especially over function fields of prime characteristic). *J. Symbolic Comput.*, 71:73–97, 2015.
[10] Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *J. Symbolic Comput.*, 52:17–34, 2013.

Elon University, Campus Box 2320, Elon, NC 27244
E-mail address: cawtrey@elon.edu

Elon University, Campus Box 4112, Elon, NC 27244
E-mail address: tcesarski@elon.edu

Elon University, Campus Box 6155, Elon, NC 27244
E-mail address: pjakes@elon.edu