North Carolina Journal of
Mathematics and Statistics
Volume 4, Pages 1–11 (Accepted January 17, 2018, published January 31, 2018)
ISSN 2380-7539

Subfields of Solvable Sextic Field Extensions

Chad Awtrey and Peter Jakes

ABSTRACT. Let F be a field, $f(x) \in F[x]$ an irreducible polynomial of degree six, K the stem field of f, and G the Galois group of f over F. We show G is solvable if and only if K/F has either a quadratic or cubic subfield. We also show that G can be determined by: the size of the automorphism group of K/F, the discriminant of f, and the discriminants of polynomials defining intermediate fields. Since most methods for computing polynomials defining intermediate subfields require factoring f over its stem, we include a method that does not require factorization over K, but rather only relies factoring two linear resolvent polynomials over F.

1. Introduction

The well-known quadratic formula shows that quadratic polynomials are "solvable by radicals." That is, their roots can be expressed using only:

(1) the polynomial's coefficients
(2) the four arithmetic operations $(+, -, \times, \div)$
(3) radicals (square roots, cube roots, etc.)

In the 16th century, Italian mathematicians proved that cubic and quartic polynomials too are solvable by radicals. However the same is not true for polynomials of degree five and higher, a fact first proved in the 19th century. How can we determine which polynomials are solvable by radicals?

One answer to the above question is given by Galois theory, an area of mathematics named in honor of French mathematician Evariste Galois. The work of Galois shows we can attach a group structure to a polynomial's roots. We call this group the Galois group of the polynomial. Properties of the Galois group encode arithmetic information concerning the polynomial's roots. For example, the polynomial is solvable by radicals if and only if its Galois group is solvable.

Therefore a standard problem in computational algebra involves designing and implementing algorithms that can determine a polynomial's Galois group. Methods for accomplishing this task have been in existence for more than a century. In fact, the original definition of the Galois group implicitly contained a technique for its determination. For a degree n polynomial, this approach essentially involves analyzing an auxiliary polynomial of degree $n!$ (see van der Waerden (1991), for example). Better methods are clearly needed.

Most modern implementations rely heavily on resolvent polynomials. These are polynomials that define subfields of the original polynomial's splitting field (see Stauduhar (1973)). The resolvent method can be divided into two approaches: (1) the absolute resolvent method, which deals with general groups, and (2) the relative resolvent method, for when the Galois group is known to

Received by the editors March 31, 2017, revised version received January 16, 2018.
2010 *Mathematics Subject Classification.* 11R32; 12Y05.
Key words and phrases. Sextic polynomials; Galois group computation; Subfields; Absolute resolvents.

have a certain structure ahead of time. For example, the algorithm used by gp (2013) uses absolute resolvents to compute Galois groups over the rational numbers up to and including degree 11. Details of the algorithm (up to degree 7) can be found in Cohen (1993). Similarly, the algorithm in Magma (Bosma et al., 1997) uses relative resolvents. Magma's algorithm is in principle not limited by the degree of the polynomial, and the base field can be more general than the rational numbers. Magma's implementation utilizes an extra feature that improves running times for imprimitive extensions (i.e., extensions with nontrivial, proper subfields); namely, it first computes subfields of the stem field of f (see van Hoeij et al. (2013)). By stem field, we mean the field extension obtained by adjoining one root of the polynomial to the base field. The task of computing polynomials defining subfields involves factoring the original polynomial over its stem field. Leveraging this subfield information and initial absolute resolvent information, Magma's algorithm proceeds with the relative resolvent method using degree-independent algorithms as described in Fieker and Klüners (2014) and Elsenhans (2017).

A benefit of Magma's algorithm for determining Galois groups is the subfield information it exploits. However, Magma's approach can be improved. In particular, the size of the automorphism group is easy to determine by factoring a polynomial over its stem field (just count the number of linear factors). This number is an invariant of the Galois group of the polynomial, as shown in Awtrey et al. (2015) for example. Since Magma's approach to computing subfields already involves factoring the polynomial over its stem fields, it makes sense to also use the size of the automorphism group when determining Galois groups. Furthermore, discriminants of polynomials defining subfields can be leveraged as well. But this is not done in Magma's algorithm. The purpose of this paper is to show how Galois groups of polynomials defining solvable sextic extensions can be computed without resorting to relative resolvents, as Magma does.

The remainder of the paper is organized as follows. In Section 2, we prove that if $f(x)$ defines a sextic extension K/F with solvable Galois group G, then K/F must have at least one proper, nontrivial subfield. While Magma and Pari/GP provide algorithms for computing subfields (e.g., van Hoeij et al. (2013)), these methods require the ability to factor a polynomial over an extension field. In Section 3, we show how to compute defining polynomials of subfields by factoring two resolvent polynomials over the base field. Furthermore, our resolvent polynomials are formed as resultants, and therefore do not require approximation of roots; normally, forming resolvents requires computing approximations to the roots of f Stauduhar (1973). We end with Section 4, which describes our algorithm for computing the Galois group of a solvable sextic polynomial. Also included in this section are examples of our algorithm in action.

2. Subfields of solvable sextic extensions

Let F be a field, $f(x) \in F[x]$ an irreducible sextic polynomial, K/F the stem field of f, and G the Galois group of f over F. In this section, we show that G is solvable if and only if K/F contains at least one proper, nontrivial subfield.

To accomplish this, we will analyze and perform computations on the possible Galois groups of f. Since f is irreducible of degree six, once we fix an ordering of the roots of f is some algebraic closure $\overline{F}$ of F, we can view G as a transitive subgroup of S_6; G is transitive because of f is irreducible. In this case, G is well-defined up to conjugation; different orderings of the roots correspond to different conjugates of G in S_6. Therefore, our approach requires that we identify the conjugacy classes of transitive subgroups of S_6 in order to determine the group structure of G. This information is well known (see Butler and McKay (1983)). In Table 2.1, we give information on the

TABLE 2.1. The 16 conjugacy classes of transitive subgroups of S_6. Generators are for one representative in each conjugacy class.

T	**Name**	**Generators**	**Size**	**Solvable?**
1	C_6	(12)(34)(56), (135)(246)	6	yes
2	S_3	(123)(456), (14)(26)(35)	6	yes
3	D_6	(12)(34)(56), (135)(246), (35)(46)	12	yes
4	A_4	(34)(56), (12)(56), (135)(246)	12	yes
5	$C_3 \times S_3$	(456), (123), (14)(25)(36)	18	yes
6	$C_2 \times A_4$	(56), (34), (12), (135)(246)	24	yes
7	S_4^+	(34)(56), (12)(56), (135)(246), (35)(46)	24	yes
8	S_4^-	(34)(56), (12)(56), (135)(246), (3546)	24	yes
9	$S_3 \times S_3$	(456), (123), (23)(56), (14)(25)(36)	36	yes
10	$E_9 \rtimes C_4$	(456), (123), (23)(56), (14)(2536)	36	yes
11	$C_2 \times S_4$	(56), (34), (12), (145)(236), (35)(46)	48	yes
12	A_5	(12346), (14)(56)	60	no
13	$E_9 \rtimes D_4$	(465), (45), (123), (23), (14)(25)(36)	72	yes
14	S_5	(15364), (16)(24), (3465)	120	no
15	A_6	(12345), (456)	360	no
16	S_6	(123456), (12)	720	no

16 conjugacy classes of transitive subgroups of S_6, including their transitive number (or T-number, as in GAP (2013)), generators of one representative, their size, whether the group is solvable, and a more descriptive name based on their structure. The descriptive names are standard: C_n represents the cyclic group of order n, D_n the dihedral group of order $2n$, E_n the elementary abelian group of order n, A_n and S_n the alternating and symmetric groups on n letters, $\times$ a direct product, and $\rtimes$ a semi-direct product.

Before we prove the main result of this section, we establish the fact that the list of Galois groups of the normal closures of nonisomorphic intermediate subfields is an invariant of the polynomial's Galois group.

Proposition 2.1. *Let F be a field, $f(x) \in F[x]$ an irreducible polynomial, K/F the stem field of f, and G the Galois group of f over F. Let L be the list of the Galois groups of the normal closures of all nonisomorphic intermediate subfields of K/F. Then L is an invariant of G. That is, if $f' \in F[x]$ is any other irreducible polynomial of the same degree as f, K' is its stem field, L' is the list of Galois groups of normal closures of nonisomorphic intermediate subfields of K'/F, and G is the Galois group of f' over F, then $L' = L$.*

Proof. Let G_1 be the point stabilizer of 1 in G. By the Galois correspondence, G_1 is the subgroup fixing K/F. Therefore the nonisomorphic intermediate subfields of K/F correspond to the subgroups H of G containing G_1, up to conjugation. Suppose E is one such subfield of K/F, and let H be the subgroup that fixes E. Then the Galois group of the normal closure of E is isomorphic to the image of the permutation representation of G acting on the cosets G/H. If L is the list of Galois groups of normal closures of the nonisomorphic intermediate subfields of K/F, then L is determined completely by a group-theoretic computation. This proves L is an invariant of G. □

If we know the Galois group G of a polynomial f defining the extension K/F, we can use the proof of Proposition 2.1 to compute the list L of Galois groups of normal closures of nonisomorphic intermediate subfields. Table 2.2 contains this data for each of the 16 transitive subgroups of

TABLE 2.2. The list **GalSubs** of Galois groups of normal closures of nonisomorphic intermediate subfields of the stem field of a polynomial whose Galois group G is one of the 16 transitive subgroups of S_6. The presence of no subfields is indicated by blank cell.

T	**Name**	**GalSubs**	**Solvable?**
1	C_6	C_2, C_3	yes
2	S_3	C_2, S_3	yes
3	D_6	C_2, S_3	yes
4	A_4	C_3	yes
5	$C_3 \times S_3$	C_2	yes
6	$C_2 \times A_4$	C_3	yes
7	S_4^+	S_3	yes
8	S_4^-	S_3	yes
9	$S_3 \times S_3$	C_2	yes
10	$E_9 \rtimes C_4$	C_2	yes
11	$C_2 \times S_4$	S_3	yes
12	A_5		no
13	$E_9 \rtimes D_4$	C_2	yes
14	S_5		no
15	A_6		no
16	S_6		no

S_6. When the extension has no subfields, the corresponding entry in the table is left blank. Group names are standard.

We computed this data with the software program GAP GAP (2013). For example, here are two functions we wrote for GAP which will accomplish this task. The main function is `SubfieldGals`, which takes one input, a transitive subgroup of S_n for some $n < 31$ (GAP's TransitiveGroup library only goes up to $n = 30$). The other function `RemoveConjugateSubgroups` is just an auxiliary function that we use in `SubfieldGals`. Note, the transitive subgroups of S_6 can be accessed in GAP by typing `TransitiveSubgroup(6,j)` for some $1 \leq j \leq 16$.

```
---------------------------
RemoveConjugateSubgroups := function(g,lis)
  local c,copy,nlis;
    c := 1;
    copy := ShallowCopy(lis);
    nlis := [lis[1]];
    copy := Filtered(copy,j->IsConjugate(g,nlis[c],j)=false);
      while Size(copy)>0 do
        Append(nlis,[copy[1]]);
        c := c+1;
        copy := Filtered(copy,j->IsConjugate(g,nlis[c],j)=false); od;
  return(nlis);
end;

---------------------------

SubfieldGals := function(g)
```

```
  local n,b,stab,sub,perm,perms,myperm,deg,degs,mydeg;
    n := Size(Orbits(g)[1]);
    b := AllBlocks(g);
      if
        Size(b)=0 then return([]);
      else
        stab   := List(b,j->Stabilizer(g,j,OnSets));
        sub    := RemoveConjugateSubgroups(g,stab);
        perm   := List(sub,j->Group(List(GeneratorsOfGroup(g),
                    i->Permutation(i,RightCosets(g,j),OnRight))));
        deg    := List(perm,j->Size(Orbits(j)[1]));
        degs   := ShallowCopy(deg);
        mydeg  := Permuted(degs,SortingPerm(deg));
        perms  := ShallowCopy(perm);
        myperm := Permuted(perms,SortingPerm(deg)); fi;
  return(List([1..Size(myperm)],j->[mydeg[j],
    TransitiveIdentification(myperm[j])]));
end;
---------------------------
```

Our main result for this section now follows easily from Proposition 2.1 and Table 2.2.

Corollary 2.2. *Let F be a field, $f(x) \in F[x]$ an irreducible sextic polynomial, K/F the stem field of f, and G the Galois group of f over F. Then G is solvable if and only if K/F has at least one proper, nontrivial intermediate subfield.*

Proof. By Proposition 2.1, the number of nonisomorphic intermediate subfields of K/F is an invariant of G. By Table 2.2, this number is greater than 0 if and only if G is solvable. □

3. Computing Subfields Via Linear Resolvents

While Magma and Pari/GP include methods for determining polynomials defining subfields of some extension K/F van Hoeij et al. (2013), their respective algorithms rely on factorization methods over the extension K/F, which can be more expensive than factorization over the base field F. In this section, we show how to compute subfields of sextic extensions using two linear absolute resolvent polynomials.

In general, resolvent polynomials are constructed as follows. Let $f(x) \in F[x]$ be irreducible polynomial of degree n, and let G be the Galois group of f over F. Let H be a subgroup of S_n. We form a resolvent polynomial $R(x)$ whose stem field corresponds to H under the Galois correspondence. Then as shown in Soicher and McKay (1985), the Galois group of $R(x)$ is isomorphic to the image of the permutation representation of G acting on the cosets S_n/H. The irreducible factors of $R(x)$ therefore correspond to the orbits of this action. In particular, the degrees of the irreducible factors correspond to the orbit lengths.

The most difficult task in the resolvent method is constructing the polynomial $R(x)$ that corresponds to a given subgroup H of S_n. The following result gives one method for accomplishing such a task. A proof can be found in Soicher and McKay (1985).

Theorem 3.1. *Let $f(x) \in F[x]$ be an irreducible polynomial of degree n, K the splitting field of f, and $\rho_1, \ldots, \rho_n$ the roots of f in $\overline{F}$. Let $T(x_1, \ldots, x_n)$ be a polynomial with coefficients from F,* *and let H be the stabilizer of T in S_n. That is*

$$H = \{\sigma \in S_n : T(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = T(x_1, \ldots, x_n)\}.$$

Let $S_n//H$ denote a complete set of (right) coset representatives of H in S_n, and define the resolvent polynomial $R(x)$ by:

$$R(x) = \prod_{\sigma \in S_n//H} (x - T(\rho_{\sigma(1)}, \ldots, \rho_{\sigma(n)})).$$

(1) If $R(x)$ is squarefree, its Galois group is isomorphic to the image of the permutation representation of G acting on the cosets S_n/H.

(2) We can ensure $R(x)$ is squarefree by taking a suitable Tschirnhaus transformation of $f(x)$ (Cohen, 1993, p.324).

(3) One choice for T is given by:

$$T(x_1, \ldots, x_n) = \sum_{\sigma \in H} \left(\prod_{i=1}^{n} x^i_{\sigma(i)} \right).$$

Though this is not the only choice.

A special class of resolvents, which Soicher calls *linear resolvents* Soicher (1981), arise when the multivariable function T is of the form:

$$T = \sum_{i=1}^{k} x_i = x_1 + x_2 + x_3 + \cdots + x_k.$$

For a given k, it is straightforward to show that T is stabilized by a subgroup H of S_n of the form $S_k \times S_{n-k}$. Thus the resolvent polynomial has degree $\binom{n}{k}$, and its roots are all possible sums of k roots, without repeats so as to avoid a non-squarefree resolvent.

As shown in Soicher (1981), these linear resolvents can be computed as resultants. We will make use of two such linear resolvents; when $k = 2$ and when $k = 3$. To distinguish these two resolvents, we will refer to the resolvent corresponding to $k = 2$ as dp, and the resolvent corresponding to $k = 3$ as tp. In other words, dp is the resolvent corresponding to the multivariable function $T = x_1 + x_2$. Similarly, tp is the resolvent corresponding to $T = x_1 + x_2 + x_3$. Each resolvent requires us to compute a compositum. If $f(x)$ and $g(x)$ are two polynomials, then define $\text{comp}(f, g)$ as follows:

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

So $\text{comp}(f, g)$ is the characteristic polynomial of $\alpha + \beta$ where $f(\alpha) = g(\beta) = 0$. Here is how we construct dp and tp for a degree n polynomial $f(x)$:

$$dp(x^2) = \frac{\text{comp}(f, f)}{2^n \cdot f(x/2)}$$

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

If we know the Galois group G of a polynomial f defining the extension K/F, we can use Theorem 3.1 to compute the degrees of the irreducible factors of dp and tp by a group-theoretic computation. Table 3.1 contains this data for each of the solvable transitive subgroups of S_6.

As before, we computed the data in Table 3.1 with the software program GAP. For example, here are two functions we wrote for GAP which will accomplish this task in general. The main function is `ResFactors`, which takes three inputs: the degree n of the polynomial, a subgroup

TABLE 3.1. The list of degrees of irreducible factors of the linear resolvent polynomials **DP** and **TP** for the solvable transitive subgroups of S_6.

T	**Name**	**DP**	**TP**
1	C_6	3,6,6	2,6,6,6
2	S_3	3,3,3,6	2,6,6,6
3	D_6	3,6,6	2,6,12
4	A_4	3,12	4,4,6,6
5	$C_3 \times S_3$	6,9	2,18
6	$C_2 \times A_4$	3,12	6,6,8
7	S_4^+	3,12	4,4,12
8	S_4^-	3,12	8,12
9	$S_3 \times S_3$	6,9	2,18
10	$E_9 \rtimes C_4$	6,9	2,18
11	$C_2 \times S_4$	3,12	8,12
13	$E_9 \rtimes D_4$	6,9	2,18

H of S_n, and a transitive subgroup G of S_n. The other function `LinRes` takes two inputs n and k and computes the direct product $S_k \times S_{n-k}$, which is the subgroup stabilizing the multivariable function $T = \sum_{i=1}^{k} x_i$.

```
---------------------------
LinRes := function(n,k)
  local h;
    h := DirectProduct(SymmetricGroup([1..k]),
           SymmetricGroup([k+1..n]));
  return(h);
end;

---------------------------

ResFactors := function(n, h, g)
  local sn, cosets, index, permrep, orb, orbs;
    sn      := SymmetricGroup(n);
    cosets  := RightCosets(sn,h);
    index   := Size(cosets);
    permrep := Group(List(GeneratorsOfGroup(g),
                 j->Permutation(j, cosets, OnRight)));
    orb     := List(Orbits(permrep, [1..index]), Size);
    orbs    := ShallowCopy(orb);
  return(Permuted(orbs, SortingPerm(orb)));
end;
---------------------------
```

When we compare Tables 2.2 and 3.1, we see that a sextic extension K/F defined by the polynomial f has a cubic subfield if and only if $dp(f)$ has a cubic irreducible factor. Similarly, K/F has a quadratic subfield if and only if $tp(f)$ has a quadratic irreducible factor. This is not a coincidence, as we show next. In particular, Proposition 3.2 shows that dp computes polynomials defining subfields of index two and tp computes polynomials defining index three subfields, when they exist.

Proposition 3.2. *Let F be a field, $f(x) \in F[x]$ an irreducible polynomial of degree n, K/F the stem field of f, G the Galois group of f over F, and $dp(f)$ and $tp(f)$ the linear resolvents (as defined above). For a nontrivial, proper divisor k of n, K/F has an index k subfield if and only if the linear resolvent corresponding to the subfield $S_k \times S_{n-k}$ has an irreducible factor of degree n/k. In particular, if K/F is a sextic extension, it has a cubic subfield if and only if $dp(f)$ has an irreducible cubic factor. Similarly, K/F has a quadratic subfield if and only if $tp(f)$ has an irreducible quadratic factor.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ denote the roots of f in $\overline{F}$, and let G_1 be the point stabilizer of 1 in G. So G_1 is the subgroup fixing $K/F = F(\alpha_1)$. As mentioned in the proof of Proposition 2.1, the nonisomorphic intermediate subfields of K/F correspond to subgroups of G containing G_1, up to conjugation. Let H be one of these intermediate groups corresponding to a subfield L. If $[G : H] = n/k$, it follows from the theory of blocks Wielandt (1964) that H partitions the set of roots into n/k sets of size k. Let B_i denote the subsets of roots arising from this partition for $1 \leq i \leq n/k$. For each i, define ρ_i by

$$\rho_i = \sum_{\alpha \in B_i} \alpha.$$

Define the polynomial $g(x)$ by

$$g(x) = \prod_{i=1}^{n/k} (x - \rho_i).$$

Thus g is the characteristic polynomial of ρ_1. Therefore if g is squarefree, it defines the extension L. We can always ensure g is squarefree by taking a suitable Tschirnhaus transformation of f. Notice that each root of g corresponds to a particular sum of k roots of f.

Now consider a linear resolvent corresponding to the multivariable function $T = \sum_{i=1}^{k} x_i$ that is stabilized by $S_k \times S_{n-k}$. It follows that the roots of this resolvent are the possible sums of k roots of f. Consequently if the resolvent is squarefree, it is guaranteed to have an irreducible factor of degree n/k defining a subfield of degree n/k if and only if K/F has a subfield of index k. This proves the first claim of the theorem. The final two claims follows since dp and tp correspond to the cases $k = 2$ and $k = 3$, respectively. □

4. Algorithm

We now turn our attention to computing the Galois group in the case where K/F has at least one intermediate subfield. According to Corollary 2.2, this is precisely the case when the Galois group of f is solvable.

In our algorithm, we make use of the size of the automorphism group of K/F as well as the discriminants of f and the discriminants of the polynomials defining the subfields of K/F. Our next result forms the basis of our algorithm.

Proposition 4.1. *Let F be a field, $f(x) \in F[x]$ an irreducible sextic polynomial, K/F the stem field of f, G the Galois group of f over F, $g(x)$ a polynomial defining the cubic subfield of K/F (if it exists), and $h(x)$ a polynomial defining the quadratic subfield of K/F (if it exists). Then,*

(1) Let Aut(K/F) denote the automorphism group of K/F.

(a) The size of Aut(K/F) is six if and only if G is either C_6 or S_3.

(b) The size of Aut(K/F) is three if and only if $G = C_3 \times S_3$.

(c) The size of Aut(K/F) is two if and only if G is either D_6, A_4, $C_2 \times A_4$, S_4^+, S_4^-, or $C_2 \times S_4$.

(d) The size of Aut(K/F) is one if and only if G is either $S_3 \times S_3$, $E_9 \rtimes C_4$, or $E_9 \rtimes D_4$.

(2) The discriminant of f is a perfect square if and only if G is either A_4, S_4^+, or $E_9 \rtimes C_4$.

(3) The discriminant of f times the discriminant of g is a perfect square if and only if G is either S_3, A_4, or S_4^-.

(4) The discriminant of f times the discriminant of h is a perfect square if and only if G is either C_6, S_3, D_6, $C_3 \times S_3$, or $S_3 \times S_3$.

Proof. By Awtrey et al. (2015), Aut(K/F) is isomorphic to the centralizer of G in S_6. Direct computation on the solvable transitive subgroups of S_6 proves item (1).

The discriminant of f is a perfect square if and only if G is a subgroup of A_6. Item (2) follows by direct computation on the solvable transitive subgroups of S_6.

To prove items (3) and (4), we first suppose G is either C_6, A_4, $C_2 \times A_4$, S_4^+, or $E_9 \rtimes C_4$, since in these cases either the discriminant of f is a perfect square or the discriminant of g is a perfect square. Using Table 2.2, we see that the product of the discriminants of f and g is a perfect square precisely when $G = A_4$. Similarly the product of the discriminants of f and h is a perfect square precisely when $G = C_6$.

For the remainder of the proof, we assume G is either S_3, D_6, $C_3 \times S_3$, S_4^-, $S_3 \times S_3$, $C_2 \times S_4$, or $E_9 \rtimes D_4$. Let d_f, d_g, and d_h denote the discriminants of f, g, and h, respectively. Thus the polynomials $x^2 - d_f$, $x^2 - d_g$, and $x^2 - d_h$ are all irreducible. Let G_g and G_h denote the subgroups corresponding to the stem fields of g and h, respectively. By the Galois correspondence, the stem field of $x^2 - d_f$ corresponds to $H_f = A_6 \cap G$. Similarly, let K_g and K_h denote the normal closures of g and h, respectively. Then the subgroups fixing K_g and K_h are the normal cores $\mathrm{Core}_G(G_g)$ and $\mathrm{Core}_G(G_h)$. It follows that the stem field of $x^2 - d_g$ corresponds to the unique subgroup H_g of G of index two (up to conjugation) that contains $\mathrm{Core}_G(G_g)$. Similarly the stem field of $x^2 - d_h$ corresponds to the unique subgroup H_h of G of index two that contains $\mathrm{Core}_G(G_h)$. Thus $d_f \cdot d_g$ is a perfect square if and only if $H_f = H_g$. Likewise $d_f \cdot d_h$ is a perfect square if and only if $H_f = H_h$. Direct computation shows that $H_f = H_g$ precisely when G is either S_3 or S_4^-, and $H_f = H_h$ precisely when G is either S_3, D_6, $C_3 \times S_3$, or $S_3 \times S_3$. □

In Table 4.1, we summarize the information presented in Propositions 2.1 and 4.1. This table forms the basis for our algorithm for computing the Galois group of a solvable sextic polynomial. Note that if K/F contains a cubic subfield defined by the polynomial $g(x)$, then the Galois group of g is C_3 if and only if the discriminant of g is a perfect square; otherwise the Galois group is S_3.

Algorithm 4.2 (Galois groups of solvable sextic polynomials)**.** *Let F be a field, $f(x) \in F[x]$ an irreducible sextic polynomial, K/F the stem field of f, and G the Galois group of f over F. Assume G is solvable. Thus K/F has either a quadratic subfield or a cubic subfield or both. Let $g(x)$ be a polynomial defining the cubic subfield of K/F (if it exists), and $h(x)$ a polynomial defining the quadratic subfield of K/F (if it exists). Let m denote the size of the automorphism group of K/F. Let d_f, d_g, and d_h denote the discriminants of f, g, and h, respectively (when they exist). This algorithm returns the Galois group of $f(x)$.*

```
(1) If $m = 6$, then
    (a) If $d_g$ is a perfect square, return $C_6$ and terminate.
    (b) Otherwise return $S_3$ and terminate.
(2) Else if $m = 3$, return $C_3 \times S_3$ and terminate.
```

TABLE 4.1. Invariant data for solvable transitive subgroups of S_6. Column **Aut** gives the size of the centralizer of the group in S_6. Column **GalSubs** is the same as Table 2.2. The remaining columns give discriminant data as described in Proposition 4.1. A blank cell indicates no subfields of that degree.

T	Name	Aut	GalSubs	$\mathbf{d_f} = \square$	$\mathbf{d_f d_g} = \square$	$\mathbf{d_f d_h} = \square$
1	C_6	6	C_2, C_3	no	no	yes
2	S_3	6	C_2, S_3	no	yes	yes
3	D_6	2	C_2, S_3	no	no	yes
4	A_4	2	C_3	yes	yes	
5	$C_3 \times S_3$	3	C_2	no		yes
6	$C_2 \times A_4$	2	C_3	no	no	
7	S_4^+	2	S_3	yes	no	
8	S_4^-	2	S_3	no	yes	
9	$S_3 \times S_3$	1	C_2	no		yes
10	$E_9 \rtimes C_4$	1	C_2	yes		no
11	$C_2 \times S_4$	2	S_3	no	no	
13	$E_9 \rtimes D_4$	1	C_2	no		no

(3) *Else if $m = 2$, then*
   - (a) *If K/F has both a quadratic and a cubic subfield, return D_6 and terminate.*
   - (b) *If d_g is a perfect square, then*
     - (i) *If d_f is a perfect square, return A_4 and terminate.*
     - (ii) *Otherwise return $C_2 \times A_4$ and terminate.*
   - (c) *If d_g is not a perfect square but d_f is, return S_4^+ and terminate.*
   - (d) *Otherwise, if both d_f and d_g are not perfect square, then*
     - (i) *If $d_f \cdot d_g$ is a perfect square, return S_4^- and terminate.*
     - (ii) *Otherwise return $C_2 \times S_4$ and terminate.*

(4) *Else if $m = 1$, then*
   - (a) *If d_f is a perfect square, return $E_9 \rtimes C_4$ and terminate.*
   - (b) *Otherwise if d_f is not a perfect square, then*
     - (i) *If $d_f \cdot d_h$ is a perfect square, return $S_3 \times S_3$ and terminate.*
     - (ii) *Otherwise return $E_9 \rtimes D_4$ and terminate.*

An Example

For example, consider the polynomial $f(x) = x^6 - x^5 - x^3 - x + 1$ defined over the rational numbers. Using Magma or Pari/GP, we see that the stem field of f has two automorphisms and one cubic subfield defined by the polynomial $g(x) = x^3 - 7x^2 + 13x - 5$. The discriminant of g is $d_g = 2^2 \cdot 37$, which is not a perfect square. The discriminant of f is $d_f = 2^4 \cdot 5 \cdot 37^2$, which is also not a perfect square. It follows that the product of the discriminants of f and g is $d_f d_g = 2^6 \cdot 5 \cdot 37^3$, which is not a perfect square either. Algorithm 4.2 thus shows that the Galois group of f is $C_2 \times S_4$.

Another Example

For our final example, consider the polynomial $f(x) = x^6 - 3x^5 + 4x^4 - x^3 + x^2 - 2x + 7$ defined over the rational numbers. We see that the stem field of f has only the identity automorphism and one quadratic subfield defined by $h(x) = x^2 + 5x + 7$. The discriminant of f is $d_f = -3^3 \cdot 29^2 \cdot 107^2$, which is not a perfect square. The product of the discriminants of f and h is $d_f d_h = 3^4 \cdot 29^2 \cdot 107^2$, which is a perfect square. Algorithm 4.2 shows that the Galois group of f is $S_3 \times S_3$.

References

(2013). *PARI/GP – Computational Number Theory, version 2.5.3*. PARI Group, The. available from `http://pari.math.u-bordeaux.fr/`.

Awtrey, C., Mistry, N., and Soltz, N. (2015). Centralizers of transitive permutation groups and applications to Galois theory. *Missouri J. Math. Sci.*, 27(1):16–32.

Bosma, W., Cannon, J., and Playoust, C. (1997). The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265. Computational algebra and number theory (London, 1993).

Butler, G. and McKay, J. (1983). The transitive groups of degree up to eleven. *Comm. Algebra*, 11(8):863–911.

Cohen, H. (1993). *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin.

Elsenhans, A.-S. (2017). Improved methods for the construction of relative invariants for permutation groups. *J. Symbolic Comput.*, 79(part 2):211–231.

Fieker, C. and Klüners, J. (2014). Computation of Galois groups of rational polynomials. *LMS J. Comput. Math.*, 17(1):141–158.

GAP (2013). *GAP – Groups, Algorithms, and Programming, Version 4.6.5*. The GAP Group.

Soicher, L. (1981). The computation of Galois groups. Master's thesis, Concordia University, Montreal.

Soicher, L. and McKay, J. (1985). Computing Galois groups over the rationals. *J. Number Theory*, 20(3):273–281.

Stauduhar, R. P. (1973). The determination of Galois groups. *Math. Comp.*, 27:981–996.

van der Waerden, B. L. (1991). *Algebra. Vol. I.* Springer-Verlag, New York. Based in part on lectures by E. Artin and E. Noether, Translated from the seventh German edition by Fred Blum and John R. Schulenberger.

van Hoeij, M., Klüners, J., and Novocin, A. (2013). Generating subfields. *J. Symbolic Comput.*, 52:17–34.

Wielandt, H. (1964). *Finite permutation groups*. Translated from the German by R. Bercov. Academic Press, New York-London.

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

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