The Minnesota Journal of Undergraduate Mathematics

Irreducible sextic polynomials and their absolute resolvents

Chad Awtrey[1], Robin French[2], Peter Jakes[1], and Alan Russell[1]

[1]Elon University, Elon, NC
[2]Williams High School, Burlington, NC

The Minnesota Journal of Undergraduate Mathematics

Volume 1 Number 1 (2015)

Sponsored by
School of Mathematics
University of Minnesota
Minneapolis, MN 55455

The Minnesota Journal of Undergraduate Mathematics

Volume 1 Number 1 (2015)

Irreducible sextic polynomials and their absolute resolvents

Chad Awtrey[1], Robin French[2], Peter Jakes* [1], and Alan Russell[1]

[1]Elon University, Elon, NC
[2]Williams High School, Burlington, NC

Abstract. We describe two new algorithms for determining the Galois group of an irreducible polynomial of degree six defined over the rational numbers. Both approaches are based on the absolute resolvent method, which involves analyzing polynomials defining subfields of the original polynomial's splitting field. Compared to the traditional algorithm for degree six Galois groups due to Cohen, our methods can be considered improvements since one uses fewer resolvents and the other uses lower degree resolvents.

1. Introduction

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

(1) the polynomial's coefficients

(2) the four basic arithmetic operations $(+,-,\times,\div)$

(3) radicals (square roots, cube roots, etc.)

In the 16th century, Italian mathematicians proved that cubic and quartic polynomials are also solvable by radicals. However the same is not true for polynomials of degree five and higher, a fact first proved in the 19th century. But 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 showed that 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.

* *Corresponding author*

Therefore, an important 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 $n!$ (cf. [12, p.189]). Methods that are more computationally feasible are clearly needed.

Most modern implementations make extensive use of resolvent polynomials. These are polynomials that define subfields of the original polynomial's splitting field (see [11]). 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 have a certain structure ahead of time.

This paper employs absolute resolvents to study Galois groups of degree six polynomials. Note, the traditional approach for degree six polynomials, due to Cohen [4], also uses absolute resolvents. Following previous research on quartic and quintic polynomials ([1, 2]), we analyze all possible resolvents for degree six polynomials. Our work results in two new algorithms for computing the Galois group of an irreducible degree six polynomial defined over the rational numbers that are more efficient than Cohen's.

One algorithm is based on Cohen's method, but removes the need to factor a degree 10 resolvent. Instead we count quadratic subfields of the polynomial's stem field; note that computing subfields is a straightforward task (see [13]). Our second algorithm uses a single degree 30 resolvent along with the discriminant of the original polynomial. We also prove that unlike the case for quartic and quintic polynomials, there is no single absolute resolvent the degrees of whose irreducible factors completely determine the Galois group of irreducible degree six polynomials. Therefore, our algorithm that uses two resolvents is the best possible scenario.

The remainder of the paper is organized as follows. In Section 2 we provide a brief introduction to Galois theory along with an explicit computation, not using resolvents, of the Galois group of a degree six polynomial. In Section 3 we give an introduction to resolvent polynomials, including a discussion of the most widely-used resolvent; namely, the discriminant. Section 4 gives the details of Cohen's algorithm as well as our modification of his algorithm. In the final section, we discuss our new approach that uses two resolvents to determine the Galois group, and we prove there is no way to use only the degrees of the irreducible factors of a single resolvent to compute the Galois group of an irreducible degree six polynomial.

2. Overview of Galois Theory

In this section, we give a very brief overview of Galois theory in our context. More details can be found in any standard text on abstract algebra (such as [5]).

Let $f(x)$ be an irreducible degree n polynomial defined over the rational numbers $\mathbb{Q}$. Let ρ be a root of f in the complex numbers $\mathbb{C}$. Let F be the n-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \rho, \ldots, \rho^{n-1}\}$. Since f is irreducible, F is a field, called the **stem field** of

Table 1. Roots of the polynomial $f(x) = x^6 + 3$ expressed as linear combinations of powers of one root ρ. Also included are the corresponding elements of the automorphism group of f's stem field as permutations of the roots.

Root	Linear Combination	Automorphism	Cycle
1	$-\rho$	$\sigma_1(\rho) = -\rho$	$\sigma_1 = (12)(34)(56)$
2	ρ	$\sigma_2(\rho) = \rho$	$\sigma_2 = \mathrm{id}$
3	$(-\rho^4 - \rho)/2$	$\sigma_3(\rho) = (-\rho^4 - \rho)/2$	$\sigma_3 = (164)(235)$
4	$(-\rho^4 + \rho)/2$	$\sigma_4(\rho) = (-\rho^4 + \rho)/2$	$\sigma_4 = (15)(24)(36)$
5	$(\rho^4 - \rho)/2$	$\sigma_5(\rho) = (\rho^4 - \rho)/2$	$\sigma_5 = (146)(253)$
6	$(\rho^4 + \rho)/2$	$\sigma_6(\rho) = (\rho^4 + \rho)/2$	$\sigma_6 = (13)(26)(45)$

f. We say F is a **degree** n extension of $\mathbb{Q}$. Furthermore, F is the smallest subfield of the complex numbers $\mathbb{C}$ that contains ρ and $\mathbb{Q}$.

Arithmetic in F can be accomplished via polynomial remainders and GCD (greatest common divisor) computations. In particular, let $b = b_0 + b_1\rho + \cdots + b_{n-1}\rho^{n-1}$ and $c = c_0 + c_1\rho + \cdots + c_{n-1}\rho^{n-1}$ be any two elements in F. Let $B(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ and $C(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, so that $b = B(\rho)$ and $c = C(\rho)$. We can identify the product bc as a element of F by using the Division Algorithm to compute polynomials $Q(x)$ and $R(x)$ such that $B(x)C(x) = f(x)Q(x)+R(x)$ where $0 \le \mathrm{degree}(R) < n$. Then $R(\rho)$ is the desired representation of bc in F. Similarly, suppose $b \neq 0$, which is equivalent to $\gcd(B(x), f(x)) = 1$. We can identify $1/b$ as an element of F by using the Euclidean Algorithm to compute polynomials $U(x)$ and $V(x)$ such that $U(x)B(x) + f(x)V(x) = 1$. In this case, $1/b = U(\rho)$.

The **automorphisms** $\mathrm{Aut}(F)$ of F are the collection of all field isomorphisms $\sigma : F \to F$ such that σ **fixes** $\mathbb{Q}$; that is, $\sigma(a) = a$ for all $a \in \mathbb{Q}$. Under the operation of function composition, $\mathrm{Aut}(F)$ forms a group. Since F is generated by powers of ρ, it follows that each $\sigma \in \mathrm{Aut}(F)$ is completely determined by where it sends ρ. Furthermore, each such σ must send ρ to a root of f that is contained in F.

Therefore, elements in $\mathrm{Aut}(F)$ correspond precisely with the roots of f that are contained in F, and each automorphism permutes the roots of f. In the case where F contains all n roots of f, $\mathrm{Aut}(F)$ is called the **Galois group** of f. Otherwise, the Galois group of f is the automorphism group of the **splitting field** of f; that is, the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$ and all n roots of f.

Example 2.1. For example, let $f(x) = x^6 + 3$, ρ a root of f, and F the stem field of f (with powers of ρ as a basis). We can determine how many roots of f are contained in its stem field by factoring f over F and searching for linear factors; the root of each linear factor is a root of f in F. Note that many computer algebra systems are capable of such a factorization (e.g., [9]). In this case, we find that F contains all six roots of f. Thus $\mathrm{Aut}(F)$ contains six elements, each sends ρ to one of the other six roots. Since F contains all roots of f, $\mathrm{Aut}(F)$ is the Galois group of f. In Table 1, we list all the roots (labeled **1** – **6**) and all the automorphisms (labeled $\sigma_1 - \sigma_6$).

Since we have labeled the roots, we can identify $\mathrm{Aut}(F)$ as subgroup of S_6; i.e., as a permutation group. The element σ_2 acts as the identity, since it sends ρ to itself. The element

σ_1 sends root **2** to **1**, and vice versa. To see where σ_1 sends root **3**, recall that each automorphism acts trivially on $\mathbb{Q}$. Thus we have

$$\begin{aligned}\sigma_1(\mathbf{3}) &= \sigma_1((-\rho^4-\rho)/2)\\ &= (-\sigma_1(\rho)^4-\sigma_1(\rho))/2\\ &= (-(-\rho)^4-(-\rho))/2\\ &= (-\rho^4+\rho)/2\\ &= \mathbf{4}\end{aligned}$$

So σ_1 sends root **3** to root **4**. Similary, σ_1 sends root **4** to root **3**, root **5** to root **6**, and root **6** to root **5**. In cycle notation, we have $\sigma_1 = (12)(34)(56)$.

Each of the previous computations is straightforward. However, occasionally it is necessary to use polynomial long division to determine how an automorphism permutes the roots. For example, suppose we wish to determine where σ_3 sends root **6**. As before, we have

$$\begin{aligned}\sigma_3(\mathbf{6}) &= \sigma_3((\rho^4+\rho)/2)\\ &= (\sigma_3(\rho)^4+\sigma_3(\rho))/2\\ &= (((-\rho^4-\rho)/2)^4+(-\rho^4-\rho)/2)/2\\ &= \rho^{16}/32+\rho^{13}/8+3\rho^{10}/16+\rho^7/8-7\rho^4/32-\rho/4\end{aligned}$$

The remainder of this quantity when divided by $f(\rho) = \rho^6+3$ is:

$$\begin{aligned}&= (-\rho^4+\rho)/2\\ &= \mathbf{4}\end{aligned}$$

So σ_3 sends root **6** to root **4**. Table 1 lists the cycle notations for each of the six permutations. Notice that the Galois group of f has six elements: the identity, two elements of order 3, and three elements of order 2. This proves that the Galois group of f is isomorphic to S_3 the symmetric group of order 6.

We note that the Galois group of $f(x) = x^6+3$ was relatively straightforward to compute, precisely because the stem field of f and the splitting field of f were equal. This is not always the case. For example, the stem field of $g(x) = x^6+2x+2$ contains only one root of g, which can be verified by factoring $g(x)$ over its stem field and searching for linear factors. However, as we show later in Section 4, the Galois group of $g(x)$ is S_6. This means the splitting field of $g(x)$ has degree $6! = 720$. Therefore, the approach to compute Galois groups taken above would be significantly more computationally expensive. The use of absolute resolvents is one way to improve this.

The Fundamental Theorem. As we have seen, we can attach two structures to an irreducible polynomial: (1) its splitting field and (2) its Galois group. But more is true, as the Fundamental Theorem of Galois Theory states. Theorem 2.2 contains a statement of the Fundamental Theorem in our context, along with several properties of the Galois correspondence. For proofs, see [5].

TABLE 2. The 16 conjugacy classes of transitive subgroups of S_6. Generators are for one representative in each conjugacy class.

T	Name	Generators	Size
1	C_6	(12)(34)(56), (135)(246)	6
2	S_3	(123)(456), (14)(26)(35)	6
3	D_6	(12)(34)(56), (135)(246), (35)(46)	12
4	A_4	(34)(56), (12)(56), (135)(246)	12
5	$C_3 \times S_3$	(456), (123), (14)(25)(36)	18
6	$C_2 \times A_4$	(56), (34), (12), (135)(246)	24
7	S_4^+	(34)(56), (12)(56), (135)(246), (35)(46)	24
8	S_4^-	(34)(56), (12)(56), (135)(246), (3546)	24
9	$S_3 \times S_3$	(456), (123), (23)(56), (14)(25)(36)	36
10	$E_9 \rtimes C_4$	(456), (123), (23)(56), (14)(2536)	36
11	$C_2 \times S_4$	(56), (34), (12), (145)(236), (35)(46)	48
12	A_5	(12346), (14)(56)	60
13	$E_9 \rtimes D_4$	(465), (45), (123), (23), (14)(25)(36)	72
14	S_5	(15364), (16)(24), (3465)	120
15	A_6	(12345), (456)	360
16	S_6	(123456), (12)	720

Theorem 2.2 (Fundamental Theorem of Galois Theory). *Let K be the splitting field of an irreducible polynomial f of degree n defined over the rational numbers, and let G be the Galois group of f. There is a bijective correspondence between the subfields of K and the subgroups of G. Specifically, if F is a subfield of K, then F corresponds to the set of all $\sigma \in G$ such that $\sigma(a) = a$ for all $a \in F$. Similarly, if H is a subgroup of G, then H corresponds to the set of all $a \in K$ such that $\sigma(a) = a$ for all $\sigma \in H$.*

The Galois correspondence has the following properties (among others).

(1) *If H_1 and H_2 are subgroups of G that correspond to subfields F_1 and F_2 respectively, then $H_1 \leq H_2$ if and only if $F_2 \subseteq F_1$.*

(2) *If F defines a subfield of K of degree d over $\mathbb{Q}$, then F corresponds to a subgroup $H \leq G$ of index d.*

(3) *Let F be a subfield of K defined by the polynomial g and let $H \leq G$ be subgroup corresponding to F. The splitting field of g corresponds to the largest normal subgroup N of G contained inside H; i.e., the kernel of the permutation representation of G acting on G/H. The Galois group of g is isomorphic to G/N.*

(4) *If we label the roots of f as $\rho_1, \ldots, \rho_n$, then G can be identified with a transitive subgroup of S_n, well-defined up to conjugation.*

(5) *If we label the roots of f as $\rho_1, \ldots, \rho_n$, then the stem field of f (generated by ρ_1) corresponds to G_1, the point stabilizer of 1 inside G.*

Notice that by item (4) above, we must 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 [3]). In Table 2, we give information on the 16 conjugacy classes of transitive subgroups of S_6, including their transitive number (or T-number, as in [6]), generators of

Table 3. The 40 conjugacy classes of intransitive subgroups of S_6. Generators are for one representative in each conjugacy class.

#	Generators	Size
1	id	1
2	(56)	2
3	(12)(34)(56)	2
4	(34)(56)	2
5	(456)	3
6	(123)(456)	3
7	(34)(56), (12)(56)	4
8	(34)(56), (35)(46)	4
9	(34)(56), (12)(3546)	4
10	(34)(56), (12)(35)(46)	4
11	(34)(56), (3546)	4
12	(56), (34)	4
13	(56), (12)(34)	4
14	(23456)	5
15	(456), (56)	6
16	(456), (23)(56)	6
17	(123)(456), (23)(56)	6
18	(56), (234)	6
19	(56), (12)(34), (13)(24)	8
20	(56), (34), (12)	8
21	(56), (34), (12)(35)(46)	8
22	(56), (34), (35)(46)	8
23	(34)(56), (35)(46), (12)(56)	8
24	(34)(56), (3546), (12)(56)	8
25	(56), (12)(34), (1324)	8
26	(456), (123)	9
27	(23456), (36)(45)	10
28	(34)(56), (35)(46), (456)	12
29	(56), (234), (34)	12
30	(34), (56), (35)(46), (12)	16
31	(456), (123), (23)(56)	18
32	(456), (56), (123)	18
33	(23456), (36)(45), (3465)	20
34	(56), (12)(34), (13)(24), (234)	24
35	(34)(56), (35)(46), (456), (12)(56)	24
36	(34)(56), (35)(46), (456), (56)	24
37	(456), (56), (123), (23)	36
38	(56), (12)(34), (13)(24), (234), (34)	48
39	(12345), (345)	60
40	(15432), (243), (45)	120

one representative, their size, 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.

Our study of absolute resolvents also makes use of the 40 conjugacy classes of intransitive subgroups of S_6 as well. Table 3 contains information on these groups, similar in format to Table 2. We also include a numbering system for intransitive groups that we reference later in the paper, but such a numbering system is not standard.

3. The Absolute Resolvent Method

Most modern techniques for computing Galois groups are based on the use of resolvent polynomials [11]. In short, this method works as follows. Let $f(x)$ be an irreducible polynomial (over $\mathbb{Q}$) of degree n, and let G be the Galois group of f. Let G^u be a subgroup of S_n that contains G, and let $H \leq G^u$. We form a resolvent polynomial $R(x)$ whose stem field corresponds to H under the Galois correspondence for G^u. Then as shown in [10], the Galois group of $R(x)$ is isomorphic to the image of the permutation representation of G acting on the cosets G^u/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. As such, one effective approach in the absolute resolvent method is to first compute the orbit sizes of all appropriate actions, enough so that no two transitive subgroups of S_n have the same data. Then the corresponding resolvent polynomials are constructed and factored. Computing the Galois group amounts to simply matching the data from the factored resolvent to its corresponding group's data.

When $G^u = S_n$, $R(x)$ is called an **absolute resolvent**. Otherwise, $R(x)$ is called a **relative resolvent**. Since resolvent polynomials are constructed via subgroups of G^u, it follows that a single absolute resolvent can yield invariant data for *all* transitive subgroups of S_n. This fact was exploited in [1, 2] where the authors showed that the degrees of the irreducible factors of a single absolute resolvent were enough to determine the Galois groups for degree 4 and degree 5 polynomials, respectively. Clearly the same cannot be accomplished with relative resolvents, since there is no proper subgroup of S_n that contains all the transitive subgroups of S_n.

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 [10].

Theorem 3.1. *Let $f(x)$ be an irreducible polynomial of degree n with integer coefficients, K the splitting field of f, and $\rho_1, \ldots, \rho_n$ the complex roots of f. Let $T(x_1, \ldots, x_n)$ be a polynomial with integer coefficients, 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 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 $f(x)$ [4, 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.

Example 3.2 (Discriminant)**.** Perhaps the most well known example of a resolvent polynomial is the discriminant. Recall that the discriminant of a degree n polynomial $f(x)$ is given by

$$\mathrm{disc}(f) = \prod_{1\le i<j\le n}(\rho_i-\rho_j)^2,$$

where ρ_i are the roots of f. In particular, let

$$T = \prod_{1\le i<j\le n}(x_i-x_j).$$

It is well-known that T is stabilized by A_n [5, p.610]. Notice that a complete set of coset representatives of S_n/A_n is $\{\mathrm{id},(12)\}$. Also notice that applying the permutation (12) to the subscripts of T results in $-T$. In this case, we can form the resolvent polynomial $R(x)$ as follows,

$$R(x) = \prod_{\sigma\in S_n/A_n}(x-\sigma(T)) = x^2 - T^2 = x^2 - \mathrm{disc}(f).$$

In particular, this resolvent factors if and only if the discriminant is a perfect square.

4. The Degree 6 Resolvent Method

We now turn our attention to computing the Galois group in the case where the degree of $f(x)$ is six. One efficient approach, detailed in [4, §6.3], employs a degree six resolvent polynomial corresponding to the transitive group T14 $= S_5 \simeq PGL(2,5)$ of S_6, which is itself related to the nontrivial outer automorphism of S_6 [8].

This approach uses the discriminant of f, the degrees of the irreducible factors of the resolvent, as well as the discriminants of all cubic, quartic, and quintic factors of the resolvent. This information is enough to determine the Galois group of f in all but 4 of the 16 cases. For these final cases, the approach taken in [4] is to use the discriminant of f and another resolvent, this one of degree 10 and corresponding to the transitive group T13 $= E_9 \rtimes D_4$ of S_6. For convenience, Table 4 provides coset representatives and multivariable functions T that can be used to compute the degree 6 and the degree 10 resolvents. Table 5 provides a summary of how these resolvents factor.

For example, consider the polynomial $f(x) = x^6 + 2x + 2$. The degree six resolvent $R_6(x)$ for f is:

$$R_6(x) = x^6 - 36x^5 - 540x^4 + 25920x^3 - 3185984x - 6743936,$$

which remains irreducible over $\mathbb{Q}$. Thus the Galois group of f is either T10, T13, T15, or T16, according to Table 5. The discriminant of f is:

$$\mathrm{disc}(f) = -2^6\cdot 89\cdot 227,$$

Table 4. Coset representatives for S_6/H for Cohen's degree 6 and degree 10 resolvent polynomials. This corresponds to transitive groups T14 = S_5 and T13 = $E_9 \rtimes D_4$, respectively (see Table 2). Also included are multivariable functions T that are stabilized by each H.

	$\mathbf{T14 = S_5}$	$\mathbf{T13 = E_9 \rtimes D_4}$
Coset Reps	id, (5,6), (4,5), (3,5), (3,4), (4,6)	id, (5,6), (4,5), (3,4) (3,4)(5,6), (3,5,6,4) (2,3), (2,3)(5,6) (2,3)(4,5), (2,4,5,3)
T	$x_6x_3x_1^2x_2^2 + x_5x_4x_1^2x_2^2 + x_5x_2x_1^2x_3^2$ $+x_3x_2x_1^2x_4^2 + x_4x_2x_1^2x_6^2 + x_6x_2x_1^2x_5^2$ $+x_6x_4x_1^2x_3^2 + x_5^2x_4x_3x_1^2 + x_6^2x_5x_3x_1^2$ $+x_6x_5x_1^2x_4^2 + x_4x_3^2x_1x_2^2 + x_5^2x_3x_1x_2^2$ $+x_6x_4^2x_1x_2^2 + x_6^2x_5x_1x_2^2 + x_6^2x_3^2x_1x_2$ $+x_5^2x_4^2x_1x_2 + x_5x_4^2x_1x_3^2 + x_6x_5^2x_1x_3^2$ $+x_6^2x_4^2x_1x_3 + x_6^2x_5^2x_1x_4 + x_6x_5x_2^2x_3^2$ $+x_5x_4^2x_3x_2^2 + x_6^2x_4x_3x_2^2 + x_6x_5^2x_4x_2^2$ $+x_6x_4^2x_2x_3^2 + x_5^2x_4x_2x_3^2 + x_6^2x_5^2x_2x_3$ $+x_6^2x_5x_2x_4^2 + x_6^2x_5x_4x_3^2 + x_6x_5^2x_3x_4^2$	$(x_1+x_3+x_5)^2$ $+(x_2+x_4+x_6)^2$

which is clearly not a square in $\mathbb{Q}$. Thus the Galois group is either T13 or T16. Finally, the degree 10 resolvent $R_{10}(x)$ for f is:

$$R_{10}(x) = x^{10} + 1056x^7 - 15744x^5 + 33024x^4 + 135168x^2 + 262144x + 16384,$$

which remains irreducible over $\mathbb{Q}$. Therefore, the Galois group is T16 = S_6. This proves the splitting field of f forms a degree 720 extension over $\mathbb{Q}$.

Alternative Approach: Quadratic Subfields. As an alternative to constructing and factoring the degree 10 resolvent used in Cohen's method, we propose instead to compute quadratic subfields of the stem field of f. There exist efficient algorithms for accomplishing this (cf. [13]). In Proposition 4.1, we show that the number of quadratic subfields of a polynomial's stem field is an invariant of its Galois group.

Proposition 4.1. *Let $f(x)$ be an irreducible polynomial of degree n, F the stem field of f, and G the Galois group of f. The number of nonisomorphic quadratic subfields of F is an invariant of G. That is, if $g(x)$ is any other irreducible polynomial of degree n with Galois group G and stem field K, then the number of nonisomorphic quadratic subfields of K is the same as for F.*

Proof. Let $f(x)$ be an irreducible polynomial of degree n and let $\rho_1, \ldots, \rho_n$ be the complex roots of f. Let F be the stem field of f generated by ρ_1 and let G be the Galois group of f. Then under the Galois correspondence, F corresponds to G_1, the point stabilizer of 1 in G. Therefore, the nonisomorphic quadratic subfields of F corresponds to conjugacy classes of subgroups H of G that contain G_1. Thus the number of such quadratic subfields is completely determined by a subgroup computation inside G, proving the result. □

For each of the 16 transitive subgroups of S_6, the column **Quad** in Table 5 indicates whether there exists a subgroup H such that $G_1 \leq H \leq G$, where G_1 is the point stabilizer of 1 in G.

TABLE 5. A summary of Cohen's method [4] and a new method for computing the Galois group of an irreducible degree six polynomial $f(x)$. The column **D6** gives the degrees of the irreducible factors of the resolvent polynomial corresponding to the transitive subgroup T14 of S_6. The superscripts on the factors of degree 3–5 correspond to whether the factor's polynomial discriminant is a square (+) or isn't (−). The column **Disc** indicates whether the discriminant of f is a square (+) or not (−). The Column **D10** gives the degrees of the irreducible factor of the resolvent polynomial corresponding to the transitive subgroup T13 of S_6. The final column indicates whether f's stem field has a quadratic subfield or not.

T	D6	Disc	D10	Quad
T1	$1,2,3^+$	−	$1,3,6$	Y
T2	$1,1,1,3^-$	−	$1,3,3,3$	Y
T3	$1,2,3^-$	−	$1,3,6$	Y
T4	$1,1,4^+$	+	$4,6$	N
T5	$3^+,3^-$	−	$1,9$	Y
T6	$2,4^+$	−	$4,6$	N
T7	$2,4^+$	+	$4,6$	N
T8	$1,1,4-$	−	$4,6$	N
T9	$3^-,3^-$	−	$1,9$	Y
T10	6	+	$1,9$	Y
T11	$2,4^-$	−	$4,6$	N
T12	$1,5^+$	+	10	N
T13	6	−	$1,9$	Y
T14	$1,5^-$	−	10	N
T15	6	+	10	N
T16	6	−	10	N

For example, let $f(x) = x^6 - x^5 + x^4 - x^3 - 4x^2 + 5$. The degree six resolvent, $R_6(x)$ for f is:

$$R_6(x) = x^6 - 82x^5 - 4255x^4 + 362235x^3 + 3935805x^2 - 353299137x + 3563797189,$$

which remains irreducible over $\mathbb{Q}$. As before, the Galois group of f is either T10, T13, T15, or T16. The discriminant of f is:

$$\mathrm{disc}(f) = 5^4 \cdot 29^2,$$

which is a square in $\mathbb{Q}$. Thus the Galois group is either T10 or T15. Finally, using [9] we find that the stem field of f does have a quadratic subfield defined by the polynomial $g(x) = x^2 - 5x + 5$. In fact, if F is the stem field of f generated by a root ρ of f, then $g(x)$ factors over F as follows:

$$g(x) = (x - \alpha)(x + \alpha - 5),$$

where $\alpha = 3\rho^5 + \rho^4 + 4\rho^3 + 2\rho^2 - 9\rho - 10$. The conclusion is that the Galois group of f is $\mathrm{T10} = E_9 \rtimes C_4$.

We note that other authors have also used alternative approaches to Cohen's method. For example, the approach taken in [7] is to use a degree 15 resolvent (corresponding to the transitive group $\mathrm{T11} = C_2 \times S_4$) instead of the degree 6 resolvent used by Cohen. The author also uses the discriminant and the same degree 10 resolvent Cohen uses. Still in this case, it is necessary to use additional resolvents to distinguish half of the groups. So both Cohen's method and our modification are more efficient than this one.

5. The Degree 30 Resolvent Method

As stated in Theorem 3.1, we can use information on how resolvent polynomials factor to determine the Galois group of a degree six polynomial. Cohen's approach, described in the last section, utilizes three resolvents as well as the discriminant of the factors of one of the resolvents. In this section, we develop an algorithm that uses only one resolvent and the discriminant of the original polynomial. Our final result shows that it is not possible to use the degrees of the irreducible factors of a single resolvent polynomial to determine the Galois group; i.e., at least two resolvent polynomials are required. This is unlike the case for quartic and quintic polynomial, as shown in [1,2].

All Possible Resolvent Factorizations. Given a transitive subgroup G of S_6, our first step is to determine the factorizations of all possible resolvents arising from a degree 6 polynomial $f(x)$ whose Galois group is G. The function `resfactors` below will perform such a task. Written for the program GAP [6], the function `resfactors` takes as input a subgroup H of S_6 and a transitive subgroup G of S_6. It computes the image of the permutation representation of G acting on the cosets S_6/H, and then it outputs the lengths of the orbits of this action. By Theorem 3.1, the output of the function `resfactors` is precisely the list of degrees of the irreducible factors of the resolvent polynomial $R(x)$ corresponding to the subgroup H.

```
resfactors := function(h, g)
  local s6, cosets, index, permrep, orb, orbs;
    s6        := SymmetricGroup(6);
    cosets    := RightCosets(s6,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;
```

Table 6 shows for each conjugacy class of transitive subgroups of S_6 the degrees of the irreducible factors of the corresponding resolvent polynomial according to the Galois group of f. Tables 7–9 do the same thing for intransitive subgroups. Note, the multiplicity of each degree is listed as an exponent. For example, the entry $1^2, 2^2, 3^2, 6^{18}$ means the resolvent factors as two linears times two quadratics times two cubics times 18 sextics.

The Degree 30 Resolvent Algorithm. We can use the information in the tables to develop algorithms for computing Galois groups of irreducible degree six polynomials. In

Table 6. The top row contains the transitive subgroups H of S_6. The left column also contains transitive subgroups G of S_6. For a particular pair (H,G), the entry in the table gives the output of the function `resfactors(H,G)`.

	T1	T2	T3	T4	T5	T6
T1	$1^2,2^2,3^2,6^{18}$	$2^3,3^8,6^{15}$	$1,2,3^5,6^7$	$2^6,6^8$	$1^2,2,3^2,6^5$	$1^2,2^2,6^4$
T2	$2^3,3^8,6^{15}$	$1^6,3^{18},6^{10}$	$1^3,3^{13},6^3$	$2^6,6^8$	$1^2,2,3^6,6^3$	$2^3,3^2,6^3$
T3	$2,4,6^5,12^7$	$2^3,6^{13},12^3$	$1,2,3^3,6^6,12$	$4^3,6^2,12^3$	$2^2,6^4,12$	$2,4,6^2,12$
T4	$4^6,12^8$	$4^6,12^8$	$4^3,6^2,12^3$	$1^4,4^8,12^2$	$4^4,12^2$	$1^2,4^4,12$
T5	$3^2,6,9^2,18^5$	$3^2,6,9^6,18^3$	$3^2,9^4,18$	$6^4,18^2$	$1^2,2^2,9,18$	$3^2,6,18$
T6	$4^2,8^2,24^4$	$8^3,12^2,24^3$	$4,8,12^2,24$	$2^2,8^4,24$	$4^2,8,24$	$1^2,8^2,12$
T7	$8^3,24^4$	$8^3,24^4$	$4,8,12^2,24$	$2^2,8^4,12^2$	$8^2,24$	$2,8^2,12$
T8	$8^3,12^4,24^2$	$4^6,12^6,24$	$4^3,6^2,12^3$	$2^2,8^4,24$	$4^2,8,12^2$	$2,8^2,12$
T9	$6^2,18^2,36^2$	$6^2,18^6$	$3^2,9^2,18^2$	$12^2,18^2$	$2^2,18^2$	$6^2,18$
T10	$12,36^3$	$12,36^3$	$6,18,36$	$12^2,18^2$	$4,36$	$12,18$
T11	$8,16,24^2,48$	$8^3,24^4$	$4,8,12^2,24$	$4,16^2,24$	$8^2,24$	$2,12,16$
T12	$20^3,60$	$20^3,60$	$10,20,30$	$5^4,20^2$	20^2	$5^2,20$
T13	$12,36,72$	$12,36^3$	$6,18,36$	$24,36$	$4,36$	$12,18$
T14	$20,40,60$	$20^3,60$	$10,20,30$	$10^2,40$	20^2	$10,20$
T15	120	120	60	30^2	40	30
T16	120	120	60	60	40	30

	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16
T1	$2^3,6^4$	$2^3,3^4,6^2$	$1^2,3^2,6^2$	$2,6^3$	$1,2,3^2,6$	$2^3,6$	$1,3,6$	$1,2,3$	2	1
T2	$2^3,6^4$	$1^6,3^6,6$	$1^2,3^6$	$2,6^3$	$1^3,3^4$	$2^3,6$	$1,3^3$	$1^3,3$	2	1
T3	$2,4,6^2,12$	$2^3,3^2,6^3$	$1^2,3^2,6^2$	$2,6,12$	$1,2,3^2,6$	$2,4,6$	$1,3,6$	$1,2,3$	2	1
T4	$1^2,4^4,6^2$	$1^2,4^4,12$	$4^2,6^2$	$4^2,6^2$	$1,4^2,6$	$1^4,4^2$	$4,6$	$1^2,4$	1^2	1
T5	$6^2,18$	$3^2,6,9^2$	$1^2,9^2$	$2,18$	$3^2,9$	6^2	$1,9$	3^2	2	1
T6	$2,8^2,12$	$2,8^2,2$	$4^2,12$	$8,12$	$1,6,8$	$2^2,8$	$4,6$	$2,4$	2	1
T7	$1^2,6^2,8^2$	$2,8^2,12$	$4^2,12$	$4^2,6^2$	$1,6,8$	$2^2,4^2$	$4,6$	$2,4$	1^2	1
T8	$2,8^2,12$	$1^2,4^4,12$	$4^2,6^2$	$8,12$	$1,4^2,6$	$2^2,8$	$4,6$	$1^1,4$	2	1
T9	$6^2,18$	$6^2,9^2$	$1^2,9^2$	$2,18$	$3^2,9$	6^2	$1,9$	3^2	2	1
T10	$6^2,9^2$	$12,18$	$2,18$	$1^2,9^2$	$6,9$	6^2	$1,9$	6	1^2	1
T11	$2,12,16$	$2,8^2,12$	$4^2,12$	$8,12$	$1,6,8$	$4,8$	$4,6$	$2,4$	2	1
T12	$5^2,10^2$	$5^2,20$	10^2	10^2	$5,10$	$1^2,5^2$	10	$1,5$	1^2	1
T13	$12,18$	$12,18$	$2,18$	$2,18$	$6,9$	12	$1,9$	6	2	1
T14	$10,20$	$5^2,20$	10^2	20	$5,10$	$2,10$	10	$1,5$	2	1
T15	15^2	30	20	10^2	15	6^2	10	6	1^2	1
T16	30	30	20	20	15	12	10	6	2	1

particular, we will use the discriminant of the polynomial as well as the degree 30 resolvent corresponding to the transitive group T6 $= C_2 \times A_4$. Here is a method to construct this degree 30 resolvent.

A complete set of right coset representatives for S_6/T6 is:

> (1), (56), (45), (456), (465), (46), (34), (34)(56), (345), (3465), (354), (35), (23), (23)(56), (23)(45), (23)(456), (23)(465), (23)(46), (234), (234)(56), (2354), (243), (243)(56), (24563), (2463), (24), (24)(56), (25643), (2563), (2564).

TABLE 7. Similar to Table 6, except columns correspond to intransitive subgroups of S_6.

	I1	I2	I3	I4	I5	I6	I7	I8
T1	6^{120}	6^{60}	$3^8,6^{56}$	6^{60}	6^{40}	$2^6,6^{38}$	6^{30}	6^{30}
T2	6^{120}	6^{60}	$3^{24},6^{48}$	6^{60}	6^{40}	$2^6,6^{38}$	6^{30}	6^{30}
T3	12^{60}	12^{30}	$6^{16},12^{22}$	$6^4,12^{28}$	12^{20}	$4^3,12^{19}$	$6^6,12^{12}$	$6^6,12^{12}$
T4	12^{60}	12^{30}	12^{30}	$6^4,12^{28}$	12^{20}	$4^{12},12^{16}$	$3^4,12^{14}$	$6^6,12^{12}$
T5	18^{40}	18^{20}	$9^8,18^{16}$	18^{20}	$6^4,18^{12}$	$6^4,18^{12}$	18^{10}	18^{10}
T6	24^{30}	$12^6,24^{12}$	$12^2,24^{14}$	$12^2,24^{14}$	24^{10}	$8^6,24^8$	$6^2,24^7$	$12^3,24^6$
T7	24^{30}	24^{15}	24^{15}	$12^6,24^{12}$	24^{10}	$8^6,24^8$	$6^2,12^6,24^4$	$6^6,24^6$
T8	24^{30}	24^{15}	$12^{12},24^9$	$12^2,24^{14}$	24^{10}	$8^6,24^8$	$6^2,24^7$	$12^3,24^6$
T9	36^{20}	36^{10}	$18^8,36^6$	$18^4,36^8$	$12^2,36^6$	$12^2,36^6$	$18^6,36^2$	$18^6,36^2$
T10	36^{20}	36^{10}	36^{10}	$18^4,36^8$	$12^2,36^6$	$12^2,36^6$	$18^6,36^2$	$18^6,36^2$
T11	48^{15}	$24^3,48^6$	$24^7,48^4$	$24^3,48^6$	48^5	$16^3,48^4$	$12,24^3,48^2$	$12^3,48^3$
T12	60^{12}	60^6	60^6	$30^4,60^4$	60^4	$20^6,60^2$	$15^4,60^2$	30^6
T13	72^{10}	$36^4,72^3$	$36^4,72^3$	$36^2,72^4$	$24,72^3$	$24,72^3$	$36^3,72$	$36^3,72$
T14	120^6	120^3	$60^4,120$	$60^2,120^2$	120^2	$40^3,120$	$30^2,120$	60^3
T15	360^2	360	360	180^2	120^2	120^2	90^2	90^2
T16	720	360	360	360	240	240	180	180

	I9	I10	I11	I12	I13	I14	I15
T1	6^{30}	$3^8,6^{26}$	6^{30}	6^{30}	$3^4,6^{28}$	6^{24}	6^{20}
T2	6^{30}	$3^{24},6^{18}$	6^{30}	6^{30}	$3^{12},6^{24}$	6^{24}	6^{20}
T3	$6^2,12^{14}$	$3^4,6^{12},12^8$	$6^2,12^{14}$	$6^2,12^{14}$	$6^{10},12^{10}$	12^{12}	12^{10}
T4	$6^2,12^{14}$	$6^2,12^{14}$	$6^2,12^{14}$	$6^2,12^{14}$	$6^2,12^{14}$	12^{12}	12^{10}
T5	18^{10}	$9^8,18^6$	18^{10}	18^{10}	$9^4,18^8$	18^8	$6^2,18^6$
T6	$12,24^7$	$12^3,24^6$	$12,24^7$	$6^2,12^4,24^5$	$6^2,12^2,24^6$	24^7	$12^6,24^2$
T7	$6^2,12^2,24^6$	$12^3,24^6$	$12^3,24^6$	$12^3,24^6$	$12^3,24^6$	24^7	24^5
T8	$12,24^7$	$6^2,12^{10},24^2$	$6^2,24^7$	$12,24^7$	$12^7,24^4$	24^7	24^5
T9	$18^2,36^4$	$9^4,18^4,36^2$	$18^2,36^4$	$18^2,36^4$	$18^6,36^2$	36^4	$12,36^3$
T10	$9^4,36^4$	$18^2,36^4$	$18^2,36^4$	$18^2,36^4$	$18^2,36^4$	36^4	$12,36^3$
T11	$12,24,48^3$	$12^3,24^4,48$	$12,24,48^3$	$12,24^3,48^2$	$12^3,24^2,48^2$	48^3	$24^3,48$
T12	$30^2,60^2$	$30^2,60^2$	$30^2,60^2$	$30^2,60^2$	$30^2,60^2$	$12^2,60^2$	60^2
T13	$18^2,72^2$	$18^2,36^2,72$	$36,72^2$	$18^2,36^2,72$	36^5	72^2	$12,36^3$
T14	$60,120$	$30^2,60^2$	$30^2,120$	$60,120$	60^3	$24,120$	120
T15	90^2	180	180	180	180	72^2	120
T16	180	180	180	180	180	144	120

A form which is stabilized by T6 is

$$T = (x_1 + x_2 - x_3 - x_4)(x_1 + x_2 - x_5 - x_6)(x_3 + x_4 - x_5 - x_6).$$

An algorithm for determining Galois groups of irreducible degree six polynomials based on the discriminant and the degree 30 resolvent proceeds as follows. Letting f denote the degree six polynomial, G its Galois group, d the discriminant of f, and L the list of degrees of the irreducible factors of the degree 30 resolvent corresponding to T6, we have:

(1) If $L = [1,1,2,2,6,6,6,6]$, then $G = C_6$.

(2) If $L = [2,2,2,3,3,6,6,6]$, then $G = S_3$.

TABLE 8. A continuation of Table 7.

	I16	I17	I18	I19	I20	I21	I22
T1	6^{20}	$2^3,6^{19}$	6^{20}	$3^6,6^{12}$	$3^2,6^{14}$	$3^4,6^{13}$	6^{15}
T2	6^{20}	$2^3,6^{19}$	6^{20}	$3^{18},6^6$	$3^6,6^{12}$	$3^{12},6^9$	6^{15}
T3	$6^4,12^8$	$2,4,6^3,12^8$	12^{10}	$3^6,6^6,12^3$	$6^7,12^4$	$3^2,6^6,12^4$	$6^3,12^6$
T4	$6^4,12^8$	$4^6,6^4,12^6$	12^{10}	$6^3,12^6$	$3^2,12^7$	$6,12^7$	$6^3,12^6$
T5	$6^2,18^6$	$6^2,18^6$	$6^2,18^6$	$9^6,18^2$	$9^2,18^4$	$9^4,18^3$	18^5
T6	$12^2,24^4$	$8^3,12^2,24^3$	$12^2,24^4$	$6^3,24^3$	$3^2,12^3,24^2$	$6,12^3,24^2$	$6,12^3,24^2$
T7	$12^6,24^2$	$4^2,8^2,12^4,24^2$	24^5	$6^3,24^3$	$6,12^3,24^2$	$6,12,24^3$	$6^3,24^3$
T8	$12^2,24^4$	$8^3,12^2,24^3$	24^5	$6^3,12^6$	$6,12^3,24^2$	$6,12^5,24$	$6,12,24^3$
T9	$6^2,18^2,36^2$	$6^2,18^2,36^2$	$12,36^3$	$9^6,36$	18^5	$9^2,18^2,36$	$18^3,36$
T10	$6^2,18^2,36^2$	$6^2,18^2,36^2$	$12,36^3$	$18^3,36$	$18^3,36$	$9^2,36^2$	$18^3,36$
T11	$24^3,48$	$8,16,24^2,48$	$24,48^2$	$6^3,24^3$	$6,12^3,48$	$6,12,24^3$	$6,12,24,48$
T12	30^4	$10^2,20^2,30^2$	60^2	30^3	$15^2,60$	$30,60$	30^3
T13	$12,36,72$	$12,36,72$	$12,36,72$	$18^3,36$	$18^3,36$	$9^2,36^2$	$18,36^2$
T14	60^2	$20,40,60$	120	30^3	$30,60$	$30,60$	$30,60$
T15	60^2	60^2	120	90	90	90	90
T16	120	120	120	90	90	90	90

	I23	I24	I25	I26	I27	I28	I29
T1	6^{15}	$3^4,6^{13}$	$3^2,6^{14}$	$2^4,6^{12}$	6^{12}	6^{10}	6^{10}
T2	6^{15}	$3^{12},6^9$	$3^6,6^{12}$	$2^4,6^{12}$	6^{12}	6^{10}	6^{10}
T3	$6^5,12^5$	$3^2,6^8,12^3$	$6^5,12^5$	$4^2,12^6$	$6^4,12^4$	$6^2,12^4$	$6^2,12^4$
T4	$3^2,6^2,12^6$	$3^2,12^7$	$6,12^7$	$4^8,12^4$	$6^4,12^4$	$6^2,12^4$	$6^2,12^4$
T5	18^5	$9^4,18^3$	$9^2,18^4$	$2^4,18^4$	18^4	$6^4,18^2$	$6,18^3$
T6	$6,12,24^3$	$6,12,24^3$	$6,12,24^3$	$8^4,24^2$	$12^2,24^2$	$12,24^2$	$6^2,12^2,24$
T7	$3^2,6^2,12^2,24^2$	$6,12^3,24^2$	$6,12,24^3$	$8^4,24^2$	12^6	$6^2,24^2$	$12^3,24$
T8	$6,12,24^3$	$3^2,12^5,24$	$6,12^3,24^2$	$8^4,24^2$	$12^2,24^2$	$12,24^2$	$12,24^2$
T9	18^5	$9^2,18^4$	$18^3,36$	$4^2,36^2$	18^4	$12^2,18^2$	$6,18,36$
T10	$9^2,18^4$	$18^3,36$	$9^2,36^2$	$4^2,36^2$	18^4	$12^2,18^2$	$6,18,36$
T11	$6,12,24,48$	$6,12,24^3$	$6,12,24,48$	$16^2,48$	24^3	$12,48$	$12,24^2$
T12	$15^2,30^2$	$15^2,60$	$30,60$	20^4	$6^2,30^2$	30^2	30^2
T13	$18,36^2$	$18,36^2$	$18,36^2$	$8,72$	36^2	$24,36$	$6,18,36$
T14	$30,60$	$15^2,60$	$30,60$	40^2	$12,60$	60	60
T15	45^2	90	90	40^2	36^2	30^2	60
T16	90	90	90	80	72	60	60

(3) If $L=[2,4,6,6,12]$, then $G=D_6$.

(4) If $L=[1,1,4,4,4,4,12]$, then $G=A_4$.

(5) If $L=[3,3,6,18]$, then $G=C_3\times S_3$.

(6) If $L=[1,1,8,8,12]$, then $G=C_2\times A_4$.

(7) If $L=[6,6,18]$, then $G=S_3\times S_3$.

(8) If $L=[2,12,16]$, then $G=C_2\times S_4$.

(9) If $L=[5,5,20]$, then $G=A_5$.

(10) If $L=[10,20]$, then $G=S_5$.

TABLE 9. A continuation of Tables 7 and 8.

	I30	I31	I32	I33	I34	I35	I36	I37	I38	I39	I40
T1	$3^3,6^6$	$2^2,6^6$	$2^2,6^6$	6^6	$3^2,6^4$	6^5	6^5	$2,6^3$	$3,6^2$	6^2	6
T2	$3^9,6^3$	$2^2,6^6$	$2^2,6^6$	6^6	$3^6,6^2$	6^5	6^5	$2,6^3$	$3^3,6$	6^2	6
T3	$3^3,6^4,12$	$2^2,6^2,12^2$	$4,12^3$	$6^2,12^2$	$3^2,6^6,12$	$6^3,12$	$6,12^2$	$2,6,12$	$3,6^2$	6^2	6
T4	$3,6,12^3$	$4^4,6^4$	$4^4,12^2$	$6^2,12^2$	$6,12^2$	$3^2,12^2$	$6,12^2$	$4^2,6^2$	$3,12$	6^2	6
T5	$9^3,18$	$2^2,18^2$	$2^2,18^2$	18^2	$6^2,9^2$	$6^2,18$	$6^2,18$	$2,18$	$6,9$	6^2	6
T6	$3,6,12,24$	$8^2,12^2$	$8^2,12^2$	$12,24$	$6,24$	$6,24$	$6,12^2$	$6^2,8$	$3,12$	12	6
T7	$3,6,12,24$	$4^4,12^2$	$8^2,24$	12^3	$6,24$	$3^2,12^2$	$6,24$	$4^2,12$	$3,12$	6^2	6
T8	$3,6,12^3$	$8^2,12^2$	$8^2,24$	$6^2,24$	$6,12^2$	$6,24$	$6,24$	$8,12$	$3,12$	12	6
T9	$9^3,18$	$2^2,18^2$	$4,36$	18^2	$9^2,12$	$6^2,18$	$12,18$	$2,18$	$6,9$	6^2	6
T10	$9,18^2$	$2^2,18^2$	$4,36$	18^2	$12,18$	$6^2,9^2$	$12,18$	$2,18$	$6,9$	6^2	6
T11	$3,6,12,24$	$8^2,24$	$16,24$	$12,24$	$6,24$	$6,24$	$6,24$	$8,12$	$3,12$	12	6
T12	$15,30$	10^4	20^2	$6,30$	30	15^2	30	10^2	15	6^2	6
T13	$9,18^2$	$4,36$	$4,36$	36	$12,18$	$12,18$	$12,18$	$2,18$	$6,9$	12	6
T14	$15,30$	20^2	40	$6,30$	30	30	30	20	15	12	6
T15	45	20^2	40	36	30	15^2	30	20	15	6^2	6
T16	45	40	40	36	30	30	30	20	15	12	6

(11) If $L = [2,8,8,12]$ and d is a square, then $G = S_4^+$.

(12) If $L = [2,8,8,12]$ and d is not a square, then $G = S_4^-$.

(13) If $L = [12,18]$ and d is a square, then $G = E_9 \rtimes C_4$.

(14) If $L = [12,18]$ and d is not a square, then $G = E_9 \rtimes D_4$.

(15) If $L = [30]$ and d is a square, then $G = A_6$.

(16) If $L = [30]$ and d is not a square, then $G = S_6$.

Example 5.1. Here are two examples of our algorithm in action. First, consider the polynomial $f(x) = x^6 + x^4 - 2x^3 + x^2 - x + 1$. The degree 30 resolvent $R_{30}(x) = x^{30} + 1944x^{28} + 574956x^{26} + \cdots$. Over $\mathbb{Q}$, R_{30} factors as:

$$\begin{aligned} R_{30}(x) =&(x^2+23)\times(x^4+1657x^2+70225)\times(x^6+135x^4-1458x^2+19683)\times \\ &(x^6+162x^4+6561x^2-452709)\times(x^{12}-33x^{10}+\cdots+308037601). \end{aligned}$$

The degrees of the irreducible factors are $[2,4,6,6,12]$. Therefore, the Galois group of $f(x)$ is $\mathrm{T}3 = D_6$.

Finally, consider the polynomial $f(x) = x^6 - 3x^5 + 6x^4 - 7x^3 + 2x^2 + x - 1$. The degree 30 resolvent is $R_{30}(x) = x^{30} + 6130272x^{28} + \cdots$. Over $\mathbb{Q}$, R_{30} factors as:

$$\begin{aligned} R_{30}(x) =&(x^2-9472)\times(x^8+2150576x^6+\cdots)\times \\ &(x^8+2775728x^6+\cdots)\times(x^{12}+1213440x^{10}+\cdots). \end{aligned}$$

The degrees of the irreducible factors are $[2,8,8,12]$. Thus the Galois group of f is either $\mathrm{T}7 = S_4^+$ or $\mathrm{T}8 = S_4^-$. The discriminant of f is:

$$\mathrm{disc}(f) = 2^4 \cdot 37^3,$$

which is not a square. So the Galois group of f is T8 = S_4^-.

A Single Resolvent Will Not Work. Our final result shows that it is not possible to use the degrees of the irreducible factors of a single resolvent polynomial to determine the Galois group of a degree six polynomial; i.e., at least two resolvent polynomials are required. Therefore, our algorithm that uses two resolvents minimizes the number of resolvents required to compute the Galois group. Recall that Cohen's approach uses three resolvents (plus discriminants of the sextic resolvent's factors). Moreover, among all methods that completely determine the Galois group using two resolvents, ours minimizes the product of their degrees. The proof involves analyzing the columns of Tables 6 – 9. For example, that no single resolvent suffices follows since every column has at least two entries that are the same (two such entries cannot be distinguished by that particular resolvent).

Corollary 5.2. *Unlike the scenario for polynomials of degree less than or equal to five, there is no single absolute resolvent that can determine the Galois group of a degree six polynomial using the degrees of the resolvent's irreducible factors.*

The Galois group can be determined by two resolvent polynomials, say of degrees d_1 and d_2. The minimum product $d_1 d_2$ is $60 = 2\cdot 30$, and this is achieved using the the resolvents corresponding to the transitive groups $T15 = A_6$ and $T6 = C_2 \times A_4$.

Acknowledgements

This research was supported in part by NSF Grant #DMS-1148695. The authors would like to thank the reviewer for their careful reading and helpful comments that have increased the clarity of the paper. The authors would also like to thank Elon University for supporting this project and the Center for Undergraduate Research in Mathematics for their support.

References

[1] Chad Awtrey, Brett Barkley, Jeremy Guinn, and Mackenzie McCraw. Resolvents, masses, and Galois groups of irreducible quartic polynomials. *Pi Mu Epsilon J.*, 13(10):609–618, 2014.

[2] Chad Awtrey and Christopher R. Shill. Absolute resolvents and masses of irreducible quintic polynomials. In *Collaborative Mathematics and Statistics Research: Topics from the 9th Annual UNCG Regional Mathematics in Statistics Conference*, volume 109 of *Springer Proceedings of Mathematics & Statistics*, pages 31–41. Springer, New York, 2015.

[3] Gregory Butler and John McKay. The transitive groups of degree up to eleven. *Comm. Algebra*, 11(8):863–911, 1983.

[4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[5] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[6] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[7] Thomas R. Hagedorn. General formulas for solving solvable sextic equations. *J. Algebra*, 233(2):704–757, 2000.

[8] T. Y. Lam and David B. Leep. Combinatorial structure on the automorphism group of S_6. *Exposition. Math.*, 11(4):289–308, 1993.

[9] PARI Group, The. *PARI/GP – Computational Number Theory, version 2.3.4*, 2008. available from `http://pari.math.u-bordeaux.fr/`.

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

[11] Richard P. Stauduhar. The determination of Galois groups. *Math. Comp.*, 27:981–996, 1973.

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

[13] Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *J. Symbolic Comput.*, 52:17–34, 2013.

Student biographies

Robin French: Robin graduated from Elon University in North Carolina in May 2015. She is currently employed as a secondary mathematics teacher in North Carolina.

Peter Jakes: (*Corresponding author:* pjakes@elon.edu) Peter is currently a mathematics and statistics double major at Elon University in North Carolina. He plans to attend graduate school after finishing his undergraduate degree.