Canad. Math. Bull. Vol. **63** (3), 2020 pp. 670–676
http://dx.doi.org/10.4153/S0008439519000754

Galois Groups of Even Sextic Polynomials

Chad Awtrey and Peter Jakes

Abstract. Let $f(x) = x^6 + ax^4 + bx^2 + c$ be an irreducible sextic polynomial with coefficients from a field F of characteristic $\neq 2$, and let $g(x) = x^3 + ax^2 + bx + c$. We show how to identify the conjugacy class in S_6 of the Galois group of f over F using only the discriminants of f and g and the reducibility of a related sextic polynomial. We demonstrate that our method is useful for producing one-parameter families of even sextic polynomials with a specified Galois group.

1 Introduction

Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial of degree n. Let L/F denote the splitting field of f in a fixed algebraic closure $\overline{F}$ of F. The following two tasks are of fundamental importance in computational algebra:

T1 Identify the conjugacy class in S_n of the Galois group of f over F.

T2 For each conjugacy class $\mathcal{G}$ of transitive subgroups of S_n, identify a family of polynomials $\mathcal{F}$ such that for all $f \in \mathcal{F}$ the Galois group of f over F is isomorphic to some $G \in \mathcal{G}$.

Task **T2** is not always possible; *e.g.*, Galois groups over p-adic fields must be solvable. But when it is possible, it is helpful to have a symbolic algorithm that accomplishes **T1**. For example, the following well-known result determines the Galois group of an irreducible even quartic polynomial defined over an arbitrary base field F of characteristic $\neq 2$ by testing whether two elements in F are perfect squares (see, for example, [6]).

Note Throughout this paper, we identify conjugacy classes of transitive subgroups of S_n by their "T" number as listed in [1]. For example, 4T1 $\simeq C_4$ (the cylic group of order 4), 4T2 $\simeq V_4 \simeq C_2 \times C_2$ (the Klein 4-group), and 4T3 $\simeq D_4$ (the dihedral group of order 8).

Algorithm 1.1 (Even Quartic Polynomials) *Let $f(x) = x^4 + ax^2 + b \in F[x]$ be an irreducible polynomial defined over a field of characteristic $\neq 2$. This algorithm returns the Galois group of f over F.*

(i) *If b is a perfect square in F, return 4T2 (V_4) and terminate.*

(ii) *Else, if $b(a^2 - 4b)$ is a perfect square in F, return 4T1 (C_4) and terminate. Otherwise, return 4T3 (D_4) and terminate.*

Received by the editors February 6, 2019; revised August 31, 2019.
Published online on Cambridge Core December 12, 2019.
AMS subject classification: **11Y40**, 12F10.
Keywords: even polynomials, sextic, Galois group.

https://doi.org/10.4153/S0008439519000754 Published online by Cambridge University Press

Table 1: One-parameter families of even quartic polynomials defined over **Q**.

Group	Name	Polynomials	
4T2	V_4	$x^4 + (2t+1)^2$	
4T1	C_4	$x^4 + 4tx^2 + 2t^2$	$t \neq 0$
4T3	D_4	$x^4 + t^2 + 1$	$t \neq 0$

Table 2: Possible Galois groups of irreducible even sextic polynomials. **Size** gives the order of the group.

T	Name	Size
6T1	C_6	6
6T2	S_3	6
6T3	D_6	12
6T4	A_4	12
6T6	$A_4 \times C_2$	24
6T7	S_4^+	24
6T8	S_4^-	24
6T11	$S_4 \times C_2$	48

Using Algorithm 1.1, it is not difficult to produce families of polynomials that have the indicated Galois group. See Table 1 for examples of such polynomials defined over **Q**.

Since even polynomials come equipped with a polynomial defining an index-two subfield of the polynomial's stem field (obtained by halving all exponents), they are therefore a natural object of study in relation to task **T2**. And as Algorithm 1.1 makes it possible to easily accomplish task **T2** for even quartics, much attention has been given to even sextic polynomials; see, for example, [3–5].

For an even sextic polynomial $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$, let K/F denote the stem field of f, G the Galois group of f, and $g(x) = x^3 + ax^2 + bx + c$. Then g defines a cubic subfield K_4 of K/F. Under the Galois correspondence, K_4 corresponds to a subgroup H of G of index 3 that contains the point stabilizer of 1. Of the 16 transitive subgroups of S_6, only 8 have such a subgroup H. Table 2 gives these 8 groups, their transitive numbers, their orders, and a descriptive name for each group. As is customary, × denotes a direct product, C_n the cyclic group of order n, D_n the dihedral group of order $2n$, and A_n and S_n are the alternating and symmetric groups on n letters, respectively.

Note 6T7 and 6T8 are isomorphic copies of S_4 that are distinguished by their parity; that is, 6T7 contains only even permutations while 6T8 does not. This fact is reflected in the table by the respective superscripts of each group's *Name*.

In [7], the author gives one family of even sextic polynomials for each possible Galois group over $\mathbb{Q}$, except 6T1. Focusing just on 6T4, [3] gives another family, and [5] provides four additional families. For both 6T4 and 6T7, [4] provides three more families. In all instances, the techniques used to accomplish task **T1** are specific to the case where the base field F is $\mathbb{Q}$, though [7] does mention that his method "might be extended to cover other possibilities, such as p-adic or number field base fields."

https://doi.org/10.4153/S0008439519000754 Published online by Cambridge University Press

The purpose of this paper is to present a generic algorithm for computing Galois groups of even sextic polynomials defined over arbitrary base fields of characteristic $\neq 2$ that is similar in spirit to Algorithm 1.1. This is carried out in Section 2. In particular, our method involves testing whether three elements of the base field are perfect squares and whether a related sextic polynomial is reducible. Our method allows us to easily verify that the families in [3–5,7] have the correct Galois groups. We include an example of such a verification in Section 2.1. We end with Section 3, where we give new one-parameter families for each possible Galois group (defined over $\mathbf{Q}$).

2 Algorithm for Even Sextic Polynomials

As before, let F be a field of characteristic $\neq 2$ and let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be an irreducible polynomial. Let K/F denote the stem field of f and let G be the Galois group of f. Let $g(x) = x^3 + ax^2 + bx + c$. Then g defines a cubic subfield of K/F. We can determine properties of G from properties of $g(x)$ using the Galois correspondence.

Note In all of our computational group-theoretic arguments, we performed the computation in the computer algebra system Magma, which includes representatives of conjugacy classes of transitive subgroups of S_n for $n \leq 47$.

Proposition 2.1 *Let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be irreducible, let K be the stem field of f, let G be the Galois group of f, and $g(x) = x^3 + ax^2 + bx + c$. Let d denote the discriminant of g so that $d = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$.*

(i) *$-c$ is a perfect square in F if and only if G is either A_4 or S_4^+.*
(ii) *d is a perfect square in F if and only if G is either C_6, A_4, or $A_4 \times C_2$.*
(iii) *$-cd$ is a perfect square in F if and only if G is either S_3, A_4, or S_4^-.*

Proof The discriminant of $f(x) = x^6 + ax^4 + bx^2 + c$ is $-c(8d)^2$. Therefore, G is a subgroup of A_6 if and only if $-c$ is a square in F. Of the 8 possibilities for G, only A_4 and S_4^+ are subgroups of A_6. This proves item (i).

Since d is the discriminant of the cubic polynomial $g(x) = x^3 + ax^2 + bx + c$, d is a perfect square if and only if the Galois group of $g(x)$ is C_3. But since $g(x)$ defines a cubic subfield of K/F, the stem field of $g(x)$ corresponds to an index 3 subgroup H of G containing the point stabilizer of 1 in G. By the Galois correspondence, the Galois group of $g(x)$ is isomorphic to the image of the permutation representation of G acting on the cosets G/H. By direct computation on the 8 possibilities for G, we see that each has a unique such subgroup H of index 3, up to conjugation.

Note This means K/F has a unique cubic subfield, up to isomorphism. Further group computations show that in the cases of C_6, A_4, and $A_4 \times C_2$, the image of the permutation representation of G acting on G/H is isomorphic to C_3; in all other cases, it is isomorphic to S_3. This proves item (ii).

If both $-c$ and d are perfect squares, then clearly $-cd$ is a perfect square. Based on the previous two paragraphs, there is only one group among the 8 where this occurs, namely, A_4. Otherwise, if $-cd$ is a perfect square, it must be the case that both $-c$ and d are not perfect squares. For the remainder of the proof, we suppose neither $-c$ nor d

https://doi.org/10.4153/S0008439519000754 Published online by Cambridge University Press

are perfect squares. Thus, the polynomials x^2+c and x^2-d define quadratic subfields of the splitting field of $f(x)$. By the Galois correspondence, the stem field of x^2+c corresponds to $H_c = A_6 \cap G$. Similarly, if K' is the normal closure of $g(x)$, then the subgroup fixing K' is the normal core, $\mathrm{Core}_G(H)$, of H in G; recall H is the subgroup fixing the stem field of $g(x)$. Thus, the stem field of x^2-d corresponds to the unique subgroup H_d of G of index 2 (up to conjugation) that contains $\mathrm{Core}_G(H)$. It follows that $-cd$ is a perfect square if and only if $H_c = H_d$. Among the four remaining possible Galois groups, direct computation shows S_3 and S_4^- have $H_c = H_d$. The groups D_6 and $S_4 \times C_2$ have $H_c \neq H_d$. ■

Based on Proposition 2.1, we can now determine when the Galois group of $f(x) = x^6+ax^4+bx^2+c$ is either A_4 or S_4^+. If $-c$ is a perfect square, then the Galois group of $f(x)$ is A_4 if d is a perfect square and S_4^+ if d is not a perfect square. We note that this observation plays a prominent role in the Galois group computations in [4, 5], though their context was $F = \mathbb{Q}$.

To determine the Galois group in the remaining six cases, we introduce a degree six resolvent polynomial.

Proposition 2.2 *Let $f(x) = x^6+ax^4+bx^2+c \in F[x]$ be irreducible and G the Galois group of f. Define $h(x)$ to be the following degree 6 polynomial:*

$$h(x) = x^6 - bx^4 + acx^2 - c^2.$$

(i) *$h(x)$ is squarefree if and only if characteristic of $F \neq 2$.*

(ii) *$h(x)$ is reducible if and only if G is either C_6, S_3, or D_6.*

Proof Let $S = \{\pm r_1, \pm r_2, \pm r_3\}$ be the roots of f in $\overline{F}$. The roots of h are $\{\pm r_1r_2, \pm r_1r_3, \pm r_2r_3\}$, which can be verified by expanding $(x^2-r_1^2r_2^2)(x^2-r_1^2r_3^2)(x^2-r_2^2r_3^2)$ and using the theory of elementary symmetric functions to express the resulting coefficients in terms of a, b, c. It follows that if the characteristic of $F = 2$, then h is not squarefree (*e.g.*, then $r_1r_2 = -r_1r_2$).

Suppose the characteristic of $F \neq 2$. Since f is irreducible, we have $0 \notin S$ and all elements of S are distinct. If h were not squarefree, this would imply that two roots of h are equal. In particular, we would have $AB = AC$ where $A, B, C \in S$. Dividing by A contradicts the fact that the elements of S are distinct. Thus, h must be squarefree, proving part (i).

To prove part (ii), let H be the subgroup of S_6 generated by the permutations (12), (34), and (3456). Thus H is a group of order 48 isomorphic to $S_2 \times S_4$. Define a function $R(x)$ by

$$R(x)^2 = \frac{\mathrm{Resultant}_y(f(y), f(x-y))}{2^6 \cdot f(x/2)}.$$

Using a computer algebra system, we can show that $R(x)$ is the product of x^3 and an even degree 12 polynomial. In fact, this degree 12 polynomial is equal to $\tilde{h}(x^2)$ where

$$\widetilde{h}(x) = x^6+4ax^5+(6a^2-2b)x^4+(4a^3-2ab-26c)x^3+(a^4+2a^2b-7b^2-24ac)x^2 \\ + 2(a^2-3b)(ab-9c)x + (a^2b^2-4b^3-4a^3c+18abc-27c^2).$$

https://doi.org/10.4153/S0008439519000754 Published online by Cambridge University Press

Table 3: For an irreducible even sextic polynomial $f(x) = x^6 + ax^4 + bx^2 + c$, let d be the discriminant of $g(x) = x^3 + ax^2 + bx + c$ and let $h(x) = x^6 - bx^4 + acx^2 - c^2$. The table lists whether the values of $-c$, d, and $-cd$ are perfect squares and whether $h(x)$ is reducible, according to the Galois group G of f.

T	**G**	$\mathbf{-c}$ **= square**	**d = square**	$\mathbf{-cd}$ **= square**	**h(x) = reducible**
1	C_6	no	yes	no	yes
2	S_3	no	no	yes	yes
3	D_6	no	no	no	yes
4	A_4	yes	yes	yes	no
6	$A_4 \times C_2$	no	yes	no	no
7	S_4^+	yes	no	no	no
8	S_4^-	no	no	yes	no
11	$S_4 \times C_2$	no	no	no	no

In the language of [2, §6.3], $R(x)$ is the (absolute) resolvent polynomial corresponding to the multivariable function $T = x_1 + x_2$ that is stabilized by H. As shown in [8, Prop. 2.9], the irreducible factors of $R(x)$ that occur with multiplicity one correspond to orbits of the action of G on the cosets S_6/H. Direct computation on the 8 possible groups shows that all have an orbit of length 12 except C_6, S_3, and D_6. It follows that if $\widetilde{h}(x^2)$ is squarefree, it is reducible if and only if G is one of these three groups. Hence, if $\tilde{h}(x)$ is squarefree it is reducible if and only if G is either C_6, S_3, or D_6. By construction, h and $\widetilde{h}$ define isomorphic sextic sub-algebras of the algebra defined by $R(x)$. In fact, h corresponds to an analogous resolvent construction except with $T = x_1x_2$ instead of $T = x_1 + x_2$. Since h is always squarefree (assuming characteristic $F \neq 2$), it follows that h is reducible if and only if G is either C_6, S_3, or D_6, proving item (ii). ■

In Table 3, we summarize the information presented in Propositions 2.1 and 2.2. This table forms the basis for our algorithm for computing the Galois group of an irreducible even sextic polynomial.

Algorithm 2.3 *Let $f(x) = x^6 + ax^4 + bx^2 + c \in F[x]$ be irreducible, let $d = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$ be as in Proposition 2.1, and let $h(x) = x^6 - bx^4 + acx^2 - c^2$ be as in Proposition 2.2. This algorithm returns the Galois group of $f(x)$.*

(i) *If $-c$ is a perfect square in F, then*
  (a) *if d is a perfect square, return 6T4 (A_4) and terminate;*
  (b) *otherwise, return 6T7 (S_4^+) and terminate.*

(ii) *Else, if d is a perfect square, then*
  (a) *if $h(x)$ is reducible, return 6T1 (C_6) and terminate;*
  (b) *otherwise, return 6T6 ($A_4 \times C_2$) and terminate.*

(iii) *Else, if $-cd$ is a perfect square, then*
  (a) *if $h(x)$ is reducible, return 6T2 (S_3) and terminate;*
  (b) *otherwise, return 6T8 (S_4^-) and terminate.*

(iv) *Else, if $h(x)$ is reducible, return 6T3 (D_6) and terminate. Otherwise, return 6T11 ($S_4 \times C_2$) and terminate*

Table 4: One-parameter families of even sextic polynomials with specified Galois group over **Q**.

T	G	Polynomials
1	C_6	$x^6+(t^2+5)x^4+((t-1)^2+5)x^2+1$
2	S_3	x^6+3t^2
3	D_6	x^6+2t^2
4	A_4	$x^6-3t^4x^2-t^6$
6	$A_4\times C_2$	$x^6-3t^2x^2+t^3,\ -t\neq\square$
7	S_4^+	$x^6+t^2x^4-t^6$
8	S_4^-	$x^6+(31t^2)^2x^2+(31t^2)^3$
11	$S_4\times C_2$	$x^6+(2t^2)^2x^2+(2t^2)^3$

2.1 An Example

We will use Algorithm 2.3 to compute the Galois group of a family of even sextic polynomials from [7]. In particular, let $t\in\mathbb{Z}$ and suppose $f(x)=x^6+6x^4+9x^2+3t^2+4$ is irreducible over the rationals.

In this case, we have

$$\begin{aligned}-c &= -3t^2-4,\\ d &= -243t^4-324t^2=-c(9t)^2,\\ -cd &= (9ct)^2,\\ h(x) &= x^6-9x^4+(18t^2+24)x^2-9t^4-24t^2-16\\ &= (x^3-3x^2+3t^2+4)(x^3+3x^2-3t^2-4).\end{aligned}$$

So $-c$ is not a square; d is not a square; $-cd$ is a square, and $h(x)$ is reducible. Thus, the Galois group of f is S_3, as indicated in [7].

3 One-Parameter Families

In this section, we develop one-parameter families of even sextic polynomials defined over **Q** for each of the 8 possible Galois groups.

Proposition 3.1 *The polynomials in Table 4 have the indicated Galois group over* **Q**, *except for values of t that result in reducible polynomials.*

Proof Let $f(x)=x^6+ax^4+bx^2+c$ be one of the polynomials in Table 4 and let $g(x)=x^3+ax^2+bx+c$. Let $d=a^2b^2-4b^3-4a^3c+18abc-27c^2$ as defined in Proposition 2.1 and let $h(x)=x^6-bx^4+acx^2-c^2$ be as defined in Proposition 2.2. Using a computer algebra system, it can be verified that $h(x)$ is reducible (over $\mathbf{Q}(t)$) precisely in the cases C_6, S_3, and D_6. In particular, for C_6, $h(x)$ factors as $x^3+(2-t)x^2-(t+1)x-1$ times $x^3-(2-t)x^2-(t+1)x+1$. For S_3, $h(x)$ factors as x^3-3t^2 times x^3+3t^2. And for D_6, $h(x)$ factors as x^3-2t^2 times x^3+2t^2.

It remains to analyze whether the following are perfect squares: $-c$, d, and $-cd$. But this is a straightforward computation. The results are listed in Table 5. Comparing the

https://doi.org/10.4153/S0008439519000754 Published online by Cambridge University Press

Table 5: Discriminant data for polynomials listed in Table 4.

T	G	$-\mathbf{c}$	d	$-\mathbf{cd}$
1	C_6	-1	$[(t^2-t-1)(t^2-t+7)]^2$	$-[(t^2-t-1)(t^2-t+7)]^2$
2	S_3	$-3t^2$	$-3(3t)^4$	$(3t)^6$
3	D_6	$-2t^2$	$-3(6t^2)^2$	$(6t^2)^3$
4	A_4	t^6	$(3t^3)^4$	$(9t^9)^2$
6	$A_4 \times C_2$	$-t^3$	$(9t^3)^2$	$-t(3t^2)^4$
7	S_4^+	t^6	$-23t^{12}$	$-23t^{18}$
8	S_4^-	$-(31t^2)^3$	$-31(31t^2)^6$	$(31^5t^9)^2$
11	$S_4 \times C_2$	$-(2t^2)^3$	$-31(2t^2)^6$	$31(2t^2)^9$

data in Table 5 and the reducibility of $h(x)$ with the data in Table 3, it follows that each of the polynomials in Table 4 has the indicated Galois group (for values of t that result in irreducible polynomials). ■

Acknowledgements We thank the anonymous referee for their careful reading and many helpful suggestions that have improved the proofs and clarity of writing throughout the paper.

References

[1] G. Butler and J. McKay, *The transitive groups of degree up to eleven*. Comm. Algebra 11(1983), no. 8, 863–911. https://doi.org/10.1080/00927878308822884

[2] H. Cohen, *A course in computational algebraic number theory*. Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993. https://doi.org/10.1007/978-3-662-02945-9

[3] D. Eloff, B. K. Spearman, and K. S. Williams, *A 4-sextic fields with a power basis*. Missouri J. Math. Sci. 19(2007), no. 3, 188–194.

[4] J. Harrington and L. Jones, *The irreducibility of power compositional sextic polynomials and their Galois groups*. Math. Scand. 120(2017), no. 2, 181–194. https://doi.org/10.7146/math.scand.a-25850

[5] J. Ide and L. Jones, *Infinite families of A_4-sextic polynomials*. Canad. Math. Bull. 57(2014), no. 3, 538–545. https://doi.org/10.4153/CMB-2014-008-1

[6] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*. Amer. Math. Monthly 96(1989), no. 2, 133–137. https://doi.org/10.2307/2323198

[7] G. W. Smith, *Some polynomials over $Q(t)$ and their Galois groups*. Math. Comp. 69(2000), no. 230, 775–796. https://doi.org/10.1090/S0025-5718-99-01160-6

[8] L. Soicher, *The computation of Galois groups*. Master's thesis, Concordia University, Montreal, 1981.

Department of Mathematics and Statistics, Elon University, Campus Box 2320, Elon, NC 27244
e-mail: cawtrey@elon.edu pjakes@elon.edu