Bull. Aust. Math. Soc. (First published online 2025), page 1 of 15*
doi:10.1017/S0004972725000048
*Provisional—final page numbers to be inserted when paper edition is published

ON GALOIS GROUPS OF POWER COMPOSITIONAL NONIC POLYNOMIALS

CHAD AWTREY✉, FRANK PATANE and BRIAN TOONE

(Received 16 December 2024; accepted 28 December 2024)

Abstract

Let $g(x) = x^3 + ax^2 + bx + c$ and $f(x) = g(x^3)$ be irreducible polynomials with rational coefficients, and let $\mathrm{Gal}(f)$ be the Galois group of $f(x)$ over $\mathbb{Q}$. We show $\mathrm{Gal}(f)$ is one of 11 possible transitive subgroups of S_9, defined up to conjugacy; we use $\mathrm{Disc}(f)$, $\mathrm{Disc}(g)$ and two additional low-degree resolvent polynomials to identify $\mathrm{Gal}(f)$. We further show how our method can be used for determining one-parameter families for a given group. Also included is a related algorithm that, given a field $L/\mathbb{Q}$, determines when L can be defined by an irreducible polynomial of the form $g(x^3)$ and constructs such a polynomial when it exists.

2020 *Mathematics subject classification*: primary 11Y40; secondary 12F10.

Keywords and phrases: Galois group, computation, nonic polynomials, discriminant.

1. Introduction

Let $\mathbb{Q}$ denote the rational numbers and consider an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. An important problem in computational algebra is the determination of the Galois group, $\mathrm{Gal}(f)$, of $f(x)$. Standard techniques for doing so involve forming and factoring resolvent polynomials, which are polynomials that define subfields of the splitting field of $f(x)$ (see [14, 15]). In general, forming and factoring resolvent polynomials is a difficult task. However, in the special case where $f(x) = g(x^k)$ for some integer $k > 1$, it is often possible to compute the Galois group via more elementary methods. Previous results in this direction have produced elementary characterisations for $\mathrm{Gal}(f)$ in the following cases:

- $k = 2$ and $g(x) = x^2 + ax + b$ (see [13]);
- $k = 3$ and $g(x) = x^2 + ax + b$ (see [1]);
- $k = 4$ and $g(x) = x^2 + ax + b$ (see [3]);
- $k = 2$ and $g(x) = x^3 + ax^2 + bx + c$ (see [2]).

The purpose of this paper is to give a similar characterisation for the case $k = 3$ and $g(x) = x^3 + ax^2 + bx + c$. Such polynomials are of the form $f(x) = x^9 + ax^6 + bx^3 + c$, and we call them *power compositional nonic* polynomials, in accordance with [9].

Further, we give an algorithm to determine when an extension $L/\mathbb{Q}$ can be defined by a power compositional polynomial of the form $f(x) = g(x^3)$. This is similar in spirit to what was done in [1], where the focus was on the special case where the degree of $g(x)$ was 2. An implementation of our algorithm is available at [4].

The remainder of the paper is organised as follows. In Section 2, we give a formula for discriminants of general power compositional polynomials of the form $f(x) = g(x^n)$, where the degree of $g(x)$ is m. In the subsequent sections, we restrict our attention to irreducible polynomials $f(x) = g(x^3)$, where $g(x) = x^3 + ax^2 + bx + c$. In Section 3, we establish notation, and recall two basic results about Galois groups of cubic polynomials and the relationship between $\mathrm{Gal}(f)$ and $\mathrm{Disc}(f)$, the discriminant of $f(x)$. We end by establishing bounds on the degree of the splitting field of $f(x)$ as well as the Galois group of the relative extension L/K, where L and K are the fields defined by $f(x)$ and $g(x)$, respectively. The purpose of Section 4 is to develop a list of possibilities for $\mathrm{Gal}(f)$, defined up to conjugacy in S_9 (the symmetric group of degree 9). The list includes 11 possible groups, and we show that each one is realised as a Galois group over $\mathbb{Q}$ of an irreducible power compositional nonic polynomial. In Section 5, we develop a characterisation of $\mathrm{Gal}(f)$ that involves the squareness of $\mathrm{Disc}(f)$ and $\mathrm{Disc}(g)$ as well as the factorisation pattern of a related degree 9 resolvent polynomial. These three pieces of information are enough to determine $\mathrm{Gal}(f)$ in 9 out of 11 cases. For the other two cases, we use a standard linear resolvent (following [14]). This section culminates in our main result, Theorem 5.5. In the following section, we give several examples that illustrate the use of Theorem 5.5. Example 6.1 recovers the characterisation in [11] that $\mathrm{Gal}(x^9 + 9mx^6 + 192m^3)$ is isomorphic to the dihedral group of order 18 for all $m \neq 0$. In addition, Table 5 gives one-parameter families with a given Galois group, where the verification that each polynomial in a given family has the associated Galois group follows from Theorem 5.5; Examples 6.2 and 6.3 illustrate this. We end with Section 7, which is devoted to describing an algorithm that, given an extension $L/\mathbb{Q}$, constructs an irreducible power compositional polynomial of the form $g(x^3)$ that defines L when such a polynomial exists; we make no restrictions on the degree of $g(x)$.

Note. While we are assuming all polynomials have rational coefficients, this is only for concreteness. Our proofs are valid for polynomials defined over any finite extension of $\mathbb{Q}$ that does not contain the cube roots of unity. With minor modifications, the results also apply more generally, including all fields of characteristic 0.

2. Discriminants of power compositional polynomials

In this section, we give a formula for the discriminant of a polynomial of the form $g(x^n)$ that we will use later. We note that our result is a special case of [10, Theorem 2.7], but our method of proof is different.

For complete generality, we let K be a field, $\overline{K}$ an algebraic closure of K, $f(x) \in K[x]$ a monic polynomial of degree n, R_f the set of roots of $f(x)$ in $\overline{K}$ and $f'(x)$ the derivative

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

of $f(x)$. Recall that the discriminant of $f(x)$, which we denote by $\mathrm{Disc}(f)$, can be computed as follows (see for example [6, Section 3.3]):

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \prod_{\rho \in R_f} f'(\rho).$$

LEMMA 2.1. *Let K be a field and $f(x) \in K[x]$ a monic polynomial, where $f(x) = g(x^n)$ and $g(x) \in K[x]$ is monic of degree m. Let $c = f(0)$. Then,*

$$\mathrm{Disc}(f) = (-1)^{nm(n-1)(m+2)/2} \cdot n^{nm} \cdot c^{n-1} \cdot \mathrm{Disc}(g)^n.$$

PROOF. Let R_f and R_g denote the roots of $f(x)$ and $g(x)$ in an algebraic closure $\overline{K}$, respectively. Let $\zeta \in \overline{K}$ be a primitive nth root of unity. Thus, there exist $\rho_1, \ldots, \rho_m \in \overline{K}$ such that $R_f = \{\rho_i \zeta^j : 1 \le i \le m, 0 \le j \le n-1\}$ and $R_g = \{\rho_1^n, \ldots, \rho_m^n\}$. We note that

$$c = f(0) = (-1)^{nm} \prod_{\rho \in R_f} \rho.$$

We define d_f and d_g by

$$d_f = \prod_{\rho \in R_f} g'(\rho^n), \quad d_g = \prod_{\rho \in R_g} g'(\rho).$$

Since the map R_f to R_g defined by $x \mapsto x^n$ is n-to-one, we have $d_f = d_g^n$. Further,

$$\mathrm{Disc}(g) = (-1)^{m(m-1)/2} \prod_{\rho \in R_g} g'(\rho) = (-1)^{m(m-1)/2} d_g.$$

We can therefore conclude that

$$(-1)^{nm(1-m)/2} \mathrm{Disc}(g)^n = d_g^n.$$

Using the chain rule, we see that $f'(x) = nx^{n-1} g'(x^n)$. Therefore, the discriminant of $f(x)$ is

$$\begin{aligned}
\mathrm{Disc}(f) &= (-1)^{nm(nm-1)/2} \prod_{\rho \in R_f} f'(\rho) = (-1)^{nm(nm-1)/2} \prod_{\rho \in R_f} (n \cdot \rho^{n-1} \cdot g'(\rho^n)) \\
&= (-1)^{nm(nm-1)/2} \Big(\prod_{\rho \in R_f} n \Big) \Big(\prod_{\rho \in R_f} \rho^{n-1} \Big) \Big(\prod_{\rho \in R_f} g'(\rho^n) \Big) \\
&= (-1)^{nm(nm-1)/2} \cdot n^{nm} \cdot (-1)^{nm(n-1)} \cdot c^{n-1} \cdot d_f \\
&= (-1)^{nm(nm-2n-3)/2} \cdot n^{nm} \cdot c^{n-1} \cdot d_g^n \\
&= (-1)^{nm(n-1)(m+2)/2} \cdot n^{nm} \cdot c^{n-1} \cdot \mathrm{Disc}(g)^n.
\end{aligned}$$

□

3. Notation and preliminary results

For the rest of this paper, we fix the following notation:

- $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$, irreducible;
- $g(x) = x^3 + ax^2 + bx + c$;

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

- ζ a primitive cube root of unity (that is, a root of $x^2 + x + 1$);
- S_n the symmetric group of degree n;
- A_n the alternating group of degree n;
- Gal(h) the Galois group of a polynomial $h(x)$, where the base field will be clear from context.

It follows that the complex roots of $f(x)$ are

$$\{\alpha, \alpha\zeta, \alpha\zeta^2, \beta, \beta\zeta, \beta\zeta^2, \gamma, \gamma\zeta, \gamma\zeta^2\},$$

where $\alpha^3, \beta^3, \gamma^3$ are the roots of $g(x)$. From Lemma 2.1,

$$\mathrm{Disc}(f) = -3^9 c^2 \mathrm{Disc}(g)^3.$$

This leads to the following results.

COROLLARY 3.1. *Suppose* $f(x) = x^9 + ax^6 + bx^3 + c$ *is irreducible over* $\mathbb{Q}$. *Then,* $\mathrm{Disc}(f) \in \mathbb{Q}^2$ *if and only if* $-3\mathrm{Disc}(g) \in \mathbb{Q}^2$.

We recall two facts about discriminants and Galois groups (see for example [8, Section 14.6]).

(1) For any irreducible polynomial $\tilde{g}(x) \in \mathbb{Q}[x]$ of degree n, Gal($\tilde{g}$) is isomorphic to a subgroup of A_n if and only if $\mathrm{Disc}(\tilde{g}) \in \mathbb{Q}^2$.
(2) If F is any field of characteristic 0 and $\tilde{g}(x) \in F[x]$ is irreducible of degree 3, then Gal($\tilde{g}$) over F is isomorphic to A_3 (cyclic of order 3) if $\mathrm{Disc}(\tilde{g}) \in F^2$ and is isomorphic to S_3 if $\mathrm{Disc}(\tilde{g}) \notin F^2$.

Combining item (2) above with Corollary 3.1 yields the following result.

COROLLARY 3.2. *Suppose* $f(x) = x^9 + ax^6 + bx^3 + c$ *is irreducible over* $\mathbb{Q}$ *and let* $g(x) = x^3 + ax^2 + bx + c$. *If* Gal($g$) *is cyclic of order 3 (that is,* A_3*), then* $\mathrm{Disc}(f) \notin \mathbb{Q}^2$.

Let L denote the splitting field of $f(x)$ over $\mathbb{Q}$. Thus, $L = \mathbb{Q}(\alpha, \beta, \gamma, \zeta)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 9$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, we see that $[L : \mathbb{Q}] \geq 18$. Let K denote the splitting field of $g(x)$. Thus, $K = \mathbb{Q}(\alpha^3, \sqrt{\mathrm{Disc}(g)})$, and we have $\beta^3, \gamma^3 \in K$ as well. We note further that $[K : \mathbb{Q}] \leq 6$ and, therefore, $[K(\zeta) : \mathbb{Q}] \leq 12$. It follows that for each $\rho \in \{\alpha, \beta, \gamma\}$, we have $[K(\rho, \zeta) : K(\zeta)] \leq 3$. We have therefore established the following result.

LEMMA 3.3. *Suppose* $f(x) = x^9 + ax^6 + bx^3 + c$ *is irreducible over* $\mathbb{Q}$ *and let* $L/\mathbb{Q}$ *denote its splitting field. Then,* $18 \leq [L : \mathbb{Q}] \leq 324$.

We turn our attention to the relative extension $\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha^3)$. Factoring $f(x)$ over $\mathbb{Q}(\alpha^3)$, we obtain the factorisation

$$f(x) = (x^3 - \alpha^3)(x^6 + (a + \alpha^3)x^3 + (\alpha^6 + a\alpha^3 + b),$$

which can be verified by expanding the factored expression and using the fact that $f(\alpha) = 0$ so that $c = -\alpha^9 - a\alpha^6 - b\alpha^3$. It follows that $x^3 - \alpha^3$ is irreducible, for if it were not, then this would contradict the fact that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 9$, thereby contradicting

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

the irreducibility of $f(x)$. It therefore also follows that $x^3 - \alpha^3$ defines the relative extension $\mathbb{Q}(\alpha)/\mathbb{Q}(\alpha^3)$. The following result will be useful in the determination of $\mathrm{Gal}(f)$.

LEMMA 3.4. *Suppose $f(x) = x^9 + ax^6 + bx^3 + c$ is irreducible over $\mathbb{Q}$ and let $f(\alpha) = 0$. Then, $\mathrm{Gal}(x^3 - \alpha^3)$ over $\mathbb{Q}(\alpha^3)$ is isomorphic to S_3, the symmetric group of degree 3.*

PROOF. Let $\tilde{f} = x^3 - \alpha^3$. Since $\tilde{f}$ is irreducible over $\mathbb{Q}(\alpha^3)$, we have already mentioned that $\mathrm{Gal}(\tilde{f})$ is isomorphic to S_3 if and only if $\mathrm{Disc}(\tilde{f}) \notin \mathbb{Q}(\alpha^3)^2$. Since $\mathrm{Disc}(\tilde{f}) = -27\alpha^6$, we have $\mathrm{Disc}(\tilde{f}) \notin \mathbb{Q}(\alpha^3)^2$ since $-3 \notin \mathbb{Q}(\alpha^3)^2$ (since $[\mathbb{Q}(\alpha^3) : \mathbb{Q}] = 3$ and therefore does not contain the quadratic extension $\mathbb{Q}(\sqrt{-3})$). □

4. Possible Galois groups

Since $f(x)$ is irreducible of degree 9, $\mathrm{Gal}(f)$ can be realised as a transitive subgroup of S_9, the symmetric group of degree 9; it is well defined up to conjugation as different orderings of the roots correspond to conjugate groups.

There are 34 such transitive subgroups, and they can be accessed with GAP [16] or at the L-functions and Modular Forms Database [17]. We use the standard 'T-number' notation to identify transitive groups as given in [5]. For example, 9T1 represents cyclic groups of order 9 and 9T34 represents S_9. See Table 1, which gives several pieces of information about representatives of conjugacy classes of transitive subgroups of S_9.

Specifically, let G be a representative from one of these conjugacy classes. Then, the table gives the following information:

- the T-number of G;
- the order of G;
- the parity of G; the parity is $+1$ if $G \leq A_9$ and -1 otherwise;
- the subfields of G.

The subfields of G are identified as follows. Let G_1 denote the stabiliser of 1 in G. For each subgroup H of G of index 3 containing G_1 up to conjugacy, we compute the action of G on the cosets G/H and the action of H on the cosets H/G_1, and we identify each action as a transitive subgroup of S_3. We are justified in calling this list the 'subfields' of G for the following reason: if $\mathrm{Gal}(f)$ is isomorphic to G and $f(\alpha) = 0$, then G_1 corresponds to $\mathbb{Q}(\alpha)$ under the Galois correspondence and the nontrivial proper subfields $\mathbb{Q}(\alpha)$ correspond to the proper subgroups H properly containing G_1; conjugate subgroups correspond to isomorphic subfields. For each such subgroup H, let K denote its fixed field. Let the irreducible cubic polynomials $g(x)$ and $\tilde{g}(x)$ define $K/\mathbb{Q}$ and $\mathbb{Q}(\alpha)/K$, respectively. Then, by the Galois correspondence, $\mathrm{Gal}(g)$ and $\mathrm{Gal}(\tilde{g})$ are isomorphic to the actions of G on G/H and H on H/G_1, respectively. Each entry in this column of the table is of the form $[i, j]$, where $\mathrm{Gal}(g)$ is isomorphic to 3Ti and $\mathrm{Gal}(\tilde{g})$ is isomorphic to 3Tj; there is an entry for each such subgroup H (up to conjugacy). This is slightly more general than what is listed at [17], which only includes the transitive number for $\mathrm{Gal}(g)$ for each subfield $K/\mathbb{Q}$.

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

TABLE 1. Transitive subgroups of S_9 by T-number, order, parity and subfield information, as defined in Section 4.

T	Order	Parity	Subfields
1	9	+1	[1,1]
2	9	+1	[1,1], [1,1], [1,1], [1,1]
3	18	+1	[2,2]
4	18	−1	[1,2], [2,1]
5	18	+1	[2,2], [2,2], [2,2], [2,2]
6	27	+1	[1,1]
7	27	+1	[1,1]
8	36	−1	[2,2], [2,2]
9	36	+1	
10	54	+1	[2,2]
11	54	+1	[2,2]
12	54	−1	[2,1]
13	54	−1	[1,2]
14	72	+1	
15	72	−1	
16	72	−1	
17	81	+1	[1,1]
18	108	−1	[2,2]
19	144	−1	
20	162	−1	[2,1]
21	162	+1	[2,2]
22	162	−1	[1,2]
23	216	+1	
24	324	−1	[2,2]
25	324	+1	[1,2]
26	432	−1	
27	504	+1	
28	648	−1	[1,2]
29	648	−1	[2,2]
30	648	+1	[2,2]
31	1296	−1	[2,2]
32	1512	+1	
33	181440	+1	
34	362880	−1	

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

TABLE 2. Sample irreducible power compositional nonic polynomials with specified Galois group over $\mathbb{Q}$.

T	Name	Polynomial
3	D_9	$x^9 - 9x^6 + 27x^3 - 3$
4	$C_3 \times S_3$	$x^9 - 4x^6 + 3x^3 + 1$
5	$C_3 : S_3$	$x^9 - 3x^6 + 3x^3 + 1$
8	$S_3 \times S_3$	$x^9 + 3x^3 - 1$
10	$C_9 : C_6$	$x^9 - 2$
11	$C_3^2 : C_6$	$x^9 - x^6 + 5x^3 + 1$
13	$C_3^2 : S_3$	$x^9 - 3x^3 - 1$
18	$C_3^2 : D_6$	$x^9 + x^3 - 1$
21	$C_3^3 : S_3$	$x^9 - x^6 - 3x^3 - 3$
22	$C_3^3 : C_6$	$x^9 - 3x^6 + 3$
24	$C_3^3 : D_6$	$x^9 + x^3 - 3$

PROPOSITION 4.1. *Suppose* $f(x) = x^9 + ax^6 + bx^3 + c$ *is irreducible over* $\mathbb{Q}$ *and let* $g(x) = x^3 + ax^2 + bx + c$. *If* $G = \mathrm{Gal}(f)$, *then* G *is isomorphic to 9Tj for some* $j \in \{3, 4, 5, 8, 10, 11, 13, 18, 21, 22, 24\}$.

PROOF. We make use of Table 1. By Lemma 3.3, the order of G is bounded between 18 and 324. This rules out $j = 1, 2$ and all $j > 25$. If $f(\alpha) = 0$, then $\mathbb{Q}(\alpha^3)$ is a cubic subfield of $\mathbb{Q}(\alpha)$ defined by $g(x)$. Thus, we can use Lemma 3.4 to rule out $j \in \{6, 7, 9, 12, 14, 15, 16, 17, 19, 20, 23\}$ since these groups do not have at least one entry of the form $[1, 2]$ or $[2, 2]$. To rule out 9T25, we note that its parity is $+1$ and its subfield entry is $[1, 2]$. This means $\mathrm{Disc}(f) \in \mathbb{Q}^2$ and $\mathrm{Gal}(g)$ is isomorphic to 3T1. However, this is a contradiction to Corollary 3.2. □

We note that if $\mathrm{Gal}(f)$ is isomorphic to 9T4, then it is not clear immediately if $\mathrm{Gal}(g)$ is isomorphic to 3T1 or 3T2. However, it follows from Lemma 3.4 that $\mathrm{Gal}(g)$ must be 3T1. We formalise this in the following corollary.

COROLLARY 4.2. *Suppose* $f(x) = x^9 + ax^6 + bx^3 + c$ *is irreducible over* $\mathbb{Q}$ *and let* $g(x) = x^3 + ax^2 + bx + c$. *If* $\mathrm{Gal}(f)$ *is isomorphic to 9T4, then* $\mathrm{Gal}(g)$ *is isomorphic to 3T1.*

We also note that each of the 11 groups appearing in Table 1 does indeed occur as a Galois group of some irreducible power compositional polynomial of degree 9 over $\mathbb{Q}$; see Table 2 for one such polynomial per group. Also in the table, we give standard descriptive names, such as C_n for the cyclic group of order n, D_n for the dihedral group of order $2n$ and S_n for the symmetric group of degree n. We use $\times$ for direct products and : for semidirect products (that are not direct products).

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

5. Determining Gal(f)

In this section, we fix a generic ordering of the roots of $f(x)$ as defined in Table 3.

As the roots of $g(x)$ are $\{\alpha^3, \beta^3, \gamma^3\}$, we see that $\mathcal{B} = \{B_1, B_2, B_3\}$ forms a complete block system for Gal(f), where $B_1 = \{1, 4, 7\}$, $B_2 = \{2, 5, 8\}$ and $B_3 = \{3, 6, 9\}$. In other words, for each $\sigma \in \text{Gal}(f)$, we have $\sigma(B_i) \in \mathcal{B}$.

By reordering the roots within each block if necessary, it follows that Gal(f) is a subgroup of the permutation group $G \simeq$ 9T24, where

$$G = \langle (1,5,9)(2,3,7,8,6,4), (2,6,5,9,8,3) \rangle. \tag{5.1}$$

Consider the subgroup $H \simeq$ 9T8 of G, where

$$H = \langle (1,3,2)(4,9,5,7,6,8), (1,4,7)(2,6,8,3,5,9) \rangle. \tag{5.2}$$

Consider also the multivariable function $T(x_1, \ldots, x_9) = (x_1 + x_2 + x_3)^3$. Letting each $\sigma \in G$ act on T via subscripts, we see that the stabiliser of T inside G is H; this straightforward computation can be carried out with [16], for example.

Let $r(x)$ be the resolvent polynomial corresponding to G, H and T, according to [6, Definition 6.3.2]. More concretely, we can specify the roots of $r(x)$ in terms of the roots of $f(x)$ as follows. A group computation shows that a complete set of right coset representatives for G/H is: Id, $(3,6,9)$, $(3,9,6)$, $(2,3,5,6,8,9)$, $(2,5,8)(3,6,9)$, $(2,5,8)(3,9,6)$, $(2,3,8,9,5,6)$, $(2,6)(3,8)(5,9)$ and $(2,8,5)(3,9,6)$. Letting each of these coset representatives act on T via subscripts and then evaluating each image of T at the roots of $f(x)$ as specified in Table 3, we see that the roots of $r(x)$ are of the form $(\alpha + \beta\zeta^i + \gamma\zeta^j)^3$ for $0 \le i, j \le 2$. We can expand $r(x)$ and express its coefficients as elementary symmetric polynomials in the roots of $f(x)$. Doing so leads us to the following definition.

DEFINITION 5.1. Let $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$ be irreducible and let $r(x) = x^9 + \sum_{i=0}^{8} a_i x^i$, where

$$\begin{aligned}
a_8 &= -9a;\\
a_7 &= 36a^2 - 81b;\\
a_6 &= -84a^3 + 486ab - 4293c;\\
a_5 &= 9(14a^4 - 135a^2b + 243b^2 + 189ac);\\
a_4 &= -9(14a^5 - 180a^3b + 729ab^2 - 1836a^2c + 4860bc);\\
a_3 &= -2673c(19a^3 - 81ab)(28a^6 - 405a^4b + 2187a^2b^2 - 6561b^3) + 61236c^2;\\
a_2 &= -9(4a^7 - 54a^5b + 243a^3b^2 + 108a^4c + 1458a^2bc - 6561b^2c + 13851ac^2);\\
a_1 &= 9(a^8 - 9a^6b + 432a^5c - 1701a^3bc + 7290a^2c^2 - 6561bc^2);\\
a_0 &= -(a^3 - 27c)^3.
\end{aligned}$$

We have the following result about $r(x)$.

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

TABLE 3. Generic ordering of the roots of $f(x) = x^9 + ax^6 + bx^3 + c$.

#	1	2	3	4	5	6	7	8	9
Root	α	β	γ	$\alpha\zeta$	$\beta\zeta$	$\gamma\zeta$	$\alpha\zeta^2$	$\beta\zeta^2$	$\gamma\zeta^2$

TABLE 4. Possible Galois groups of $f(x) = g(x^3)$, where $g(x) = x^3 + ax^2 + bx + c$. For each possible $G = \mathrm{Gal}(f)$, we include the T-number of G, the parity of G, the T-number of $\mathrm{Gal}(g)$, the degrees of the irreducible factors of $r(x)$ and the degrees of the irreducible factors of $s(x)$ when $\mathrm{Gal}(f)$ is either 9T10 or 9T21. The polynomials $r(x)$ and $s(x)$ are given in Definitions 5.1 and 5.3, respectively.

T	Parity	Gal(g)	r(x)	s(x)
3	+1	3T2	3,3,3	
4	−1	3T1	1,2,6	
5	+1	3T2	1,1,1,6	
8	−1	3T2	1,2,6	
10	+1	3T2	9	9,9,18
11	+1	3T2	3,6	
13	−1	3T1	3,6	
18	−1	3T2	3,6	
21	+1	3T2	9	9,27
22	−1	3T1	9	
24	−1	3T2	9	

PROPOSITION 5.2. *Let $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$ be irreducible and define $r(x)$ as in Definition 5.1. Then:*

(1) *$r(x)$ is separable;*
(2) *the degrees of the irreducible factors of $r(x)$ are listed in Table 4, according to* $\mathrm{Gal}(f)$.

PROOF. Item (2) follows from item (1) and a group computation, since the degrees of the irreducible factors of $r(x)$ correspond to the orbit lengths of the action of $\mathrm{Gal}(f)$ on the cosets G/H; which in turn follows from a general result about irreducible factors of resolvent polynomials (see for example [6, Theorem 6.3.3]).

To prove item (1), we verify that $(\alpha + \beta\zeta^i + \gamma\zeta^j)^3$ is not equal to $(\alpha + \beta\zeta^k + \gamma\zeta^l)^3$ except when $(i,j) = (k,l)$. This is equivalent to showing $\beta\zeta^i + \gamma\zeta^j$ is not equal to $\beta\zeta^k + \gamma\zeta^l$ for $(i,j) \neq (k,l)$ and $j,k,l \in \{0,1,2\}$.

If $i = k$ (and $j \neq l$), then $\gamma = 0$; this contradicts the irreducibility of $f(x)$. We reach a similar contradiction if $j = l$ (and $i \neq k$). By dividing both expressions by ζ^i, we may also assume $i = 0$. This leaves 12 cases to analyse; namely $j \in \{0,1,2\}$, $k \in \{1,2\}$ and $l \in \{0,1,2\} \setminus \{j\}$.

Suppose $(j,k,l) = (0,1,1)$ so that $\beta + \gamma = \beta\zeta + \gamma\zeta$. In this case, $\beta = -\gamma$, which implies that $\beta^3 = -\gamma^3$. This in turn implies $-\alpha^3 = a$ is a rational root of $g(x)$, indicating

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

that $g(x)$ is reducible, contradicting the irreducibility of $f(x)$. Similar reasoning also applies to the cases $(j,k,l) \in \{(0,2,2),(1,1,2),(1,2,0),(2,1,0),(2,2,1)\}$.

Suppose $(j,k,l) = (0,1,2)$ so that $\beta + \gamma = \beta\zeta + \gamma\zeta^2$. Thus, $\beta(1-\zeta) = \gamma(\zeta^2 - 1)$. This implies $\beta = \gamma\zeta^2$, and thus $f(x)$ is not separable and therefore reducible. Similar reasoning also applies to the cases $(j,k,l) \in \{(0,2,1),(1,1,0),(1,2,2),(2,1,1),(2,2,0)\}$. □

An inspection of Table 4 shows that $\mathrm{Gal}(f)$ is uniquely determined in all cases except for 9T10 versus 9T21 by considering: (1) whether $\mathrm{Disc}(f)$ is a square in $\mathbb{Q}$; (2) whether $\mathrm{Disc}(g)$ is a square in $\mathbb{Q}$; and (3) the degrees of the irreducible factors of $r(x)$.

To determine whether $\mathrm{Gal}(f)$ is 9T10 or 9T21, we use another resolvent polynomial, which we define next.

DEFINITION 5.3. Let $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$ be irreducible and $r(x)$ be as in Definition 5.1. Let $s(x)$ be defined by

$$s(x)^2 = \frac{\mathrm{Resultant}_y(r(y), r(x-y))}{2^9 \cdot r(x/2)}.$$

Thus, $s(x)$ is the polynomial whose roots are sums of the form $\rho_i + \rho_j$ for $i < j$, where $\rho_1, \ldots, \rho_9$ are the roots of $r(x)$.

We note that resultants can be computed via [6, Algorithm 3.3.7]. The following result completes our classification.

PROPOSITION 5.4. *Let $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$ be irreducible, $r(x)$ as defined in Definition 5.1 and assume $\mathrm{Gal}(f)$ is either 9T10 or 9T21. Let $s(x)$ be defined as in Definition 5.3 and assume $s(x)$ is separable. If the degrees of the irreducible factors of $s(x)$ are:*

(1) $[9,9,18]$, *then $\mathrm{Gal}(f)$ is 9T10;*
(2) $[9,27]$, *then $\mathrm{Gal}(f)$ is 9T21.*

PROOF. By Table 4, we see that $r(x)$ is irreducible of degree 9. Letting 9T10 act on the cosets of G/H, where G and H are defined in (5.1) and (5.2), respectively, we see that:

- $\mathrm{Gal}(r)$ is 9T4 if $\mathrm{Gal}(f)$ is 9T10;
- $\mathrm{Gal}(r)$ is 9T12 if $\mathrm{Gal}(f)$ is 9T21.

It follows from [14, Section 3.5] that $s(x)$ is the resolvent polynomial corresponding to the subgroup $\tilde{H} = \langle (1,2),(3,4),(3,4,5,6,7,8,9)\rangle$ of S_9 that stabilises the multivariable function $x_1 + x_2$. We can assume $s(x)$ is separable by taking a Tschirnhaus transformation of $r(x)$ if necessary and recomputing $s(x)$; see [6, Algorithm 3.6.4]. Letting representatives for the conjugacy classes of 9T10 and 9T21 act on the cosets $S_9/\tilde{H}$ and extracting the orbit lengths of these actions proves the proposition. □

Using Table 4, we can summarise the characterisation of $\mathrm{Gal}(f)$ as follows.

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

THEOREM 5.5. *Let $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$ be irreducible and let $g(x) = x^3 + ax^2 + bx + c$. Let $r(x)$ and $s(x)$ be defined as in Definitions 5.1 and 5.3, respectively, and let R and S be the degrees of the irreducible factors of $r(x)$ and $s(x)$, respectively.*

- *If $R = [3, 3, 3]$, then $\mathrm{Gal}(f)$ is 9T3 $\simeq D_9$.*
- *If $R = [1, 1, 1, 6]$, then $\mathrm{Gal}(f)$ is 9T5 $\simeq C_3 : S_3$.*
- *If $R = [1, 2, 6]$, then:*
  - *if $\mathrm{Disc}(g) \in \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T4 $\simeq C_3 \times S_3$;*
  - *if $\mathrm{Disc}(g) \notin \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T8 $\simeq S_3 \times S_3$.*
- *If $R = [3, 6]$, then:*
  - *if $\mathrm{Disc}(f) \in \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T11 $\simeq C_9 : C_6$;*
  - *if $\mathrm{Disc}(f) \notin \mathbb{Q}^2$ and $\mathrm{Disc}(g) \in \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T13 $\simeq C_3^3 : S_3$;*
  - *if $\mathrm{Disc}(f) \notin \mathbb{Q}^2$ and $\mathrm{Disc}(g) \notin \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T18 $\simeq C_3^3 : D_6$.*
- *If $r(x)$ is irreducible, then:*
  - *if $\mathrm{Disc}(f) \notin \mathbb{Q}^2$ and $\mathrm{Disc}(g) \in \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T22 $\simeq C_3^3 : C_6$;*
  - *if $\mathrm{Disc}(f) \notin \mathbb{Q}^2$ and $\mathrm{Disc}(g) \notin \mathbb{Q}^2$, then $\mathrm{Gal}(f)$ is 9T24 $\simeq C_3^3 : D_6$;*
  - *if $\mathrm{Disc}(f) \in \mathbb{Q}^2$ and $S = [9, 9, 18]$, then $\mathrm{Gal}(f)$ is 9T10 $\simeq C_9 : C_6$;*
  - *if $\mathrm{Disc}(f) \in \mathbb{Q}^2$ and $S = [9, 27]$, then $\mathrm{Gal}(f)$ is 9T21 $\simeq C_3^3 : S_3$.*

6. Examples

In this section, we give several examples that apply Theorem 5.5 to compute Galois groups of power compositional nonic polynomials. Our first example recovers [11, Theorem 1.1].

EXAMPLE 6.1. Let $f(x) = x^9 + 9mx^6 + 192m^3 \in \mathbb{Q}[x]$, $m \neq 0$. Then, $\mathrm{Gal}(f) =$ 9T3 $\simeq D_9$.

PROOF. Factoring $r(x)$ gives three irreducible factors of degree 3:

$$x^3 + 27mx^2 + 7047m^2x - 107811m^3,$$
$$x^3 - 135mx^2 + 2187m^2x - 10125m^3,$$
$$x^3 + 27mx^2 + 243m^2x + 81m^3.$$

By Theorem 5.5, this shows $\mathrm{Gal}(f) =$ 9T3 $\simeq D_9$. □

Table 5 gives one-parameter families of polynomials for each of the 11 possible Galois groups of $f(x)$, assuming the resulting polynomial is irreducible when specialised at a particular rational value of the parameter. Here are two additional examples that illustrate the correctness of Table 5.

EXAMPLE 6.2. Let $f(x) = x^9 + 3tx^6 - 4t^2x^3 + t^3 \in \mathbb{Q}[x]$. Then, $\mathrm{Gal}(f) =$ 9T4 $\simeq C_3 \times S_3$.

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

TABLE 5. One parameter families of polynomials of the form $f(x) = x^9 + ax^6 + bx^3 + c \in \mathbb{Q}[x]$ with prescribed Galois group when $f(x)$ is irreducible.

T	Name	$f(x)$, $t \in \mathbb{Q}$
3	D_9	$x^9 - 225tx^6 + 27t^2x^3 - 3t^3$
4	$C_3 \times S_3$	$x^9 + 3tx^6 - 4t^2x^3 + t^3$
5	$C_3 : S_3$	$x^9 + 3tx^6 + 3t^2x^3 - t^3$
8	$S_3 \times S_3$	$x^9 + tx^6 + 3t^2x^3 + t^3$
10	$C_9 : C_6$	$x^9 + 9tx^6 + 9t(2t+1)x^3 - t(t-1)^3$
11	$C_3^2 : C_6$	$x^9 + 3t^2x^6 + 3t^4x^3 + 1$
13	$C_3^2 : S_3$	$x^9 + t^3x^6 - 9x^3 - t^3$
18	$C_3^2 : D_6$	$x^9 + 2tx^3 + 1$
21	$C_3^3 : S_3$	$x^9 + 6x^6 + 12x^3 + t^3 - 3$
22	$C_3^3 : C_6$	$x^9 + tx^6 - 9x^3 - t, \quad t \notin \mathbb{Q}^3$
24	$C_3^3 : D_6$	$x^9 + x^3 + t, \quad t \notin \mathbb{Q}^3$

PROOF. Factoring $r(x)$ gives

$$r(x) = x(x^2 - 27tx + 189t^2)(x^6 + 459t^2x^4 + 7290t^4x^2 + (27t^2)^3).$$

Thus, $R = [1, 2, 6]$. It follows from Theorem 5.5 that $\mathrm{Gal}(f)$ is either 9T4 or 9T8. We have $g(x) = x^3 + 3tx^2 - 4t^2x + t^3$ and $\mathrm{Disc}(g) = (7t^3)^2$ which is a square. Thus, $\mathrm{Gal}(f) = 9\mathrm{T}4 \simeq C_3 \times S_3$. □

EXAMPLE 6.3. Let $f(x) = x^9 + 9tx^6 + 9t(2t+1)x^3 - t(t-1)^3 \in \mathbb{Q}[x]$. Then, $\mathrm{Gal}(f) = 9\mathrm{T}10 \simeq C_9 : C_6$.

PROOF. Using Mathematica, we see that $r(x)$ is irreducible over $\mathbb{Q}(t)$. Thus, we assume that $t \in \mathbb{Q}$ is chosen so that $r(x)$ is irreducible. We also see that

$$\mathrm{Disc}(f) = (3^9t^4(t-1)^3(t^3 - 3t^2 - 24t - 1)^3)^2,$$

which is a perfect square. By Theorem 5.5, we see that $\mathrm{Gal}(f)$ is either 9T10 or 9T21. Forming $s(x)$ as given in Definition 5.3 and factoring it, we see it has three factors:

$$x^9 - 162tx^8 + (8019t^2 + 729t)x^7 + \cdots;$$
$$x^9 - 162tx^8 + (10206t^2 + 729t)x^7 + \cdots;$$
$$x^{18} + 324tx^{17} + \cdots.$$

Assuming t is chosen so that $s(x)$ is separable, we see that $S = [9, 9, 18]$. Thus, $\mathrm{Gal}(f) = 9\mathrm{T}10 \simeq C_9 : C_6$. □

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

7. Field extensions defined by polynomials of the form $g(x^3)$

In this section, we are interested in determining when a field extension $L/\mathbb{Q}$ of degree n can be defined by an irreducible polynomial $f(x) = g(x^3) \in \mathbb{Q}[x]$. We make use of the following previous results.

THEOREM 7.1 [1, Proposition 1.2]. *Suppose $L/\mathbb{Q}$ is an extension of degree mk. Then, L can be defined by an irreducible polynomial $g(x^k) \in \mathbb{Q}[x]$ if and only if L has a subfield K of degree m such that L/K is defined by an irreducible polynomial $x^k - a \in K[x]$.*

Moreover, if $\tilde{g}(x) \in \mathbb{Q}[x]$ is irreducible of degree m defining K and $h(x) = x^k - a \in K[x]$ is irreducible defining L/K, then $f(x) = g(x^k)$ defines $L/\mathbb{Q}$, where

$$f(x) = \mathit{Resultant}_y(x^k - a, \tilde{g}(y)).$$

We can guarantee that $f(x)$ is irreducible by replacing a by ab^k for some $b \in K$, if necessary (see for example [7, Appendix A]).

THEOREM 7.2 [12, Theorem 1]. *Let $K/\mathbb{Q}$ be a finite extension and let L/K be a cubic extension defined by the irreducible polynomial $h(x) = x^3 + ax^2 + bx + c$. Then, L/K is defined by a polynomial of the form $x^3 - d \in K[x]$ if and only if $-3\mathrm{Disc}(h) \in K^2$.*

Moreover, if $-3\mathrm{Disc}(h) \in K^2$, let $u = 3a^2 - 9b$, $v = -2a^3 + 9ab - 27c$ and e be a solution to $u^2x^2 - 9vx + 3u = 0$. Then, L/K is defined by $x^3 - u/(3e)$.

As a consequence of Theorems 7.1 and 7.2, the following algorithm is guaranteed to produce an irreducible power compositional polynomial $g(x^3)$ defining $L/\mathbb{Q}$, when it exists.

ALGORITHM 7.3. Suppose $L = \mathbb{Q}(\alpha)$, where α is a root of the irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n = km$.

(1) Determine irreducible polynomials $g_i(x)$ defining subfields K_i of L of degree m. If no such polynomials exist, L does not have subfields of degree m. (Note: computing subfields is a built-in command in several computer algebra systems, such as Pari/GP [18].)
(2) Factor $f(x)$ over each K_i and extract an irreducible cubic polynomial $h_i(x) \in K_i[x]$. Discard polynomials where $-3\mathrm{Disc}(h_i) \notin {K_i}^2$, since in these cases, L/K_i cannot be defined by a polynomial of the form $x^3 - a \in K_i[x]$.
(3) For each $h_i(x)$ that remains, use Theorem 7.2 to produce an irreducible polynomial $\tilde{h}_i(x) = x^3 - a_i \in K_i[x]$ that defines L/K_i.
(4) For each $\tilde{h}(x)$, compute $f_i(x) = \mathrm{Resultant}_y(\tilde{h}_i(x), g_i(y))$ to produce power compositional polynomials. If none of the $f_i(x)$ are irreducible, choose an $\tilde{h}_i(x)$, perform a Tschirnhaus transformation as described in Theorem 7.1 and recompute $f_i(x)$.

We have implemented [18, Algorithm 7.3] and created a web-interface [4], where a user can enter a polynomial $f(x) \in \mathbb{Q}[x]$. The website returns a power compositional $g(x^3)$ that defines an extension isomorphic to the extension defined by $f(x)$, when such a power compositional polynomial exists.

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press

EXAMPLE 7.4. To illustrate Algorithm 7.3, consider the irreducible polynomial in $\mathbb{Q}[x]$:

$$\begin{aligned} f(x) = x^{18} &- 6x^{17} + 19x^{16} - 35x^{15} + 41x^{14} \\ &- 29x^{13} + 9x^{12} + 14x^{11} - 35x^{10} + 34x^9 - 9x^8 \\ &- 6x^7 + 4x^6 - 15x^5 + 12x^4 + 8x^3 - 6x^2 - x + 1. \end{aligned}$$

Let $f(\alpha) = 0$ and $L = \mathbb{Q}(\alpha)$.

(1) Using [18], we see that the irreducible polynomial $g(x) = x^6 + 7x^5 + 18x^4 + 18x^3 + 2x^2 - 4x + 1$ defines a subfield K of L of degree 6.

(2) Let $g(\beta) = 0$. Factoring $f(x)$ over K and extracting an irreducible cubic factor, we obtain the polynomial $h(x) = x^3 + h_2x^2 + h_1x - \beta$, where

$$h_2 = \beta^5 + 6\beta^4 + 12\beta^3 + 8\beta^2 + \beta; \quad h_1 = -\beta^5 - 5\beta^4 - 7\beta^3 + 3\beta - 1.$$

(3) Using Theorem 7.2, we obtain

$$\tilde{h}(x) = x^3 + (-9\beta^5 - 42\beta^4 - 60\beta^3 - 12\beta^2 - 9\beta - 3) \in K[x],$$

which is irreducible over K and also defines L/K.

(4) Computing $\text{Resultant}_\beta(\tilde{h}(x), g(\beta))$, we obtain

$$x^{18} + 108x^{15} + 3834x^{12} + 43011x^9 - 107892x^6 - 2755620x^3 + 24111675,$$

which is a power compositional polynomial and irreducible over $\mathbb{Q}$.

Acknowledgements

The authors are grateful for the referee's close reading of the manuscript, and for the helpful suggestions which have increased accuracy and improved clarity throughout the paper.

References

[1] C. Awtrey, J. R. Beuerle and H. N. Griesbach, 'Field extensions defined by power compositional polynomials', *Missouri J. Math. Sci.* **33**(2) (2021), 163–180.

[2] C. Awtrey and P. Jakes, 'Galois groups of even sextic polynomials', *Canad. Math. Bull.* **63**(3) (2020), 670–676.

[3] C. Awtrey and F. Patane, 'An elementary characterization of the Galois group of a doubly even octic polynomial', *J. Algebra Appl.*, to appear; doi:10.1142/S0219498825502482.

[4] C. Awtrey, F. Patane and B. Toone, *Power Compositional Polynomial Calculator*. Available from https://math.samford.edu/cubic.

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

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, 138 (Springer-Verlag, Berlin, 1993).

[7] J. D. Dixon, 'Computing subfields in algebraic number fields', *J. Aust. Math. Soc. Ser. A* **49**(3) (1990), 434–448.

[8] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd edn (John Wiley and Sons, Inc., Hoboken, NJ, 2004).

[9] J. Harrington and L. Jones, 'The irreducibility of power compositional sextic polynomials and their Galois groups', *Math. Scand.* **120**(2) (2017), 181–194.
[10] J. Harrington and L. Jones, 'Monogenic cyclotomic compositions', *Kodai Math. J.* **44**(1) (2021), 115–125.
[11] L. Jones and T. Phillips, 'An infinite family of ninth degree dihedral polynomials', *Bull. Aust. Math. Soc*. **97**(1) (2018), 47–53.
[12] M.-C. Kang, 'Cubic fields and radical extensions', *Amer. Math. Monthly* **107**(3) (2000), 254–256.
[13] L.-C. Kappe and B. Warren, 'An elementary test for the Galois group of a quartic polynomial', *Amer. Math. Monthly* **96**(2) (1989), 133–137.
[14] L. Soicher, *The computation of Galois groups*, Master's thesis (Concordia University, Montreal, 1981).
[15] R. P. Stauduhar, 'The determination of Galois groups', *Math. Comp.* **27** (1973), 981–996.
[16] *The GAP Group*, 'GAP – Groups, Algorithms, and Programming', Version 4.8.10, 2018. Available from http://www.gap-system.org.
[17] *The LMFDB Collaboration*, *The L-functions and modular forms database* (2022). Available from https://www.lmfdb.org.
[18] The PARI Group, *PARI/GP – Computational Number Theory*, version 2.5.3, 2013. Available from http://pari.math.u-bordeaux.fr.

CHAD AWTREY, Department of Mathematics and Computer Science, Samford University, 800 Lakeshore Drive, Birmingham, AL 35229, USA
e-mail: cawtrey@samford.edu

FRANK PATANE, Department of Mathematics and Computer Science, Samford University, 800 Lakeshore Drive, Birmingham, AL 35229, USA
e-mail: fpatane@samford.edu

BRIAN TOONE, Department of Mathematics and Computer Science, Samford University, 800 Lakeshore Drive, Birmingham, AL 35229, USA
e-mail: brtoone@samford.edu

https://doi.org/10.1017/S0004972725000048 Published online by Cambridge University Press