MATH. SCAND. 120 (2017), 181–194

THE IRREDUCIBILITY OF POWER COMPOSITIONAL SEXTIC POLYNOMIALS AND THEIR GALOIS GROUPS

JOSHUA HARRINGTON and LENNY JONES

Abstract

We define a *power compositional sextic polynomial* to be a monic sextic polynomial $f(x) := h(x^d) \in \mathbb{Z}[x]$, where $h(x)$ is an irreducible quadratic or cubic polynomial, and $d = 3$ or $d = 2$, respectively. In this article, we use a theorem of Capelli to give necessary and sufficient conditions for the reducibility of $f(x)$, and also a description of the factorization of $f(x)$ into irreducibles when $f(x)$ is reducible. In certain situations, when $f(x)$ is irreducible, we also give a simple algorithm to determine the Galois group of $f(x)$ without the calculation of resolvents. The algorithm requires only the use of the Rational Root Test and the calculation of a single discriminant. In addition, in each of these situations, we give infinite families of polynomials having the possible Galois groups.

1. Introduction

Many techniques are known to determine whether a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$. Some of these methods require rather complicated calculations. One of the goals of this article is to present a very simple procedure to determine the irreducibility of a certain class of sextic polynomials which we refer to as power compositional sextic polynomials. We define a *power compositional sextic polynomial* as a monic sextic polynomial $f(x) := h(x^d) \in \mathbb{Z}[x]$, where $h(x)$ is an irreducible quadratic or cubic polynomial, and $d = 3$ or $d = 2$, respectively. Special cases of $f(x)$ when $d = 2$ have been studied by various authors [5], [6], [7], and the calculations used to establish the irreducibility of $f(x)$ in those papers are somewhat tedious and apply only to those specific situations. The case $d = 3$ does not seem to have been addressed previously in the literature. In this article, we use a theorem of Capelli to give necessary and sufficient conditions for the irreducibility of $f(x)$ that are very easy to implement in both cases. Moreover, in each case when $f(x)$ is reducible, we describe the degree-type of the factorization of $f(x)$ into irreducibles. For the particular situations of when $h(x)$ is a cubic and $f(0) = -c^2$, or when $h(x)$ is a quadratic and $f(0) = c^3$, these conditions give rise to an

Received 15 February 2015.
DOI: https://doi.org/10.7146/math.scand.a-25850

extremely simple algorithm (see Section 5) to determine the irreducibility of $f(x)$ and, without the use of resolvents, the Galois group of $f(x)$, when $f(x)$ is irreducible. Indeed, this algorithm represents a much easier alternative than any previously described method currently in the literature, and requires only the use of the Rational Root Test and the calculation of a single discriminant. For example, in [5], while the main agenda is to determine sextic monogenic fields, corresponding to $f(x)$, that have Galois group A_4, the methods used there to determine the irreducibility of $f(x)$ and its Galois group are more complicated than the approach given here. Additionally, this algorithm allows us to improve and extend the results in [6]. As an application of the algorithm, we provide infinite families of polynomials having the possible Galois groups.

Remark. We should point out that Stephen Brown [2], using more elementary techniques, has investigated the Galois groups that can occur for sextic polynomials of the form $x^6 + ax + b$.

2. Preliminaries and notation

Throughout this paper, we let $\Delta(f)$ denote the discriminant over $\mathbb{Q}$ of the polynomial $f(x)$, and if $f(x)$ is irreducible over $\mathbb{Q}$, we let $\mathrm{Gal}(f)$ denote its Galois group over $\mathbb{Q}$. For the sake of brevity, unless stated otherwise, when we say a polynomial is irreducible or reducible, we mean irreducible or reducible over $\mathbb{Q}$.

We now present some results, without proof, that are needed for the sequel. The following two theorems are due to Capelli (See Section 2.1 in [9]).

Theorem 2.1. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Q}[x]$ with $f(x)$ irreducible. Suppose that $f(\alpha) = 0$. Then $f(g(x))$ is reducible over $\mathbb{Q}$ if and only if $g(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$. Furthermore, if*

$$g(x) - \alpha = c_1 u_1(x)^{e_1} \cdots u_r(x)^{e_r},$$

where $c_1 \in \mathbb{Q}(\alpha)$, and the $u_j(x)$ are distinct monic irreducible polynomials in $\mathbb{Q}(\alpha)[x]$, then

$$f(g(x)) = c_2 \mathcal{N}(u_1(x))^{e_1} \cdots \mathcal{N}(u_r(x))^{e_r},$$

where $c_2 \in \mathbb{Q}$, and the norms $\mathcal{N}(u_j(x))$ are distinct monic irreducible polynomials in $\mathbb{Q}[x]$.

Theorem 2.2. *Let $r \in \mathbb{Z}$ with $r \geq 2$, and let $\alpha \in \mathbb{C}$ be algebraic. Then $x^r - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either there is a prime p dividing r such that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ or $4 \mid r$ and $\alpha = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$.*

We require the following three additional facts in Section 4.

Theorem 2.3. *Suppose that* $\deg(f(x)) = n$. *If* $f(x)$ *is irreducible, then* $\mathrm{Gal}(f)$ *is isomorphic to a subgroup of the alternating group* A_n *if and only if* $\sqrt{\Delta(f)} \in \mathbb{Z}$.

Theorem 2.4. *Let* $f(x) \in \mathbb{Z}[x]$ *be an irreducible monic sextic polynomial, and suppose that* $f(\alpha) = 0$. *Then* $\mathrm{Gal}(f)$ *is isomorphic to an element of* $\{A_4, S_4\}$ *if and only if* $\mathbb{Q}(\alpha)$ *contains a cubic subfield and* $\sqrt{\Delta(f)} \in \mathbb{Z}$.

Theorem 2.5. *Let* $f(x) \in \mathbb{Z}[x]$ *be an irreducible monic sextic polynomial, and suppose that* $f(\alpha) = 0$. *Then* $\mathrm{Gal}(f)$ *is isomorphic to an element of* $\{C_6, S_3, C_2 \times S_3\}$ *if and only if* $\mathbb{Q}(\alpha)$ *contains both a quadratic and a cubic subfield.*

Theorem 2.3 can be found in many basic Galois theory texts, and it also appears as Proposition 6.3.1 in [4]. Theorem 2.4 can be deduced from Theorem 2.3 and the more recent work of Butler and McKay [3] on the classification of transitive groups. Theorem 2.5 also follows from [3]. For additional information, see [1], [8], and the remark at the end of Section 6.3.5 in [4]. We have presented formal statements of these results for the convenience of the reader.

3. The irreducibility theorems

Theorem 3.1. *Let* $h(x) = x^2 + bx + c \in \mathbb{Z}[x]$ *be irreducible. Then*

$$f(x) := h(x^3) = x^6 + bx^3 + c$$

is reducible if and only if $c = n^3$ *and* $b = m^3 - 3mn$ *for some* $m, n \in \mathbb{Z}$. *Furthermore, if* $f(x)$ *is reducible and* $b^2 \geq 4c$, *then* $f(x)$ *factors as an irreducible quadratic polynomial times an irreducible quartic polynomial.*

Proof. Let $h(\alpha) = h(\bar{\alpha}) = 0$. By Theorems 2.1 and 2.2, $f(x)$ is reducible if and only if $\alpha = \beta^3$ for some $\beta \in \mathbb{Q}(\alpha)$. Suppose this is the case. We then deduce from Theorem 2.1 that

$$\begin{aligned} f(x) &= \mathcal{N}(x - \beta) \cdot \mathcal{N}(x^2 + \beta x + \beta^2) \\ &= (x^2 + mx + n)(x^4 + d_3x^3 + d_2x^2 + d_1x + d_0), \end{aligned} \tag{3.1}$$

where $m, n, d_i \in \mathbb{Z}$. Since

$$\mathcal{N}(x - \beta) = x^2 - (\beta + \bar{\beta})x + \beta\bar{\beta},$$

it follows that

$$n = \beta\bar{\beta} = \alpha^{1/3}\bar{\alpha}^{1/3} = c^{1/3} \in \mathbb{Z},$$

and thus $c = n^3$. By expanding and equating coefficients in (3.1), we get the system of equations

$$\begin{aligned} m + d_3 &= 0, \\ d_2 + md_3 + n &= 0, \\ d_1 + md_2 + nd_3 &= b, \\ d_0 + md_1 + nd_2 &= 0, \\ md_0 + nd_1 &= 0, \\ d_0 &= n^2. \end{aligned}$$

From this system, we see that $b = m^3 - 3mn$, completing the proof of the first part of the theorem.

To establish the second part of the theorem, notice that $\alpha \in \mathbb{R}$ if $b^2 \geq 4c$. However, the quadratic polynomial $x^2 + \beta x + \beta^2$ in (3.1) has negative discriminant, and so it is irreducible over $\mathbb{Q}(\alpha)$. Since $x - \beta$ is clearly irreducible over $\mathbb{Q}(\alpha)$, we deduce from Theorem 2.1 that $f(x)$ is reducible if and only if its irreducible factors are of degree 2 and 4.

Corollary 3.2. *Let $h(x) = x^2 + bx + c^3 \in \mathbb{Z}[x]$ be irreducible. Then $f(x) = x^6+bx^3+c^3$ is reducible if and only if $g(x) = x^3-3cx-b$ is reducible. Furthermore, if $g(x)$ factors as the product of three linear polynomials, then $f(x)$ factors as the product of three irreducible quadratic polynomials, and if $g(x)$ has exactly two irreducible factors, then $f(x)$ factors as an irreducible quadratic polynomial times an irreducible quartic polynomial.*

Proof. We know from Theorem 3.1 that $f(x)$ is reducible if and only if $b = m^3 - 3mc$ for some integer m. This is equivalent to saying that $f(x)$ is reducible if and only if $g(x) = x^3 - 3cx - b$ has an integer zero, which establishes the first part of the corollary.

To prove the second part of the corollary, suppose first that $g(x)$ factors as the product of three linear factors. Then there are three values of m that satisfy the equation $b = m^3 - 3mc$. Thus, since the factorization of $f(x)$ in (3.1) is unique up to the order of multiplication, we deduce that $f(x)$ has three quadratic factors. Hence, $x^2 + \beta x + \beta^2$ factors as the product of two linear factors, and therefore, by Theorem 2.1, the three quadratic factors of $f(x)$ must be irreducible.

Suppose now that $g(x)$ has exactly two irreducible factors. Then there is only a single value of m that satisfies $b = m^3 - 3mc$, and so $f(x)$ has exactly one quadratic factor. Since Theorem 2.1 implies that $f(x)$ cannot have a linear factor, we deduce that $f(x)$ factors as an irreducible quadratic polynomial times an irreducible quartic polynomial.

THEOREM 3.3. *Let $h(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ be irreducible. Then*

$$f(x) := h(x^2) = x^6 + ax^4 + bx^2 + c$$

is reducible if and only if $c = -n^2$ and $m^4 + 2am^2 - 8nm + a^2 - 4b = 0$ for some $m, n \in \mathbb{Z}$. Furthermore, if $f(x)$ is reducible, then $f(x)$ factors as the product of two irreducible cubic polynomials.

PROOF. Suppose that $h(\alpha) = 0$. By Theorems 2.1 and 2.2, $f(x)$ is reducible if and only if $\alpha = \beta^2$ for some $\beta \in \mathbb{Q}(\alpha)$. Suppose this is the case. We then deduce from Theorem 2.1 that

$$\begin{aligned} f(x) &= \mathcal{N}(x-\beta)\cdot\mathcal{N}(x+\beta) \\ &= (x^3 - mx^2 + tx - n)(x^3 + mx^2 + tx + n), \end{aligned} \tag{3.2}$$

where $m, t, n \in \mathbb{Z}$. Expanding and equating coefficients in (3.2), we see that

$$a = 2t - m^2, \quad b = t^2 - 2mn, \quad \text{and} \quad c = -n^2. \tag{3.3}$$

Solving for t in the first equation of (3.3) and substituting into the second equation gives $m^4 + 2am^2 - 8nm + a^2 - 4b = 0$ as desired.

Since $x-\beta$ and $x+\beta$ are irreducible over $\mathbb{Q}(\alpha)$, it follows from Theorem 2.1 that $f(x)$ factors as the product of two irreducible cubics.

COROLLARY 3.4. *Let $h(x) = x^3 + ax^2 + bx - c^2 \in \mathbb{Z}[x]$ be irreducible. Then $f(x) = x^6 + ax^4 + bx^2 - c^2$ is reducible if and only if $g(x) = x^4 + 2ax^2 - 8cx + a^2 - 4b$ has exactly one integer zero.*

PROOF. It follows immediately from Theorem 3.3 that $f(x)$ is reducible if and only if $g(x)$ has an integer zero. The corollary will follow by showing that if $g(x)$ has a quadratic factor, then $h(x)$ is reducible. So suppose that $g(x)$ has a quadratic factor $u(x) = x^2 + rx + s$. Dividing $g(x)$ by $u(x)$, and setting the coefficients of the remainder equal to zero, gives

$$-8c - r^3 + 2rs - 2ra = 0 \;\text{ and }\; -sr^2 + a^2 - 4b + s^2 - 2sa = 0. \tag{3.4}$$

Solving the first equation in (3.4) for s, and substituting into the second equation, we see that

$$\begin{aligned} 0 = \frac{r^6 + 4ar^4 + 16br^2 - 64c^2}{64} &= \left(\frac{r^2}{4}\right)^3 + a\left(\frac{r^2}{4}\right)^2 + b\left(\frac{r^2}{4}\right) - c^2 \\ &= h\left(\frac{r^2}{4}\right), \end{aligned}$$

so that $h(x)$ is reducible.

4. The Galois groups

In this section we establish simple criteria for the determination of the Galois group of the particular power compositional sextic polynomials $f(x)$ of Corollary 3.2 and Corollary 3.4. The techniques given in those corollaries, combined with the results of this section, provide a simple algorithm to determine the irreducibility of these compositional sextic polynomials $f(x)$, and $\mathrm{Gal}(f)$, if $f(x)$ is irreducible. The summary of this algorithm is given in Section 5.

We divide the remainder of this section into two subsections, according to the two cases given by Corollary 3.2 and Corollary 3.4. In each of these situations, we provide examples of infinite families of the power compositional sextic polynomials for each possible Galois group in the corresponding corollary. In the case of Corollary 3.4, we actually give three sets of infinite families depending on whether the coefficients of $f(x)$ are such that $a = 0$ and $b \neq 0$, or $a \neq 0$ and $b = 0$, or $a \neq 0$ and $b \neq 0$.

4.1. The case of Corollary 3.2

Throughout this section, we let

$$\begin{aligned} h(x) &= x^2 + bx + c^3, \\ f(x) &= h(x^3) = x^6 + bx^3 + c^3, \\ g(x) &= x^3 - 3cx - b, \end{aligned}$$

where $b, c \in \mathbb{Z}$, with $c \neq 0$. Then

$$\Delta(f) = 3^6 \cdot c^6 \cdot \Delta(h)^3 \quad \text{and} \quad \Delta(g) = -3^3 \cdot \Delta(h),$$

where $\Delta(h) = b^2 - 4c^3$. The zeros of $f(x)$ are

$$\alpha, \quad \beta, \quad -\beta\zeta, \quad -\alpha\zeta^{-1}, \quad -\beta\zeta^{-1}, \quad -\alpha\zeta,$$

where

$$\alpha = \left(\frac{-b - \sqrt{b^2 - 4c^3}}{2}\right)^{1/3}, \quad \beta = \left(\frac{-b + \sqrt{b^2 - 4c^3}}{2}\right)^{1/3}$$

and $\zeta = \dfrac{1 + \sqrt{-3}}{2}$, a primitive sixth root of unity. Thus,

$$\begin{aligned} h(\alpha^3) = f(\alpha) &= 0 = f(\beta) = h(\beta^3), \\ \alpha^3 + \beta^3 &= -b, \\ \alpha\beta &= c. \end{aligned} \tag{4.1}$$

It is straightforward to show that the zeros of $g(x)$ are

$$-(\alpha+\beta), \quad \beta\zeta+\alpha\zeta^{-1}, \quad \text{and} \quad \beta\zeta^{-1}+\alpha\zeta. \tag{4.2}$$

LEMMA 4.1. *Suppose that $h(x)$ is irreducible. Then*

$$\mathbb{Q}(\alpha^3)=\mathbb{Q}(\zeta) \iff \sqrt{\Delta(g)}=\sqrt{108c^3-27b^2}\in\mathbb{Z}.$$

PROOF. Suppose first that $\mathbb{Q}(\alpha^3)=\mathbb{Q}(\zeta)$. Since $h(x)$ is irreducible, there exist $r, s \in \mathbb{Q}$, with $s \neq 0$, such that

$$\sqrt{b^2-4c^3}=r+s\sqrt{-3}. \tag{4.3}$$

If $r \neq 0$, we get a contradiction by squaring both sides of (4.3). Hence, $r=0$, and multiplying both sides of (4.3) by $3\sqrt{-3}$ gives

$$\sqrt{108c^3-27b^2}=-9s\in\mathbb{Q}.$$

Since $\Delta(g)\in\mathbb{Z}$, we deduce that $\sqrt{\Delta(g)}\in\mathbb{Z}$.

Conversely, suppose that $\sqrt{\Delta(g)}\in\mathbb{Z}$. Then

$$\sqrt{b^2-4c^3}=\left(\frac{-\sqrt{\Delta(g)}}{9}\right)\sqrt{-3},$$

which implies that $\mathbb{Q}(\alpha^3)=\mathbb{Q}(\zeta)$.

THEOREM 4.2. *Suppose that $f(x)$ is irreducible. Then*

$$\mathrm{Gal}(f)\simeq\begin{cases} C_2\times S_3, & \textit{if } \Delta(g) \textit{ is not a square in } \mathbb{Z},\\ C_6, & \textit{if } \Delta(g) \textit{ is a square in } \mathbb{Z}.\end{cases}$$

PROOF. We claim that $\mathrm{Gal}(f)$ is isomorphic to one of the groups in $\{C_6, S_3, C_2\times S_3\}$. Since $f(x)$ is irreducible, we have that $[\mathbb{Q}(\alpha):\mathbb{Q}]=6$. To establish the claim, it is enough, by Theorem 2.5, to show that $\mathbb{Q}(\alpha)$ contains both a quadratic subfield and a cubic subfield.

Note that $h(x)$ is irreducible since $f(x)$ is irreducible, and therefore, $\mathbb{Q}(\alpha^3)$ is a quadratic subfield of $\mathbb{Q}(\alpha)$. From (4.1), we have that $\alpha+\beta\in\mathbb{Q}(\alpha)$, and since $g(x)$ is irreducible by Corollary 3.2, it follows from (4.2) that $\mathbb{Q}(\alpha+\beta)$ is a cubic subfield of $\mathbb{Q}(\alpha)$. Hence, the claim is established.

Now suppose that $\Delta(g)$ is not a square in $\mathbb{Z}$. If $|\mathrm{Gal}(f)|=6$, then $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta\zeta)$, and so $\zeta\in\mathbb{Q}(\alpha)$ by (4.1). Since both S_3 and C_6 have a unique subgroup of order 3, it follows that $\mathbb{Q}(\alpha^3)=\mathbb{Q}(\zeta)$. Thus, from Lemma 4.1, we have that $\sqrt{\Delta(g)}\in\mathbb{Z}$, which contradicts our assumption. Therefore, $\mathrm{Gal}(f)\simeq C_2\times S_3$.

Now assume that $\Delta(g)$ is a square in $\mathbb{Z}$. Then $\mathrm{Gal}(g) \simeq A_3$ by Theorem 2.3. Consequently, $\mathbb{Q}(\alpha+\beta)$ is a normal extension of $\mathbb{Q}$ so that

$$\mathbb{Q}(\alpha+\beta) = \mathbb{Q}(\beta\zeta + \alpha\zeta^{-1}) = \mathbb{Q}(\beta\zeta^{-1} + \alpha\zeta), \tag{4.4}$$

and $\mathrm{Gal}(f)$ has a normal subgroup of order 2. Thus, $\mathrm{Gal}(f) \not\simeq S_3$. Because ζ is clearly not an element of $\mathbb{Q}(\alpha+\beta)$, we have that $[L:\mathbb{Q}] = 6$, where

$$L := \mathbb{Q}(\alpha+\beta, \zeta).$$

Since $\sqrt{\Delta(g)} \in \mathbb{Z}$, it follows from Lemma 4.1 that $\alpha^3 \in L$ and $\beta^3 \in L$. Since $(\alpha+\beta)^2 \in L$, we see by (4.1) that $\alpha^2+\beta^2 \in L$. Note that $\beta\zeta + \alpha\zeta^{-1} \in L$ from (4.4). Thus, since $\alpha^3, \beta^3, \zeta, \zeta^{-1} \in L$, we deduce that

$$\alpha^2\beta\zeta^2 + \alpha\beta^2 = \zeta\big((\alpha^2+\beta^2)(\beta\zeta+\alpha\zeta^{-1}) - (\alpha^3\zeta^{-1} + \beta^3\zeta)\big) \in L. \tag{4.5}$$

Similarly, we have

$$\alpha^2\beta + \alpha\beta^2 = (\alpha^2+\beta^2)(\alpha+\beta) - (\alpha^3+\beta^3) \in L. \tag{4.6}$$

Therefore, by (4.1), (4.5) and (4.6), we get that

$$\alpha = \frac{(\alpha^2\beta\zeta^2 + \alpha\beta^2) - (\alpha^2\beta + \alpha\beta^2)}{c(\zeta^2 - 1)} \in L.$$

Hence, $\beta \in L$ and L is the splitting field of $f(x)$. We conclude that $\mathrm{Gal}(f) \simeq C_6$, which completes the proof of the theorem.

In the following corollary we give examples of some infinite families of these polynomials having each of the possible Galois groups C_6 and $C_2 \times S_3$.

Corollary 4.3. *Define*

$$\mathscr{F}_1 = \left\{x^6 + \epsilon(3k^2+3k+1)x^3 + (3k^2+3k+1)^3 \;\middle|\; \epsilon, k \in \mathbb{Z} \textit{ with } \epsilon \in \{-1, 1\}\right\}$$

and

$$\mathscr{F}_2 = \left\{x^6 + bx^3 + c^3 \;\middle|\; b, c \in \mathbb{Z} \textit{ with } b \equiv 3 \pmod 6 \textit{ and } c \equiv 1 \pmod 6\right\}.$$

If $f(x) \in \mathscr{F}_1$, *then* $\mathrm{Gal}(f) \simeq C_6$, *and if* $f(x) \in \mathscr{F}_2$, *then* $\mathrm{Gal}(f) \simeq C_2 \times S_3$.

Proof. Let $r \in \mathbb{Z}$.

First let $f(x) \in \mathscr{F}_1$. Note that

$$h(r) = r^2 + \epsilon(3k^2+3k+1)r - 3(3k^2+3k+1)^3 \equiv 1 \pmod 2,$$

and thus $h(x)$ is irreducible. Similarly,

$$g(r) = r^3 - 3(3k^2 + 3k + 1)r - \epsilon(3k^2 + 3k + 1) \equiv 1 \pmod 2,$$

and therefore $g(x)$ is irreducible. Hence, $f(x)$ is irreducible by Corollary 3.2. Since

$$\Delta(g) = 81(2k + 1)^2(3k^2 + 3k + 1)^2,$$

it follows from Theorem 4.2 that $\mathrm{Gal}(f) \simeq C_6$.

Now let $f(x) \in \mathscr{F}_2$. As before, both $h(x)$ and $g(x)$ are irreducible since

$$h(r) \equiv g(r) \equiv 1 \pmod 2.$$

Hence, $f(x)$ is irreducible by Corollary 3.2. Since

$$\frac{\Delta(g)}{27} = \frac{108c^3 - 27b^2}{27} = 4c^3 - b^2 \equiv 1 \pmod 3,$$

we see that $\Delta(g)$ is not a square in $\mathbb{Z}$. Therefore, $\mathrm{Gal}(f) \simeq C_2 \times S_3$ by Theorem 4.2.

4.2. The case of Corollary 3.4

Throughout this section, we let

$$\begin{aligned} h(x) &= x^3 + ax^2 + bx - c^2, \\ f(x) &= h(x^2) = x^6 + ax^4 + bx^2 - c^2, \\ g(x) &= x^4 + 2ax^2 - 8cx + a^2 - 4b, \end{aligned} \tag{4.7}$$

where $a, b, c \in \mathbb{Z}$, with $c \neq 0$. Then

$$\Delta(f) = 64c^2\Delta(h)^2 \quad \text{and} \quad \Delta(g) = 2^{12}\Delta(h),$$

where $\Delta(h) = -27c^4 - 18abc^2 + a^2b^2 + 4a^3c^2 - 4b^3$. Observe that

$$\sqrt{\Delta(f)} \in \mathbb{Z} \quad \text{and} \quad \sqrt{\Delta(h)} \in \mathbb{Z} \Longleftrightarrow \sqrt{\Delta(g)} \in \mathbb{Z}. \tag{4.8}$$

The following proposition is an extension of a result in [6].

PROPOSITION 4.4. *Let $h(x) \in \mathbb{Z}[x]$ be a monic cubic polynomial such that $f(x) = h(x^2)$ is irreducible. Then* $\mathrm{Gal}(f) \simeq A_4$ *if and only if $\sqrt{\Delta(f)} \in \mathbb{Z}$ and $\sqrt{\Delta(h)} \in \mathbb{Z}$.*

PROOF. If $\sqrt{\Delta(f)} \in \mathbb{Z}$ and $\sqrt{\Delta(h)} \in \mathbb{Z}$, then $\mathrm{Gal}(f) \simeq A_4$ by Corollary 1.2 in [6]. Conversely, suppose that $\mathrm{Gal}(f) \simeq A_4$. Then $\sqrt{\Delta(g)} \in \mathbb{Z}$ by Theorem 2.4. If $\sqrt{\Delta(h)} \notin \mathbb{Z}$, then we have by Theorem 2.3 that

$$S_3 \simeq \mathrm{Gal}(h) \subset \mathrm{Gal}(f) \simeq A_4,$$

which is impossible, and the proof is complete.

THEOREM 4.5. *Suppose that $f(x)$ is irreducible. Then*

$$\mathrm{Gal}(f) \simeq \begin{cases} S_4, & \text{if } \Delta(g) \text{ is not a square in } \mathbb{Z}, \\ A_4, & \text{if } \Delta(g) \text{ is a square in } \mathbb{Z}. \end{cases}$$

PROOF. The proof is immediate from Proposition 4.4 and (4.8).

Four infinite families of sextic polynomials $f(x)$, with certain conditions on the coefficients of $f(x)$, are given in [6] such that $\mathrm{Gal}(f) \simeq A_4$. Nevertheless, for the sake of completeness, we give here three more sets of pairs of infinite families such that each polynomial in one infinite family in each pair has $\mathrm{Gal}(f) \simeq A_4$, while each polynomial in the second infinite family in each pair has $\mathrm{Gal}(f) \simeq S_4$. These three sets correspond to the three possibilities for the coefficients a and b of $f(x)$ in (4.7):

Case I: $a = 0$ and $b \neq 0$,

Case II: $a \neq 0$ and $b = 0$,

Case III: $a \neq 0$ and $b \neq 0$.

COROLLARY 4.6 (Case I). *Let $\eta = 2 + \sqrt{3}$, the fundamental unit of $\mathbb{Q}(\sqrt{3})$, and for $n \geq 0$, let $k_n = u_n/2$, where $\eta^{2n+1} = u_n + v_n\sqrt{3}$.*

Define

$$\mathscr{F}_1 = \left\{x^6 - 3k_n^2x^2 - k_n^2 \;\middle|\; n \geq 0\right\}$$

and

$$\mathscr{F}_2 = \left\{x^6 - 3m^2x^2 - m^2 \;\middle|\; \text{odd positive } m \in \mathbb{Z}, \text{ with } m \neq k_n \text{ for any } n\right\}.$$

If $f(x) \in \mathscr{F}_1$, then $\mathrm{Gal}(f) \simeq A_4$, and if $f(x) \in \mathscr{F}_2$, then $\mathrm{Gal}(f) \simeq S_4$.

PROOF. First note that, for any integer $c \equiv 1 \pmod 2$, that neither

$$h(x) = x^3 - 3c^2x - c^2 \quad \text{nor} \quad g(x) = x^4 - 8cx + 12c^2$$

has a linear factor since, for any $r \in \mathbb{Z}$,

$$h(r) \equiv 1 \pmod 2 \quad \text{and} \quad g(r) \equiv \begin{cases} 1 \pmod 2, & \text{if } r \equiv 1 \pmod 2, \\ 4 \pmod 8, & \text{if } r \equiv 0 \pmod 2. \end{cases}$$

It is easy to see by induction that $k_n \in \mathbb{Z}$ with $k_n \equiv 1 \pmod 2$. Hence, all polynomials in $\mathscr{F}_1 \cup \mathscr{F}_2$ are irreducible by Corollary 3.4.

Suppose that $f(x) \in \mathscr{F}_1$. Then

$$g(x) = x^4 - 8k_n x + 12k_n^2 = x^4 - 4u_n x + 3u_n^2,$$

and

$$\Delta(g) = 2^8 \cdot 3^3 \cdot u_n^4 \cdot (u_n^2 - 1) = 2^8 \cdot 3^4 \cdot u_n^4 \cdot v_n^2,$$

since $u_n + v_n\sqrt{3}$ is a unit in $\mathbb{Q}(\sqrt{3})$. Thus, by Theorem 4.5, we deduce that $\mathrm{Gal}(f) \simeq A_4$.

Now suppose that $f(x) \in \mathscr{F}_2$. Then $g(x) = x^4 - 8mx + 12m^2$ and

$$\Delta(g) = 2^{12} \cdot 3^3 \cdot m^4 \cdot (4m^2 - 1).$$

If $\sqrt{\Delta(g)} \in \mathbb{Z}$, then $4m^2-1 = 3t^2$ for some $t \in \mathbb{Z}$. But then, $\eta^{2n+1} = 2m+t\sqrt{3}$ for some $n \geq 0$. Thus, $m = k_n$, which contradicts the choice of m. Hence, $\sqrt{\Delta(g)} \notin \mathbb{Z}$, and $\mathrm{Gal}(f) \simeq S_4$ by Theorem 4.5.

Corollary 4.7 (Case II). *Define*

$$\mathscr{F}_1 = \left\{x^6 + (k^2 + k + 7)x^4 - (k^2 + k + 7)^2 \;\middle|\; k \in \mathbb{Z}\right\}$$

and

$$\mathscr{F}_2 = \left\{x^6 + (2k + 1)^2 x^4 - (2k + 1)^2 \;\middle|\; k \in \mathbb{Z}\right\}.$$

If $f(x) \in \mathscr{F}_1$, *then* $\mathrm{Gal}(f) \simeq A_4$, *and if* $f(x) \in \mathscr{F}_2$, *then* $\mathrm{Gal}(f) \simeq S_4$.

Proof. An argument identical to the one used in the proof of Corollary 4.6 shows that all polynomials in $\mathscr{F}_1 \cup \mathscr{F}_2$ are irreducible.

Suppose first that $f(x) \in \mathscr{F}_1$. Then

$$g(x) = x^4 - 8(k^2 + k + 7)^2 x + 4(k^2 + k + 1)^3$$
$$\Delta(g) = 2^{12}(2k + 1)^2(k^2 + k + 7)^8.$$

Thus, $\mathrm{Gal}(f) \simeq A_4$ by Theorem 4.5.

Now let $f(x) \in \mathscr{F}_2$. In this case,

$$\Delta(g) = 2^{12}(64k^4 + 128k^3 + 96k^2 + 32k - 23)(2k + 1)^8.$$

Using the command `IntegralQuarticPoints` in MAGMA, we see that there are no integer points on

$$y^2 = 64k^4 + 128k^3 + 96k^2 + 32k - 23.$$

Thus, $\mathrm{Gal}(f) \simeq S_4$ by Theorem 4.5.

COROLLARY 4.8 (Case III). *Define*

$$\mathscr{F}_1=\left\{x^6+9(2k+1)^2x^4+2(3k+1)(3k+2)(18k^2+18k+5)x^2-(2k+1)^2\right\}$$

and

$$\mathscr{F}_2=\left\{x^6+(2k^2+1)x^4+k^2(k^2+1)x^2-(k^2+1)^2\right\},$$

where $k\in\mathbb{Z}$*. If* $f(x)\in\mathscr{F}_1$*, then* $\mathrm{Gal}(f)\simeq A_4$*, and if* $f(x)\in\mathscr{F}_2$*, then* $\mathrm{Gal}(f)\simeq S_4$.

PROOF. First let $f(x)\in\mathscr{F}_1$. Then

$$\begin{aligned}h(x)&=x^3+9(2k+1)^2x^2\\&\qquad+2(3k+1)(3k+2)(18k^2+18k+5)x-(2k+1)^2\\g(x)&=x^4+18(2k+1)^2x^2-8(2k+1)x+1.\end{aligned}$$

Since $h(r)\equiv 1 \pmod 2$ for any $r\in\mathbb{Z}$, we see that $h(x)$ is irreducible. Since

$$g(-1)=72k^2+88k+28>0 \quad\text{and}\quad g(1)=72k^2+56k+12>0 \quad\text{for all } k,$$

it follows by the Rational Root Test that $g(x)$ has no linear factors, and hence $f(x)$ is irreducible by Corollary 3.4. Since

$$\Delta(g)=2^{12}(108k^4+216k^3+162k^2+54k+7)^2,$$

we conclude that $\mathrm{Gal}(f)\simeq A_4$ by Theorem 4.5.

Now let $f(x)\in\mathscr{F}_2$. Then

$$\begin{aligned}h(x)&=x^3+(2k^2+1)x^2+k^2(k^2+1)x-(k^2+1)^2\\g(x)&=x^4+2(2k^2+1)x^2-8(k^2+1)x+1.\end{aligned}$$

As before, $h(x)$ is irreducible since $h(r)\equiv 1 \pmod 2$ for any $r\in\mathbb{Z}$. Also, $g(x)$ has no linear factors by the Rational Root Test since

$$g(-1)=12k^2+12>0 \quad\text{and}\quad g(1)=-4k^2-4<0 \quad\text{for all } k.$$

Hence, $f(x)$ is irreducible by Corollary 3.4. Since $4k^6+32k^4+48k^2+23>0$ for all k, we have that

$$\Delta(g)=-2^{12}(k^2+1)^2(4k^6+32k^4+48k^2+23)<0 \quad\text{for all } k.$$

Consequently, $\mathrm{Gal}(f)\simeq S_4$ by Theorem 4.5.

5. Summary: the algorithm

Let $f(x)$ be a power compositional sextic polynomial of the form given in either Corollary 3.2 or Corollary 3.4. That is, we have the two cases:

$$\begin{aligned} f(x) &= x^6 + bx^3 + c^3, \\ h(x) &= x^2 + bx + c^3, \\ g(x) &= x^3 - 3cx - b, \end{aligned} \tag{5.1}$$

and

$$\begin{aligned} f(x) &= x^6 + ax^4 + bx^2 - c^2, \\ h(x) &= x^3 + ax^2 + bx - c^2, \\ g(x) &= x^4 + 2ax^2 - 8cx + a^2 - 4b, \end{aligned} \tag{5.2}$$

where $a, b, c \in \mathbb{Z}$, with $c \neq 0$. The algorithm to determine the irreducibility of $f(x)$ and also $\mathrm{Gal}(f)$, when $f(x)$ is irreducible, is described below.

Step 1: Use the Rational Root Test to determine whether $h(x)$ has a rational zero. If $h(x)$ has a rational zero, then $f(x)$ is reducible and the algorithm terminates. If $h(x)$ has no rational zero, then proceed to Step 2.

Step 2: Use the Rational Root Test to determine whether $g(x)$ has a rational zero. If $g(x)$ has a rational zero, then $f(x)$ is reducible and the algorithm terminates. If $g(x)$ has no rational zero, then $f(x)$ is irreducible and proceed to Step 3.

Step 3: Calculate $\Delta(g)$. Then, when $f(x)$ is in (5.1),

$$\mathrm{Gal}(f) \simeq \begin{cases} C_2 \times S_3, & \text{if } \Delta(g) \text{ is not a square in } \mathbb{Z}, \\ C_6, & \text{if } \Delta(g) \text{ is a square in } \mathbb{Z}, \end{cases}$$

and when $f(x)$ is in (5.2),

$$\mathrm{Gal}(f) \simeq \begin{cases} S_4, & \text{if } \Delta(g) \text{ is not a square in } \mathbb{Z}, \\ A_4, & \text{if } \Delta(g) \text{ is a square in } \mathbb{Z}. \end{cases}$$

REFERENCES

1. Bergé, A.-M., Martinet, J., and Olivier, M., *The computation of sextic fields with a quadratic subfield*, Math. Comp. 54 (1990), no. 190, 869–884.

2. Brown, S. C., *On the galois groups of sextic trinomials*, Master's thesis, University of British Columbia, 2011, http://hdl.handle.net/2429/36998.

3. Butler, G., and McKay, J., *The transitive groups of degree up to eleven*, Comm. Algebra 11 (1983), no. 8, 863–911.

4. Cohen, H., *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
5. Eloff, D., Spearman, B. K., and Williams, K. S., *A_4-sextic fields with a power basis*, Missouri J. Math. Sci. 19 (2007), no. 3, 188–194.
6. Ide, J., and Jones, L., *Infinite families of A_4-sextic polynomials*, Canad. Math. Bull. 57 (2014), no. 3, 538–545.
7. Lavallee, M. J., Spearman, B. K., and Williams, K. S., *Lifting monogenic cubic fields to monogenic sextic fields*, Kodai Math. J. 34 (2011), no. 3, 410–425.
8. Olivier, M., *The computation of sextic fields with a cubic subfield and no quadratic subfield*, Math. Comp. 58 (1992), no. 197, 419–432.
9. Schinzel, A., *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000.

DEPARTMENT OF MATHEMATICS
CEDAR CREST COLLEGE
ALLENTOWN
PENNSYLVANIA
USA
E-mail: Joshua.Harrington@cedarcrest.edu

DEPARTMENT OF MATHEMATICS
SHIPPENSBURG UNIVERSITY
PENNSYLVANIA
USA
E-mail: lkjone@ship.edu