Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 27, 2021, No. 2, 172–190
DOI: 10.7546/nntdm.2021.27.2.172-190

Classifying Galois groups of an orthogonal family of quartic polynomials

Pradipto Banerjee[1] **and Ranjan Bera**[2]

[1] Department of Mathematics, Indian Institute of Technology, Hyderabad
Kandi, Telangana 502285, India
e-mail: pradipto.banerjee7@gmail.com

[2] Department of Mathematics, Indian Institute of Technology, Hyderabad
Kandi, Telangana 502285, India
e-mail: ma16resch11002@iith.ac.in

Received: 12 July 2019 **Revised:** 8 November 2020 **Accepted:** 10 March 2021

Abstract: We consider the quartic generalized Laguerre polynomials $L_4^{(\alpha)}(x)$ for $\alpha \in \mathbb{Q}$. It is shown that except $\mathbb{Z}/4\mathbb{Z}$, every transitive subgroup of S_4 appears as the Galois group of $L_4^{(\alpha)}(x)$ for infinitely many $\alpha \in \mathbb{Q}$. A precise characterization of $\alpha \in \mathbb{Q}$ is obtained for each of these occurrences. Our methods involve the standard use of resolvent cubics and the theory of p-adic Newton polygons. Using these, the Galois group computations are reduced to Diophantine problem of finding integer and rational points on certain curves.

Keywords: Galois groups, Quartic polynomials, Generalized Laguerre polynomials, Newton polygons, Diophantine equations.
2020 Mathematics Subject Classification: 11R32 (primary); 11C08, 33C45 (secondary).

1 Introduction

Computing Galois groups of polynomials with rational coefficients is a classical problem in algebra. By Galois group of a polynomial $f(x) \in \mathbb{Q}[x]$, we refer to the Galois group of the splitting field of $f(x)$ over the rationals. We will denote the Galois group of $f(x)$ by $\mathrm{Gal}(f)$. Broadly speaking, there are no known algorithms to compute the Galois group of a given but arbitrary polynomial. Among exceptions are polynomials of degree ≤ 4. In theory, given a polynomial in $\mathbb{Q}[x]$ of degree ≤ 4, it is possible to determine its Galois group (for example, many mathematics software systems can do this job). But it is not always an entirely trivial task to compute the Galois groups of a family of polynomials of a fixed degree ≤ 4. In this article, we consider generalized Laguerre polynomials $L_n^{(\alpha)}(x)$ for $n \leq 4$ and $\alpha \in \mathbb{Q}$. These are defined as

$$L_n^{(\alpha)}(x) = (-1)^n \sum_{j=0}^{n} (-1)^j \binom{n+\alpha}{n-j} \frac{x^j}{j!}.$$

This family of polynomials are widely studied in mathematical physics and quantum mechanics. An interest in the algebraic aspects of these polynomials was initiated by Schur [9–11] who made use of these polynomials to resolve the inverse Galois problem for the symmetric and alternating group. His results are summarized below.

- $L_n^{(0)}(x)$ has Galois group S_n for each n.
- $L_n^{(1)}(x)$ has Galois group S_n for each even n with $n+1$ not a square.
- $L_n^{(1)}(x)$ has Galois group A_n for each odd n and each even n with $n+1$ a square.
- $L_n^{(-n-1)}(x)$ has Galois group S_n for each $n \not\equiv 0 \pmod 4$.
- $L_n^{(-n-1)}(x)$ has Galois group A_n for each $n \equiv 0 \pmod 4$.

Since the work of Schur, the algebraic aspects of generalized Laguerre polynomials have received much attention in the recent years. We refer the interested reader to [1] and the references therein.

The case $n = 4$, in some sense, is more interesting than others. In [7], Hajir and Wong showed that if $n \geq 5$ is fixed, then the Galois group of $L_n^{(\alpha)}(x)$ contains A_n, the alternating group on n letters, for all but finitely many $\alpha \in \mathbb{Q}$ (depending on n). On the other hand, Hajir [6] exhibits infinitely many $\alpha \in \mathbb{Q}$ such that $L_4^{(\alpha)}(x)$ has the associated Galois group the Dihedral group D_4 (hence, the Galois group does not contain A_4). Our main motivation was to investigate whether there are other transitive subgroups of S_4, the symmetric group on 4 letters, which appear as the Galois group of $L_4^{(\alpha)}(x)$ infinitely often. It turns out that such examples indeed exist and are plentiful.

This article, in a way, complements the results of [1, 2, 6]. In [1], the Galois properties of $L_n^{(\alpha)}(x)$ for $n \leq 4$ and $\alpha \in \mathbb{Z}$ are addressed. Obviously, one would want to extend these results to $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$. In [2], the first author obtained precise descriptions of the pairs (n, α) with $n \leq 4$ and $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$ such that the discriminant of $L_n^{(\alpha)}(x)$ is the square of a nonzero rational number. In [6], Hajir established the irreducibility of $L_4^{(\alpha)}(x)$ for all $\alpha \in \mathbb{Q}\backslash\{-1, 23\}$. Thus, one is naturally intrigued to know whether $\mathrm{Gal}(L_4^{(\alpha)})$ is Klein's four group V_4 or A_4 in the case that the discrimiant of $L_4^{(\alpha)}(x)$ is a nonzero rational square.

For $n \leq 3$, the situation is not as exciting. We briefly discuss them here, omitting some of the details. The polynomial $\mathcal{L}_2^{(\alpha)}(x) = 2!L_2^{(\alpha)}(x)$ is given by

$$\mathcal{L}_2^{(\alpha)}(x) = x^2 - 2(\alpha+2)x + (\alpha+2)(\alpha+1).$$

Its discriminant is $4(\alpha+2)$. Thus, the Galois group of $\mathcal{L}_2^{(\alpha)}(x)$ is trivial if and only if $\alpha+2$ is the square of a rational number. Otherwise, it is $\mathbb{Z}/2\mathbb{Z}$.

Now consider the case that $n = 3$. It is well known that the Galois group of a cubic polynomial in $\mathbb{Q}[x]$ contains A_3 if and only if the polynomial is irreducible.

Irreducibility here, and throughout, refers to the irreducibility over the rationals. The polynomial $\mathcal{L}_3^{(\alpha)}(x) = -3!L_3^{(\alpha)}(x)$ is given by

$$\mathcal{L}_3^{(\alpha)}(x) = x^3 - 3(\alpha+3)x^2 + 3(\alpha+3)(\alpha+2)x - (\alpha+3)(\alpha+2)(\alpha+1).$$

After killing the trace term by considering instead the polynomial $g(x) = \mathcal{L}_3^{(\alpha)}(x+\alpha+3)$, we have $g(x) = x^3 - 3(\alpha+3)x - 2(\alpha+3)$. It is easy to see that $g(x)$ is reducible over the rationals if and only if

$$\alpha = \frac{\gamma^3 - 9\gamma - 6}{3\gamma + 2}, \quad \gamma \in \mathbb{Q}\backslash\{-2/3\}. \tag{1}$$

Thus, there are essentially a couple of things to address here. First, if α is not in the form (1), then is it possible to precisely describe the instances where $\mathcal{L}_3^{(\alpha)}(x)$ has the associated Galois group A_3 or S_3. Second, in the case that α satisfy (1), under what circumstances does $\mathcal{L}_3^{(\alpha)}(x)$ split completely over the rationals. That is, for which α satisfying (1), is $\mathrm{Gal}(\mathcal{L}_3^{(\alpha)})$ the trivial group?

In order to answer the first question, we need precise information on whether the discriminant $\mathrm{Discr}(\mathcal{L}_3^{(\alpha)})$ of $\mathcal{L}_3^{(\alpha)}(x)$ is a nonzero rational square. Let us denote by $\square$ the square of an unspecified nonzero rational number. The cases where $\mathrm{Discr}(\mathcal{L}_n^{(\alpha)}) = \square$ for $n \leq 5$ and $\alpha \in \mathbb{Z}$ has already been studied in [1]. The main result in [1] states that if $n \leq 5$, $\alpha \in \mathbb{Z}$ and $\mathrm{Discr}(\mathcal{L}_n^{(\alpha)}) = \square$, then $\mathrm{Gal}(\mathcal{L}_n^{(\alpha)}) = A_n$ unless $(n, \alpha) \in \{(4,-1),(4,23)\}$. Furthermore, $\mathrm{Gal}(\mathcal{L}_4^{(-1)}) = A_3 = \mathrm{Gal}(\mathcal{L}_4^{(23)})$. A precise description of $n \leq 5$ and $\alpha \in \mathbb{Z}$ for which $\mathrm{Discr}(\mathcal{L}_n^{(\alpha)}) = \square$ was obtained in [3].

Thus, in this article, we will be interested in the cases that $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$ whenever $\mathrm{Discr}(\mathcal{L}_n^{(\alpha)}) = \square$. Using a formula of Schur [11] for $\mathrm{Discr}(\mathcal{L}_n^{(\alpha)})$, the first author [2] has described the instances where $\mathrm{Discr}(\mathcal{L}_n^{(\alpha)}) = \square$ for $n \leq 5$ and $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$. It follows from [2] that $\mathrm{Discr}(\mathcal{L}_3^{(\alpha)}) = \square$ if and only if α satisfies one of following 2 conditions. We label this list as $\mathcal{B}_3$. The letters u and v below, represent a pair of relatively prime integers.

(i) $\alpha = (3u^2 - 2v^2)/v^2$ where $v \not\equiv 0 \pmod 3$ and $v \geq 2$,

(ii) $\alpha = (u^2 - 6v^2)/3v^2$ where $u \not\equiv 0 \pmod 3$.

Thus, $\mathrm{Gal}(\mathcal{L}_3^{(\alpha)}) = A_3$ for all α satisfying (i) or (ii) of $\mathcal{B}_3$ above, as long as α is not of the form (1). In fact, it is possible to precisely describe such α. For example, suppose that α satisfies both (i) of $\mathcal{B}_3$ and (1). Writing $u/v = \beta$, we find that $(X, Y) = (\gamma, \beta)$ is a rational point on the curve

$$Y^2/3 - 2 = X^3/(3X+2) - 3; \quad X \neq -2/3. \tag{2}$$

Rewriting (2), we have

$$Y^2 = \frac{3(X+1)^2(X-2)}{3X+2}. \tag{3}$$

Since, only $\alpha \in \mathbb{Q}/\mathbb{Z}$ are being considered here, we may discard the solution $(X, Y) = (-1, 0)$. Thus, (3) can be expressed as

$$\frac{3X-6}{3X+2} = \frac{Y^2}{(X+1)^2}. \tag{4}$$

Set $Y/(X+1) = T$. Since $T = \pm 1$ do not yield any admissible solution of (4), we may suppose that $T^2 \neq 1$. We further restrict ourselves to the nonzero values of T as $\beta \neq 0$. Solving for X in (4) in terms of T, we obtain

$$X = \frac{2(3+T^2)}{3(1-T^2)}.$$

Thus, the curve (2) is parametrized by T as

$$X = \frac{2(3+T^2)}{3(1-T^2)}, \quad Y = T(X+1) = \frac{T(9-T^2)}{3(1-T^2)}.$$

Now, substituting γ in (1) by the value of X obtained above, we get that

$$\alpha = \frac{T^6 - 72T^4 + 189T^2 - 54}{27(T^4 - 2T^2 + 1)}; \quad T \in \mathbb{Q}/\{0, \pm 1\}.$$

Indeed, for α as above, a quick verification with Sage (mathematics software system) yields that the polynomial $\mathcal{L}_3^{(\alpha)}(x + \alpha + 3)$ factors over $\mathbb{Q}$ as

$$(27(T^2-1)^2)^{-1}((3T-1)x - T^2 - 3)((3T+1)x + 3T^2 + 1)(3(T^2-1)x + 2T^2 + 6).$$

That is, $\mathcal{L}_3^{(\alpha)}(x)$ factors completely into linear factors, and hence, has the trivial Galois group. Thus, setting $T = a/b$ where a and b are mutually coprime integers, we find that $\mathcal{L}_3^{(\alpha)}(x)$ factors into linear factors if and only if

$$\alpha = \frac{a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6}{27b^2(a^2-b^2)^2}; \quad a, b \in \mathbb{Z}\backslash\{0\}, \ \gcd(a,b) = 1.$$

After comparing with (i) in $\mathcal{B}_3$, we deduce that

$$3v^2 = 27\lambda^2b^2(a^2-b^2)^2 \quad \text{and} \quad u^2 - 6v^2 = \lambda^2(a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6),$$

where $\lambda \in \mathbb{Q}$ is such that the values of the integers u and v thus obtained are relatively prime. Solving for u and v above, we obtain

$$u = \pm a\lambda(a^2 - 9b^2) \quad \text{and} \quad v = \pm 3\lambda b(a^2 - b^2).$$

Since $\gcd(u,v) = 1$, we deduce that λ is of the form $1/\mu$ where $\mu \in \mathbb{Z}\backslash\{0\}$. Note that, for relatively prime integers a and b we have

$$\gcd(a, a^2 - b^2) = \gcd(b, a^2 - 9b^2) = \gcd(a,b) = 1,$$

and

$$\gcd(a^2 - b^2, a^2 - 9b^2) = \begin{cases} 1 & \text{if} \quad a \not\equiv b \pmod 2, \\ 8 & \text{if} \quad a \equiv b \pmod 2. \end{cases}$$

Thus, if a and b have the same parity, then $\mu \equiv 0 \pmod 8$, and μ is odd otherwise. Also, if $3 \mid a$, then we must have that $\mu \equiv 0 \pmod 3$. For relatively prime integers a and b, define

$$\mu(a,b) = \begin{cases} 1 & \text{if} \quad a \not\equiv b \pmod 2, \ 3 \nmid a, \\ 3 & \text{if} \quad a \not\equiv b \pmod 2, \ 3 \mid a, \\ 8 & \text{if} \quad a \equiv b \pmod 2, \ 3 \nmid a, \\ 24 & \text{if} \quad a \equiv b \pmod 2, \ 3 \mid a. \end{cases}$$

Considering various possibilities depending on the parities of a and b and whether $3 \mid a$ or not, we obtain that $\mathrm{Gal}(\mathcal{L}_3^{(\alpha)}) = A_3$ as long as α satisfies (i) of $\mathcal{B}_3$ where

$$(u,v) \notin \left\{ \frac{\pm a(a^2 - 9b^2)}{\mu(a,b)}, \frac{\pm 3b(a^2 - b^2)}{\mu(a,b)} : a, b \in \mathbb{Z}, \gcd(a,b) = 1 \right\}.$$

In the event that $(3,\alpha)$ satisfies (ii) in our list $\mathcal{B}_3$, we find that $\alpha = 3\beta^2 - 2$, where β is as defined in the preceding case. Working in a similar manner as in the previous case, we deduce that a reducible $\mathcal{L}_3^{(\alpha)}(x)$ in this case, with $\Delta(3,\alpha) = \Box$, corresponds to a pair of integral points $(X, \pm Y)$ on the curve

$$3Y^2 - 2 = X^3/(3X+2) - 3. \tag{5}$$

Rewriting (5), we have

$$Y^2 = \frac{(X+1)^2(X-2)}{3(3X+2)}; \quad x \neq -2/3.$$

As before, we set $T = Y/(X+1)$ and obtain $X = (6T^2+2)/(1-9T^2)$. Here, we suppose, as we may, that $T \notin \{0, \pm 1/3\}$ ($T = 0$ corresponds to $\alpha = -2$, an integer, and, $T = \pm 1/3$ do not yield a solution of (5)). Thus, in this case, we find that

$$\alpha = \frac{27T^6 - 216T^4 + 63T^2 - 2}{81T^4 - 18T^2 + 1}; \quad T \in \mathbb{Q}/\{0, \pm 1/3\}.$$

We verified (using sage) that $\mathcal{L}_3^{(\alpha)}(x + \alpha + 3)$ factors as

$$(9T^2-1)^{-2}((3T-1)x - 3T^2 - 1)((3T+1)x + 3T^2 + 1)((9T^2-1)x + 6T^2 + 2).$$

Thus, by setting $T = a/b$ where a and b are relatively prime integers, we have

$$\alpha = \frac{27a^6 - 216a^4b^2 + 63a^2b^4 - 2b^6}{b^2(9a^2-b^2)^2}; \quad a, b \in \mathbb{Z}\backslash\{0\}, \ \gcd(a,b) = 1.$$

After comparing and solving for u and v, we obtain

$$u = \pm 3\lambda b(a^2 - b^2) \quad \text{and} \quad v = \pm a\lambda(9a^2 - b^2).$$

Now, working similarly as in the preceding case, we get that $\mathrm{Gal}(\mathcal{L}_3^{(\alpha)}) = A_3$ as long as α satisfies (ii) of $\mathcal{B}_3$, provided

$$(u,v) \notin \left\{ \frac{\pm 3b(a^2-b^2)}{\mu(a,b)}, \frac{\pm a(a^2-9b^2)}{\mu(a,b)} : a, b \in \mathbb{Z}, \gcd(a,b) = 1 \right\}.$$

It is clear that if α does not satisfy (i) or (ii) of $\mathcal{B}_3$ and is not in the form (1), then the Galois group of $\mathcal{L}_3^{(\alpha)}(x)$ is S_3.

Now we turn to the second question, namely, classify $\alpha \in \mathbb{Q}$ for which $\mathcal{L}_3^{(\alpha)}(x)$ splits completely over the rationals. In this case, α satisfies (1). One readily checks that

$$\mathcal{L}_3^{(\alpha)}(x + \alpha + 3) = (x - \gamma)(x^2 + \gamma x + 2\gamma^2/(3\gamma + 2)).$$

Thus, $\mathcal{L}_3^{(\alpha)}(x)$ splits completely over the rationals if and only if the discriminant of the quadratic polynomial appearing in the last display above is a rational square. That is, $\mathcal{L}_3^{(\alpha)}(x)$ splits completely over the rationals if and only if

$$\gamma^2 - 8\gamma^2/(3\gamma+2) = \Box.$$

After simplifying, we find that $\gamma - 2/3$ is the abscissa of a $\mathbb{Q}$-rational point on the hyperbola

$$x^2 - y^2 = 16/9.$$

Using the $\mathbb{Q}$-rational point $(4/3, 0)$ on the hyperbola, one can find all other $\mathbb{Q}$-rational points on this curve by the standard chord-slope parametrization. Thus, γ can be given as

$$\gamma = \frac{4}{3} + \frac{2}{3} = 2 \quad \text{or} \quad \gamma = \frac{-4(1+m^2)}{3(1-m^2)} + \frac{2}{3} = \frac{-2(1+3m^2)}{3(1-m^2)}, \quad m \neq \pm 1.$$

This settles the case that $n = 3$.

Before proceeding further, we would like to note that for every integer $n \geq 1$ and $-n \leq \alpha < 0$, there is a trivial factorization of $\mathcal{L}_n^{(\alpha)}(x)$. Namely, for any such α, we have (see (1.2) in [6])

$$\mathcal{L}_n^{(\alpha)}(x) = x^{-\alpha}\mathcal{L}_{n+\alpha}^{(-\alpha)}(x). \tag{6}$$

In order to streamline our presentation, we treat these cases separately. For each integer $n \geq 1$, we let $\mathcal{E}_n = \mathbb{Z} \cap [-n, 0)$. Thus, we have $\mathcal{E}_4 = \{-1, -2, -3, -4\}$. Furthermore, from (6), it follows that for $\alpha \in \mathcal{E}_n$, the polynomials $\mathcal{L}_n^{(\alpha)}(x)$ and $\mathcal{L}_{n+\alpha}^{(-\alpha)}(x)$, have the same Galois group. Thus, $\mathrm{Gal}(\mathcal{L}_4^{(-1)}) = \mathrm{Gal}(\mathcal{L}_3^{(1)}) = A_3$ (by [11]). It is easy to check that the Galois groups in the remaining cases are trivial. Henceforth, we will only consider $\alpha \in \mathbb{Q}\backslash\mathcal{E}_4$.

The case that $n = 4$ and $\alpha \in \mathbb{Q}\backslash\mathcal{E}_4$ entails a much finer analysis. The polynomial $\mathcal{L}_4^{(\alpha)}(x) = 4!L_4^{(\alpha)}(x)$ is given by

$$\begin{aligned}\mathcal{L}_4^{(\alpha)}(x) = x^4 &- 4(\alpha+4)x^3 + 6(\alpha+4)(\alpha+3)x^2 \\ &- 4(\alpha+4)(\alpha+3)(\alpha+2)x + (\alpha+4)(\alpha+3)(\alpha+2)(\alpha+1).\end{aligned}$$

Hajir [6] has established that besides the trivial factorization (6), $\mathcal{L}_4^{(\alpha)}(x)$ is reducible if and only if $\alpha = 23$. One easily checks (we used Sage) that $\mathrm{Gal}(\mathcal{L}_4^{(23)}) = A_3$. By abuse of notation, we shall denote $\mathcal{E}_4 \cup \{23\}$ by $\mathcal{E}_4$.

We split our analysis into two cases, depending on whether the discriminant of $\mathcal{L}_4^{(\alpha)}(x)$ is the square of a rational number or not. As stated earlier, the Galois groups in the cases, where $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \square$ and $\alpha \in \mathbb{Z}$, are already addressed in [1]. Therefore, we will only consider $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$ whenever $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \square$. For $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$, we have from [2] that $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \square$ if and only if α satisfies one of the following 4 conditions. We label this list as $\mathcal{B}_4$. Below, u and v represent a pair of relatively prime integers and k is an integer.

(i) $\alpha = -2(u^2 - 6v^2)/(u^2 - 3v^2)$ where $u \not\equiv v \pmod 2$, $3 \nmid u$ and $u + v\sqrt{3} \neq \pm(2+\sqrt{3})^k$

(ii) $\alpha = -2(2u^2 - 3v^2)/(u^2 - 3v^2)$ where $u \not\equiv v \pmod 2$, $3 \nmid u$ and $u + v\sqrt{3} \neq \pm(2+\sqrt{3})^k$

(iii) $\alpha = -(u^2 + v^2 + 10uv)/(u^2 + v^2 + 4uv)$ where $u \not\equiv v \pmod 2$, $u \not\equiv v \pmod 3$ and $u + 2v + v\sqrt{3} \neq \pm(2+\sqrt{3})^k$

(iv) $\alpha = -(5u^2 + 5v^2 + 14uv)/(u^2 + v^2 + 4uv)$ where $u \not\equiv v \pmod 2$, $u \not\equiv v \pmod 3$ and $u + 2v + v\sqrt{3} \neq \pm(2+\sqrt{3})^k$

Without loss of any generality, we can assume that the integers u and v above are positive, and as such, we do so throughout. A Galois group of $\mathcal{L}_4^{(\alpha)}(x)$, different from S_4, A_4 and D_4, arises for α satisfying (i) or (ii) of $\mathcal{B}_4$ and some additional conditions. These are classified in the following.

Theorem 1.1. *Let $\alpha \in \mathbb{Q}\backslash\mathcal{E}_4$ satisfy one of (i)–(iv) in $\mathcal{B}_4$. Then the Galois group associated with $\mathcal{L}_4^{(\alpha)}(x)$ is the Klein four group V_4 if and only if one of the following holds.*

(a) α satisfies (i) or (ii) in $\mathcal{B}_4$, and additionally, there are integers a and b with $\gcd(a,b) \leq 2$ and $a \equiv b \pmod 2$ such that

$$u = \pm a(a^2 - 9b^2)/8 \quad \textit{and} \quad v = \pm 3b(a^2 - b^2)/8.$$

(b) *α satisfies (iii) or (iv) in $\mathcal{B}_4$, and additionally, there are integers a and b with* $\gcd(a,b) \leq 2$ *and* $a \equiv b \pmod 2$ *such that*

$$u = \frac{\pm 3b(a^2 - b^2 \pm a(a^2 - 9b^2))}{8} \quad \textit{and} \quad v = \frac{\pm 3b(a^2 - b^2 \mp a(a^2 - 9b^2))}{8}.$$

The Galois group is A_4 otherwise.

If α is not as in (i)–(iv) of $\mathcal{B}_4$, then we have the following.

Theorem 1.2. *Suppose $\alpha \in \mathbb{Q} \backslash \mathcal{E}_4$ does not satisfy (i)–(iv) of $\mathcal{B}_4$. Let $\mathcal{A}$ be the set of elements of the form*

$$-\frac{3\lambda^3 + 18\varepsilon\lambda^2 - 64\varepsilon}{\lambda^3 + 6\varepsilon\lambda^2 - 16\varepsilon}, \quad \lambda \neq -2\varepsilon, \quad \varepsilon \in \{\pm 1\}, \quad \lambda \in \mathbb{Q}.$$

Then for $\alpha \in \mathcal{A}$, the Galois group of $\mathcal{L}_4^{(\alpha)}(x)$ is D_4. The Galois group is S_4 if $\alpha \notin \mathcal{A}$.

In the proofs of Theorems 1.1 and 1.2, we make use of the resolvent cubics. It is well known that the Galois group of an irreducible quartic polynomial contains A_4 if and only if its resolvent cubic is irreducible. As stated before, Hajir [6] has established that $\mathcal{L}_4^{(\alpha)}(x)$ is irreducible for all $\alpha \in \mathbb{Q} \backslash \mathcal{E}_4$. Thus, our work here boils down to studying the factorization of the resolvent cubic of $\mathcal{L}_4^{(\alpha)}(x)$. This is done by parametrizing the factors of the resolvent cubic by integer (or rational) points on certain curves. The factorization problem then reduces to a Diophantine problem.

In order to parametrize the factors of the resolvent cubic of $\mathcal{L}_4^{(\alpha)}(x)$ in Theorem 1.1, we will make use of the theory of Newton polygons which we briefly describe here.

Let p be a prime, and s and r be integers relatively prime to p. If m is a nonzero number and a is an integer such that $m = p^a \frac{s}{r}$, we define $\nu(m) = \nu_p(m) = a$. By convention, we take $\nu(0) = +\infty$. Consider $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Q}[x]$ with $a_n a_0 \neq 0$, and let p be a prime. Let S be the set of points in the extended plane given by

$$S = \{(0, \nu(a_n)), (1, \nu(a_{n-1})), (2, \nu(a_{n-2})), \cdots, (n-1, \nu(a_1)), (n, \nu(a_0))\}.$$

Consider the lower edges along the convex hull of these points. The left-most endpoint is $(0, \nu(a_n))$, and the right-most endpoint is $(n, \nu(a_0))$. The endpoints of all the edges belong to S, and the slopes of the edges increase from left to right. The polygonal path formed by these edges is called the Newton polygon of $f(x)$ with respect to the prime p, and we will denote it by $NP_p(f)$. The celebrated theorem of Dumas [5] provides an effective tool to study the irreducibility aspects of polynomials over the rationals.

Theorem 1.3 (Dumas)**.** Let p be a prime and $h_1(x)$, $h_2(x) \in \mathbb{Z}[x]$ with $h_1(0)h_2(0) \neq 0$. Also, let $a \neq 0$ be the leading coefficient of $h_1(x)h_2(x)$ with $\nu_p(a) = k$. Then the edges of the Newton polygon of $h_1(x)h_2(x)$ with respect to p can be formed by constructing a polygonal path beginning with $(0, k)$ and using translates of edges of Newton polygons of $h_1(x)$ and $h_2(x)$ with respect to p (using exactly one translate for each edge). Necessarily, the edges are translated in such a way as to form a polygonal path with slopes of edges increasing from left to right.

Thus, if a polynomial $f(x)$ with integer coefficients factors in $\mathbb{Z}[x]$ into irreducible polynomials of degrees ≥ 1, then Theorem 1.3 tells us that for any prime p and a factor $h(x) \in \mathbb{Z}[x]$ of $f(x)$, a translate of every edge of $NP_p(h)$ lies on some edge of $NP_p(f)$. Thus, in particular, if for some prime p, there are no lattice points on $NP_p(f)$, other than endpoints, then $f(x)$ is irreducible. We will often exploit this fact in our proof.

2 The proofs of Theorems 1.1 and 1.2

We begin with the proof of Theorem 1.1. Thus, we are interested in computing the Galois group of

$$\begin{aligned} f(x) = \mathcal{L}_4^{(\alpha)}(x) = x^4 &- 4(\alpha+4)x^3 + 6(\alpha+4)(\alpha+3)x^2 \\ &- 4(\alpha+4)(\alpha+3)(\alpha+2)x \\ &+ (\alpha+4)(\alpha+3)(\alpha+2)(\alpha+1), \end{aligned}$$

where $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$ and satisfies $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \square$. Recall that $\mathcal{L}_4^{(\alpha)}(x)$ is irreducible for all α under consideration. By the discriminant formula of Schur [11], we have that

$$\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \prod_{j=2}^{4} j^j(\alpha+j)^{j-1}.$$

Thus, $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \square$ if and only if

$$3(\alpha+2)(\alpha+4) = \square.$$

We set $\alpha = s/t$ and rewrite the last equation as

$$(s+2t)(s+4t) = 3m^2, \quad m \in \mathbb{Z}\backslash\{0\}. \tag{7}$$

Since $\gcd(s,t) = 1$, we deduce that $\gcd(s+2t, s+4t) = 2$ if s is even, and $\gcd(s+2t, s+4t) = 1$, otherwise. After considering various possibilities, we deduce from (7) and the fundamental theorem of arithmetic that there are relatively prime integers y_1 and y_2 such that the pair $(s+2t, s+4t)$ has one of the following representations. If s is odd, then

$$\begin{aligned} (s+2t, s+4t) \in \{(3y_1^2, y_2^2), (y_1^2, 3y_2^2), (-3y_1^2, -y_2^2), (-y_1^2, -3y_2^2)\}; \\ y_1 \equiv y_2 \equiv 1 \pmod 2, \end{aligned}$$

and for even s, we have

$$\begin{aligned} (s+2t, s+4t) \in \{(6y_1^2, 2y_2^2), (2y_1^2, 6y_2^2), (-6y_1^2, -2y_2^2), (-2y_1^2, -6y_2^2)\}; \\ y_1 \not\equiv y_2 \pmod 2. \end{aligned}$$

For convenience, we will work with the translated polynomial $g(x) = \mathcal{L}_4^{(\alpha)}(x+\alpha+4)$. Thus

$$g(x) = x^4 - 6(\alpha+4)x^2 - 8(\alpha+4)x + 3(\alpha+4)(\alpha+2).$$

For a monic quartic polynomial $h(x) = x^4 + ax^3 + bx^2 + cx + d$, having roots t_1, t_2, t_3 and t_4, its resolvent cubic $R_h(x)$ is defined as the cubic whose roots are $t_1t_2+t_3t_4$, $t_1t_3+t_2t_4$ and $t_1t_4+t_2t_3$. It can be verified (see [8] for instance) that $h(x)$ and $R_h(x)$ have the same discriminant and that for the given quartic $h(x)$, $R_h(x)$ can be expressed as

$$R_h(x) = x^3 - bx^2 + (ac-4d)x - a^2d - 4bd + c^2.$$

The factorization of resolvent cubics of irreducible quartics completely determine their Galois groups. We refer to the following result from [8].

Theorem 2.1 (Kappe–Warren)**.** Let $F(x) = x^4 + ax^3 + bx^2 + cx + d$ be an irreducible quartic polynomial in $\mathbb{Q}[x]$, and let $R_F(x)$ be its resolvent cubic. Let K denote the splitting field of $R_F(x)$ over $\mathbb{Q}$. Then, we have the following.

(i) $\operatorname{Gal}(F) = S_4$ if and only if $R_F(x)$ is irreducible and $\operatorname{Discr}(F) \notin \mathbb{Q}^2$.

(ii) $\operatorname{Gal}(F) = A_4$ if and only if $R_F(x)$ is irreducible and $\operatorname{Discr}(F) \in \mathbb{Q}^2$.

(iii) $\operatorname{Gal}(F) = V_4$ if and only if $R_F(x)$ splits into product of linear factors over $\mathbb{Q}$.

(iv) $\operatorname{Gal}(F) = \mathbb{Z}/4\mathbb{Z}$ if and only if $R_F(x)$ has exactly one root A in $\mathbb{Q}$ and $G(x) = (x^2 - Ax + d)(x^2 + ax + b - A)$ splits over K.

(v) $\operatorname{Gal}(F) = D_4$ if and only if $R_F(x)$ has exactly one root A in $\mathbb{Q}$ and $G(x)$ (defined in (iv)) does not split over K.

We have

$$R_g(x) = x^3 + 6(\alpha+4)x^2 - 12(\alpha+4)(\alpha+2)x - 72(\alpha+4)^2(\alpha+2) - 64(\alpha+4)^2.$$

Instead of $R_g(x)$, we will work with the cubic $R_1(x) = R_g(2x - 2\alpha - 8)/8$, which in our case is given by

$$R_1(x) = x^3 - 6(\alpha+4)(\alpha+3)x - 4(\alpha+4)^2(\alpha+3).$$

Writing $\alpha = s/t$, and setting $R_2(x) = t^3 R_1(x/t)$, we have

$$R_2(x) = x^3 - 6(s+3t)(s+4t)x - 4(s+3t)(s+4t)^2.$$

Observe that, if $p \neq 2$ is any prime divisor of $s + 3t$, then the Newton polygon $N_p(R_2)$ has only one edge, that joining the terminal points $(0,0)$ and $(3, \nu_p(s+3t))$. By appealing to Theorem 1.3, we deduce that if $R_2(x)$ is reducible over the rationals, then

$$\nu_p(s+3t) \equiv 0 \pmod 3 \quad \text{for all} \quad p|(s+3t), p \neq 2.$$

Thus, in order for $R_2(x)$ to be reducible, $s + 3t$ is in one of the forms in the set $\{z_1^3, 2z_1^3, 4z_1^3\}$ for some $z_1 \in \mathbb{Z}$. Therefore, if $R_2(x)$ is reducible over the rationals and $\operatorname{Discr}(\mathcal{L}_4^{(\alpha)})$ is a nonzero rational square, then from the description of $s + 2t$, $s + 3t$ and $s + 4t$, and the identity $(s + 2t) + (s + 4t) = 2(s + 3t)$, we deduce that

$$(Z, Y_1, Y_2) \in \{(z_1, y_1, y_2), (z_1, y_2, y_1), (-z_1, y_1, y_2), (-z_1, y_2, y_1)\}$$

is an integer solution of

$$2\ell Z^3 = Y_1^2 + 3Y_2^2; \quad \ell \in \{1, 2, 4\} \quad \text{if} \quad s \equiv 1 \pmod 2, \tag{8}$$

or

$$\ell Z^3 = Y_1^2 + 3Y_2^2; \quad \ell \in \{1, 2, 4\} \quad \text{if} \quad s \equiv 0 \pmod 2. \tag{9}$$

Thus, we will be interested in finding integral points on the curves given by (8) and (9).

Recall that for odd s, we have $Y_1 \equiv Y_2 \equiv 1 \pmod 2$ so that, the right hand side of (8) is congruent to $4 \pmod 8$. Thus, for (8) to have an integral solution, Z must be odd, and hence, it follows that $\ell = 2$. Accordingly, we rewrite (8) as

$$4Z^3 = Y_1^2 + 3Y_2^2; \quad Z \equiv Y_1 \equiv Y_2 \equiv 1 \pmod 2. \tag{10}$$

If s is even, then from $\gcd(s,t)=1$, we find that $s+3t$ is odd, and hence, $Z\equiv 1 \pmod 2$. Recall that $Y_1 \not\equiv Y_2 \pmod 2$ in this case. As such, it follows that $\ell=1$. Thus (9) can be expressed as

$$Z^3 = Y_1^2+3Y_2^2; \quad Z\equiv 1 \pmod 2, \quad Y_1\not\equiv Y_2 \pmod 2. \tag{11}$$

We first show that solutions of (10) do not yield any reducible $R_2(x)$. Observe that, corresponding to integral solutions of (10), we have $(s+3t, s+4t) = (2\varepsilon z_1^3, \varepsilon m y_2^2)$ where $\varepsilon\in\{1,-1\}$, $m\in\{1,3\}$ and z_1, y_2 are odd integers. Instead of $R_2(x)$, we consider the polynomial $R_3(x)=R_2(z_1y_2x)/z_1^3y_2^3$. Thus,

$$R_3(x)=x^3-12mz_1x-8\varepsilon m^2y_2.$$

Since m, z_1 and y_2 are odd, the Newton polygon $NP_2(R_3)$ of $R_3(x)$ with respect to 2, has just one edge, that joining $(0,0)$ and $(3,3)$. Now, if $R_3(x)$ is reducible, then being a monic cubic with integer coefficients, it has an integer root a. From Theorem 1.3, we find that $NP_2(x-a)$ has just one edge, joining $(0,0)$ and $(1,1)$. This, in other words, means that 2 exactly divides the integer a, that is, $a=2a_1$ for some odd integer a_1. Now, from the relation $R_3(2a_1)/8=0$, we find that

$$a_1^3-3mz_1a_1-\varepsilon m^2y_2=0.$$

But this is a contradiction as an odd number of terms above are odd. This proves our claim.

Corresponding to integral solutions of (11), we have $(s+3t, s+4t)=(\varepsilon z_1^3, 2\varepsilon m y_2^2)$ for some $\varepsilon\in\{1,-1\}$, $m\in\{1,3\}$, where z_1 is an odd integer. Similarly to the previous case, we consider the reducibility of the polynomial $R_3(x)=R_2(z_1y_2x)/z_1^3y_2^3$ which, in this case, is given by

$$R_3(x)=x^3-12mz_1x-16\varepsilon m^2y_2. \tag{12}$$

Below, we show that every integral solution of (11) produces a corresponding reducible $R_3(x)$ given by (12). In fact, we will find out that $R_3(x)$ splits completely over $\mathbb{Q}$ in this case. Consequently, appealing to Theorem 2.1, we could then deduce that $\mathcal{L}_4^{(\alpha)}(x)$ has V_4 as its Galois group.

Let us set $\delta=\sqrt{-3}$. Then from (11), we have the following factorization in the ring of integers $R=\mathbb{Z}+\mathbb{Z}\big[(1+\delta)/2\big]$ of $\mathbb{Q}(\delta)$.

$$Z^3=(Y_1+\delta Y_2)(Y_1-\delta Y_2).$$

We note that R is a principal ideal domain. Let $\mathsf{d}=\gcd(Y_1+\delta Y_2, Y_1-\delta Y_2)$. Let p be a prime divisor (possibly, $p=1$) of the norm $N(\mathsf{d})=N_{\mathbb{Q}(\sqrt{-3})/\mathbb{Q}}(\mathsf{d})$. Since $N(\mathsf{d})$ also divides Z^3, and Z is odd, we may as well assume that p is odd. Observe that d divides $Y_1+\delta Y_2+Y_1-\delta Y_2=2Y_1$. Since p is odd, we deduce that p divides Y_1. Thus $p|Z^3$ and $p|Y_1^2$. Observe that $Z^3=\varepsilon(s+3t)$ and $Y_1^2=\varepsilon(s+\beta t)$ where $\beta=2$ or $\beta=4$, and $\varepsilon\in\{1,-1\}$.

Hence $\gcd(Z^3, Y_1^2)=\gcd(s+\beta t, s+3t)=\gcd(s,t)=1$. It follows that $p=1$, and hence, $Y_1+\delta Y_2$ and $Y_1-\delta Y_2$ are relatively prime in R. Since R is a unique factorization domain, we conclude that there are integers a and b of the same parity, and a unit $\gamma\in R$ such that

$$Y_1+\theta\delta Y_2=\gamma\left(\frac{a+\theta\delta b}{2}\right)^3, \quad \theta\in\{\pm1\}, \quad Z=\frac{a^2+3b^2}{4}; \quad Z\equiv 1 \pmod 2. \tag{13}$$

Note that $\gcd(a,b)\le 2$, else, $Y_1+\delta Y_2$ and $Y_1-\delta Y_2$ will have a nontrivial common factor. In particular, if a and b are even, then $a\equiv b+2 \pmod 4$.

We recall that the only units in R are $\{\pm 1, \pm(1 \pm \delta)/2\}$. Since, we have not imposed any restriction on the signs of a and b, it suffices to consider the case that $\gamma \in \{1, (1+\eta\delta)/2\}$, $\eta \in \{-1, 1\}$ and $\theta = 1$. We show that for $\gamma = (1+\eta\delta)/2$, the value of Y_1, obtained in (13), is either not an integer or do not yield admissible values for Z. Hence, for $\gamma = (1+\delta)/2$, (13) does not give any integral solutions to (11). After solving for Y_1 in (13) with $\gamma = (1+\eta\delta)/2$, we have

$$Y_1 = \frac{a^3 - 9ab^2 - 9\eta a^2 b + 9\eta b^3}{16}.$$

Let us set $Y_1(a,b) = a^3 - 9ab^2 - 9a^2b + 9b^3$. Thus, $Y_1(a,b) \equiv 0 \pmod{16}$ for Y_1 to be an integer. First, assume that a and b are odd. Since odd integer squares are congruent to 1 or $9 \pmod{16}$, we have that either $a^2 \equiv b^2 \pmod{16}$ or, $a^2 \equiv 9b^2 \pmod{16}$ and $9a^2 \equiv b^2 \pmod{16}$. In the former case, $Y_1(a,b) \equiv -8a^3 \pmod{16}$, and as such, Y_1 is not an integer in this case. In the latter case, $Y_1(a,b) \equiv \pm 8\eta b^3 \pmod{16}$. Therefore, Y_1 is not an integer in this case either. Now suppose that a and b are even integers. Note that the squares of even integers are congruent to 0 or $4 \pmod{16}$. If $a^2 \equiv b^2 \pmod{16}$, then $4Z = a^2 + 3b^2 \equiv 4a^2 \equiv 0 \pmod{16}$. But the last relation contradicts the fact that Z is an odd integer (see (13) above). In the remaining case, either $4a^2 \equiv b^2 \pmod{16}$ or $a^2 \equiv 4b^2 \pmod{16}$. In the case that $4a^2 \equiv b^2 \pmod{16}$, we have $a \equiv 2 \pmod{4}$ and $b \equiv 0 \pmod{4}$. Consequently, $Y_1(a,b) \equiv a^3 \equiv 8 \pmod{16}$. But then $Y_1 = Y_1(a,b)/16$ fails to be an integer. We get a similar contradiction in the case that $a^2 \equiv 4b^2 \pmod{16}$. Hence, we can take $\gamma = 1$ in (13). After solving for Y_1 and Y_2, we see that the complete set of solutions to (10) is given by

$$Y_1 = \frac{a(a^2-9b^2)}{8}, \quad Y_2 = \frac{3b(a^2-b^2)}{8}, \quad Z = \frac{a^2+3b^2}{4}; \quad Z \equiv 1 \pmod{2},$$

where $a \equiv b \pmod{2}$ with $\gcd(a,b) \le 2$. Thus, for even s, we have

$$s + 4t \in \left\{ \frac{\epsilon a^2(a^2-9b^2)^2}{32}, \frac{27\epsilon b^2(a^2-b^2)^2}{32} \right\}, \tag{14}$$

and

$$s + 3t = \frac{\epsilon(a^2+3b^2)^3}{64}, \tag{15}$$

where $\varepsilon \in \{-1, 1\}$. Now, plugging in $(z_1, y_2) = ((a^2+3b^2)/4, a(a^2-9b^2)/8)$ and $(z_1, y_2) = ((a^2+3b^2)/4, 3b(a^2-b^2)/8)$ in (12), we find that

$$R_3(x) = \begin{cases} x^3 - 3(a^2+3b^2)x - 2\varepsilon a(a^2-9b^2) & \text{if} \quad m = 1, \\ x^3 - 9(a^2+3b^2)x - 54\varepsilon b(a^2-b^2) & \text{if} \quad m = 3. \end{cases}$$

One verifies that for $m = 1$,

$$R_3(x) = (x - 2a\varepsilon)(x + a\varepsilon + 3b)(x + a\varepsilon - 3b),$$

and if $m = 3$, then

$$R_3(x) = (x + 6b\varepsilon)(x - 3b\varepsilon + 3a)(x - 3b\varepsilon - 3a).$$

This finishes the proof of our assertion. Solving for s and t in (14) and (15), we have

$$t = \pm\epsilon(a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6)/64. \tag{16}$$

Corresponding to the positive sign above, we have

$$s = -2\epsilon(a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6)/64, \tag{17}$$

and for the negative sign,

$$s = -2\epsilon(2a^6 - 63a^4b^2 + 216a^2b^4 - 27b^6)/64. \tag{18}$$

Here the integer parameters a and b satisfy

$$\gcd(a, b) \leq 2; \quad a \equiv b \pmod 2.$$

We further observe that, if $3 \mid a$, then $\gcd(s, t) \geq 3$. Thus, we assume that $3 \nmid a$. The two sets of values of α obtained from (16), (17) and (18) are respectively,

$$\alpha = \frac{-2(a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6)}{a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6} \tag{19}$$

and

$$\frac{-2(2a^6 - 63a^4b^2 + 216a^2b^4 - 27b^6)}{a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6}. \tag{20}$$

We will compare these with $\alpha \in \mathcal{B}_4$ and establish that there are admissible solutions integers u and v in the following cases:

- α satisfies (i) of $\mathcal{B}_4$ and (19),
- α satisfies (ii) of $\mathcal{B}_4$ and (20),
- α satisfies (iii) of $\mathcal{B}_4$ and (20),
- α satisfies (iv) of $\mathcal{B}_4$ and (19).

There are no admissible solutions in the remaining cases. We begin with the case that α satisfies (i) of $\mathcal{B}_4$ and (19). In this case,

$$\frac{u^2 - 6v^2}{u^2 - 3v^2} = \frac{a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6}{a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6}.$$

Comparing the numerators and the denominators, we have

$$u^2 - 6v^2 = \lambda(a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6)$$

and that

$$u^2 - 3v^2 = \lambda(a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6)$$

for some nonzero rational λ. Solving for u and v, we get

$$u = \pm\sqrt{\lambda}a(a^2 - 9b^2) \quad \text{and} \quad v = \pm 3\sqrt{\lambda}b(a^2 - b^2).$$

Recall that a and b have the same parity with $\gcd(a, b) \leq 2$. Thus, if a and b are odd, then $\gcd(a, b) = 1$, and

$$a^2 - b^2 \equiv a^2 - 9b^2 \pmod 8.$$

Since the odd squares $\pmod{16}$ are 1 or 9, we deduce that one among $a^2 - b^2$ and $a^2 - 9b^2$ is not divisible by 16. Since $3 \nmid a$ and $\gcd(a, b) = 1$, we deduce that

$$\gcd(b(a^2 - b^2), a(a^2 - 9b^2)) = 8.$$

Accordingly, we set $\sqrt{\lambda} = 1/8$. That is, we take $\lambda = 1/64$ in this case. Now consider the case that a and b are even. In this case, $\gcd(a, b) = 2$. Therefore, $a^2 - b^2 \not\equiv 0 \pmod 8$. Nevertheless,

$$a^2 - b^2 \equiv a^2 - 9b^2 \pmod 4.$$

Thus, $\gcd(b(a^2 - b^2), a(a^2 - 9b^2)) = 8$ in this case as well, and accordingly, we take $\lambda = 1/64$.

Now suppose α satisfies (ii) of $\mathcal{B}_4$ and (20). In this case, we have

$$\frac{2u^2 - 3v^2}{u^2 - 3v^2} = \frac{2a^6 - 63a^4b^2 + 216a^2b^4 - 27b^6}{a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6}.$$

Working similarly as before, we solve for u and v to get that

$$u = \pm a(a^2 - 9b^2)/8 \quad \text{and} \quad v = \pm 3b(a^2 - b^2)/8.$$

Next, we consider the case that α satisfies (iii) of $\mathcal{B}_4$ and (20). In this case, we have

$$u^2 + v^2 + 10uv = 2\lambda(2a^6 - 63a^4b^2 + 216a^2b^4 - 27b^6)$$

and

$$u^2 + v^2 + 4uv = \lambda(a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6),$$

where λ is a nonzero rational number. After subtracting and then dividing out by 3, we get that

$$2uv = \lambda(a^6 - 27a^4b^2 + 99a^2b^4 - 97b^6).$$

Subtracting $2uv$ from $u^2 + v^2 + 4uv$, we have

$$(u + v)^2 = -18\lambda b^2(a^2 - b^2)^2.$$

Similarly, after subtracting $6uv$ from $u^2 + v^2 + 4uv$, we get

$$(u - v)^2 = -2\lambda b^2(a^2 - 9b^2)^2.$$

Thus,

$$u + v = \pm 3\sqrt{-2\lambda}(a^2 - b^2) \quad \text{and} \quad u - v = \pm\sqrt{-2\lambda}(a^2 - 9b^2).$$

The choice of $\lambda \in \mathbb{Q}\backslash\{0\}$ must be such that $\gcd(u, v) = 1$. Proceeding similarly as before, we deduce that $\gcd(b(a^2 - b^2), a(a^2 - 9b^2)) = 8$ in this case. Accordingly, we set $\sqrt{-2\lambda} = 1/4$. That is $\lambda = -1/32$. Now, solving for u and v, we find that

$$u = \frac{\pm 3b(a^2 - b^2 \pm a(a^2 - 9b^2))}{8}$$

and

$$v = \frac{\pm 3b(a^2 - b^2 \mp a(a^2 - 9b^2))}{8}.$$

Finally, in the case that α satisfies (iv) of $\mathcal{B}_4$ and (19), we get that

$$5u^2 + 5v^2 + 14uv = 2\lambda(a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6)$$

and

$$u^2 + v^2 + 4uv = \lambda(a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6).$$

From

$$6(u^2 + v^2 + 4uv) - (5u^2 + 5v^2 + 14uv) = u^2 + v^2 + 10uv,$$

we get that

$$u^2 + v^2 + 10uv = 2\lambda(2a^6 - 63a^4b^2 + 216a^2b^4 - 27b^6).$$

Thus, this case coincides with the preceding one and, as such, one obtains the same set of values for u and v as in the previous case. This settles the sufficiency of (a) and (b) in Theorem 1.1.

It remains to show that there are no admissible solutions in the remaining cases. We begin by considering the case that α satisfies (i) of $\mathcal{B}_4$ and (20). In this case, we get that

$$\frac{u^2-6v^2}{u^2-3v^2}=\frac{2a^6-63a^4b^2+216a^2b^4-27b^6}{a^6-45a^4b^2+135a^2b^4-27b^6}.$$

Comparing and solving for $3v^2$, we find that there is a nonzero rational number λ such that

$$3v^2=-\lambda a^2(a^2-9b^2)^2.$$

Let $\lambda=p/q$ where p and q are nonzero integers with $\gcd(p,q)=1$. Since $3\nmid a$, we deduce from above that $3|p$. But then from

$$u^2-6v^2=\lambda(2a^6-63a^4b^2+216a^2b^4-27b^6),$$

we get that $3|u$ (since $3\nmid q$). But this contradicts (i) of $\mathcal{B}_4$. Next suppose that α satisfies (ii) of $\mathcal{B}_4$ and (19). In this case, we have

$$\frac{2u^2-3v^2}{u^2-3v^2}=\frac{a^6-72a^4b^2+189a^2b^4-54b^6}{a^6-45a^4b^2+135a^2b^4-27b^6}.$$

Thus, there is a nonzero rational $\lambda=p/q$ such that

$$2u^2-3v^2=\lambda(a^6-72a^4b^2+189a^2b^4-54b^6)$$

and

$$u^2-3v^2=\lambda(a^6-45a^4b^2+135a^2b^4-27b^6).$$

Solving, we have

$$u^2=-27\lambda b^2(a^2-b^2)^2 \quad \text{and} \quad 3v^2=-\lambda a^2(a^2-9b^2)^2.$$

Once again, since $3\nmid a$, we deduce from the last display that $3|p$. Consequently, from the display preceding the last display, we get that $27|u$, a contradiction since $3\nmid u$ as per (ii), $\mathcal{B}_4$.

If α satisfies (iii) of $\mathcal{B}_4$ and (19), then proceeding as before we have

$$u^2+v^2+10uv=2\lambda(a^6-72a^4b^2+189a^2b^4-54b^6)$$

and

$$u^2+v^2+4uv=\lambda(a^6-45a^4b^2+135a^2b^4-27b^6),$$

where $\lambda=p/q$ is a nonzero rational number with $\gcd(p,q)=1$. Subtracting, we get

$$6uv=\lambda(a^6-99a^4b^2+243a^2b^4-81b^6).$$

Since $3\nmid a$, we have that $3|p$. Similarly, it also follows from the display preceding the last one above that $3|(u^2+v^2+4uv)$. Recall that $u\not\equiv v \pmod 3$ in (iii) of $\mathcal{B}_4$. But this implies that

$$0\equiv u^2+v^2+4uv\equiv u^2+v^2+uv\equiv 1 \pmod 3,$$

a contradiction, and our assertion follows.

Lastly, we consider the case that α satisfies (iv) of $\mathcal{B}_4$ and (20). In this case, we have

$$5u^2 + 5v^2 + 14uv = 2\lambda(2a^6 - 63a^4b^2 + 216a^2b^4 - 27b^6)$$

and

$$u^2 + v^2 + 4uv = \lambda(a^6 - 45a^4b^2 + 135a^2b^4 - 27b^6).$$

As noted before, we have from observing that

$$6(u^2 + v^2 + 4uv) - (5u^2 + 5v^2 + 14uv) = u^2 + v^2 + 10uv,$$

that

$$u^2 + v^2 + 10uv = 2\lambda(a^6 - 72a^4b^2 + 189a^2b^4 - 54b^6).$$

Thus, we are reduced to the preceding case. Hence, there are no admissible solutions in integers u and v in this case. This concludes the proof of Theorem 1.1.

We now turn to the proof of Theorem 1.2. Thus, we assume for now that $\alpha \in \mathbb{Q}\backslash\mathcal{E}_4$, and that α does not satisfy (i)–(iv) in $\mathcal{B}_4$. In particular, $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) \neq \square$. According to Theorem 2.1, the Galois group of $\mathcal{L}_4^{(\alpha)}(x)$ is different from S_4 if and only if the resolvent cubic of $\mathcal{L}_4^{(\alpha)}(x)$ is reducible. As before, we work with the shifted polynomial

$$g(x) = \mathcal{L}_4^{(\alpha)}(x + \alpha + 4) = x^4 - 6(\alpha + 4)x^2 - 8(\alpha + 4)x + 3(\alpha + 4)(\alpha + 2),$$

and let

$$R_1(x) = R_g(2x - 2\alpha - 8)/8 = x^3 - 6(\alpha + 4)(\alpha + 3)x - 4(\alpha + 4)^2(\alpha + 3).$$

We assume that $R_1(x)$ is reducible over the rationals. Note that in the case under consideration, $R_1(x)$ has exactly one root in $\mathbb{Q}$. Else, if $R_1(x)$ has three roots in $\mathbb{Q}$, then by (iii) of Theorem 2.1,

$$\mathrm{Gal}(\mathcal{L}_4^{(\alpha)}) = \mathrm{Gal}(g) = V_4.$$

Since $V_4 \subset A_4$, it will then follow that $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = \square$, contrary to our assumption in the present case.

Now, consider the polynomial

$$\frac{R_1((\alpha + 3)x)}{(\alpha + 3)^3} = x^3 - 6\left(\frac{\alpha + 4}{\alpha + 3}\right)x - 4\left(\frac{\alpha + 4}{\alpha + 3}\right)^2.$$

Setting $s = (\alpha + 4)/(\alpha + 3)$ in the last equation, we find that $R_1(x)$ is reducible over the rationals for some $\alpha \in \mathbb{Q}$ if and only if (x, s) is a $\mathbb{Q}$-rational point on the curve $r(x, s) = x^3 - 6sx - 4s^2$. Considering $r(x, s) = 0$ as a quadratic equation in s, we see that a reducible $R_1(x)$ corresponds to $\mathbb{Q}$-rational points on the curve $\mathrm{Discr}_s(r(x, s)) = 36x^2 + 16x^3 = \square$. It is now easy to see that the $\mathbb{Q}$-rational points on this curve correspond to the $\mathbb{Q}$-rational points on the parabola $y^2 = 4x + 9$. The $\mathbb{Q}$-rational points on this parabola can be parametrized as

$$x = t^2 - 9/4, \quad y = 2t, \quad t \in \mathbb{Q}.$$

Now, solving for s in $r(x, s) = 0$, we get that

$$s = \frac{(-3 \pm 2t)x}{4}.$$

Putting $x = t^2 - 9/4$ and simplifying, we get that

$$s = \frac{\varepsilon}{4}(t^2 - 9/4)(2t - 3\varepsilon) = \begin{cases} (2t+3)(2t-3)^2/16 & \text{if} \quad \varepsilon = 1, \\ -(2t+3)^2(2t-3)/16 & \text{if} \quad \varepsilon = -1. \end{cases}$$

For notational convenience, we set $u = 2t + 3$ and $v = 2t - 3$ so that, $u - v = 6$. Thus,

$$s = \begin{cases} uv^2/16 & \text{if} \quad \varepsilon = 1, \\ -u^2v/16 & \text{if} \quad \varepsilon = -1. \end{cases}$$

Now solving for α in $s = (\alpha + 4)/(\alpha + 3)$, we get that

$$\alpha + 3 = \begin{cases} 16/(uv^2 - 16) & \text{if} \quad s = uv^2/16, \\ -16/(u^2v + 16) & \text{if} \quad s = -u^2v/16. \end{cases} \tag{21}$$

Let A be the unique rational root of $R_g(x)$. Recall that $R_g(x)$ is given by

$$R_g(x) = x^3 + 6(\alpha+4)x^2 - 12(\alpha+4)(\alpha+2)x - 72(\alpha+4)^2(\alpha+2) - 64(\alpha+4)^2.$$

It follows that

$$A = x/2(\alpha + 3) + \alpha + 4,$$

where $x \in \mathbb{Q}$ is a root of $r(x, s) = 0$. Note that $x = (4t^2 - 9)/4 = uv/4$. Putting the values of x and α above, we get

$$A = \begin{cases} \dfrac{uv(uv^2 - 16)}{128} + \dfrac{uv^2}{uv^2 - 16} & \text{if} \quad \alpha + 3 = 16/(uv^2 - 16), \\ \dfrac{-uv(u^2v + 16)}{128} + \dfrac{u^2v}{u^2v + 16} & \text{if} \quad \alpha + 3 = -16/(u^2v + 16). \end{cases} \tag{22}$$

Recall that if $R_g(x)$ has exactly one rational root A, then $\mathrm{Gal}(g) = D_4$ or $\mathrm{Gal}(g) = \mathbb{Z}/4\mathbb{Z}$. In order to finish the proof of Theorem 1.2, we must eliminate the occurrence of the latter possibility. On the other hand, we have to show that the former occurs infinitely often. This in turn is determined by the factorization of the polynomial $G(x)$ in Theorem 2.1 over the splitting field of $R_g(x)$. We recall that $\mathrm{Discr}(R_g) = \mathrm{Discr}(g) = \mathrm{Discr}(\mathcal{L}_4^{(\alpha)})$. Since, $R_g(x)$ has a rational root, it follows that the splitting field of $R_g(x)$ is

$$K = \mathbb{Q}\left(\sqrt{\mathrm{Discr}(R_g)}\right) = \mathbb{Q}\big(\sqrt{\mathrm{Discr}(g)}\big) = \mathbb{Q}\left(\sqrt{\mathrm{Discr}(\mathcal{L}_4^{(\alpha)})}\right).$$

Recall that $\mathrm{Discr}(\mathcal{L}_4^{(\alpha)}) = 3(\alpha+4)(\alpha+2) \pmod{\mathbb{Q}^2}$. Therefore,

$$K = \mathbb{Q}\big(\sqrt{\Delta}\big), \quad \Delta = 3(\alpha+4)(\alpha+2).$$

Setting $F(x) = g(x)$ in Theorem 2.1, we find that

$$G(x) = (x^2 - Ax + 3(\alpha+4)(\alpha+2))(x^2 - 6(\alpha+4) - A).$$

Thus, by (iv) of Theorem 2.1, $g(x)$ has the Galois group $\mathbb{Z}/4\mathbb{Z}$ if and only if $G(x)$ splits over $K = \mathbb{Q}\big(\sqrt{\Delta}\big)$. This is the case if and only if $A^2 - 12(\alpha+4)(\alpha+2)$ and $4(6(\alpha+4) + A)$ (these are the discriminants of the quadratic factors of $G(x)$) are nonzero squares in K. Note that

$$(A^2 - 12(\alpha+4)(\alpha+2))((6(\alpha+4) + A)) = R_g(A) + 64(\alpha+4)^2 = 64(\alpha+4)^2.$$

Since $\alpha \in \mathbb{Q}$, it therefore suffices to have $6(\alpha+4)+A$ be a square in K in order for $G(x)$ to split completely over K. From Corollary 4.3, [4], we deduce that $6(\alpha+4)+A$ is square in K if and only if $(6(\alpha+4)+A)\Delta = \square$. We substitute the values of α and A from (21) and (22), say, we consider first

$$\alpha + 3 = 16/(uv^2 - 16).$$

After substituting α, A and Δ in $(6(\alpha+4)+A)\Delta = \square$, we get

$$3 \times \frac{uv^2}{uv^2-16} \times \frac{32-uv^2}{uv^2-16} \times \left(\frac{7uv^2}{uv^2-16} + \frac{uv(uv^2-16)}{128}\right) = \square.$$

We show that the last equation does not hold for any choice of integers u and v satisfying $u = v+6$. After identifying the obvious squares appearing on the left hand side above, we rewrite the equation as

$$v(32-uv^2)(uv^2-16)((uv^2-16)^2+896v) = 3z^2, \tag{23}$$

where $z \neq 0$ is an integer. As noted previously, we may assume without any loss of generality that u and v (as described in $\mathcal{B}_4$) are positive. Therefore, for (23) to hold, we must have that $(32-uv^2)(uv^2-16) > 0$. This implies that $16 < uv^2 < 32$. Note that if $v \geq 2$, then $u = v+6 \geq 8$ so that, $uv^2 \geq 32$. Therefore, we are left with the possibility that $v = 1$, and as such, $u = 7$. But then $uv^2 = 7 < 16$. This proves our assertion.

In the case that $\alpha + 3 = -16/(uv^2+16)$, after substituting the values of $\Delta = 3(\alpha+4)(\alpha+4)$ and α from above and A from (21) in $(6(\alpha+4)+A)\Delta = \square$, we get

$$\frac{3u^2v}{u^2v+16} \times \frac{-32-u^2v}{u^2v+16} \times \left(\frac{7u^2v}{u^2v+16} - \frac{uv(u^2v+16)}{128}\right) = \square,$$

where $u = v+6$. Proceeding as before, we identify the obvious squares here and rewrite the last equation as

$$u(u^2v+32)(u^2v+16)((u^2v+16)^2 - 896u) = 3z^2, \tag{24}$$

where $z \neq 0$ is an integer. Observe that after putting $u = v+6$ in u^2v+32, we get

$$u^2v + 32 = v^3 + 12v^2 + 36v + 32 = (v+2)^2(v+8).$$

Doing the same for u^2v+16 gives

$$u^2v + 16 = v^3 + 12v^2 + 36v + 16 = (v+4)(v^2+8v+4).$$

Plugging these values in (24), ignoring the square factors, we get

$$(v+4)(v+6)(v+8)(v^2+8v+4)((v+4)^2(v^2+8v+4)^2 - 896(v+6)) = 3z^2. \tag{25}$$

We would like to establish that there are no integer points (v,z) with $vz \neq 0$ on the curve given by (25). This is achieved as follows. First, we show that if (v,z) is an integer point on (25), then for some integer $z_1 \neq 0$, the integer point (v, z_1) lies on an elliptic curve of the shape

$$(v+4)(v+6)(v+8) = bz_1^2 \quad \text{where} \quad b|42. \tag{26}$$

We then take the help of Sage to find the integer points on these elliptic curves. Finally, we arrive at a contradiction by plugging the values of v in (25) and showing that the product on the left hand side of (25) is not of the form $3z^2$.

In order to obtain the desired elliptic curves, we first note that each factor appearing on the left hand side of (25) can be uniquely expressed as $m\ell^2$ where m and ℓ are nonzero integers with m squarefree. We refer to m as the squarefree part of the concerned factor. Observe that product of the squarefree parts of all the factors must be of the form $3k^2$ where $k|z$ in (25). Thus, if m is the squarefree part of a factor in (25), and p is prime diving m, then either $p = 3$ or there is another factor in (25) with squarefree part m' such that $p|m'$. Let m_i denote the squarefree part of $v + i$ for $i = 4, 6$ and 8. We investigate the possible prime divisors of m_i for each $i \in \{4, 6, 8\}$. Let $p|m_i$ and $p \neq 3$. Note that if $p|m_j$ for some $j \neq i$, then p divides $v + i - (v + j) = i - j \in \{\pm 2, \pm 4\}$. Thus, $p = 2$ in that case. Now, if $p|(v^2 + 8v + 4)$, then we have

$$q(i) = i^2 - 8i + 4 \equiv 0 \pmod{p}.$$

Now, $q(4) = -12$, $q(6) = -8$ and $q(8) = 4$. It follows that $p = 2$ (note that we have assumed $p \neq 3$). Similarly, if $p|((v + 4)^2(v^2 + 8v + 4)^2 - 896(v + 6))$, then

$$q(i) = (4 - i)^2(i^2 - 8i + 4)^2 - 896(6 - i) \equiv 0 \pmod{p}.$$

We have $q(4) = -2^8 \cdot 7$, $q(6) = -2^8$ and $q(8) = 2^{11}$. Thus, $p \in \{2, 7\}$. The above analysis shows that if $p|m_i$ for some $i \in \{4, 6, 8\}$, then either $p = 3$ or $p \in \{2, 7\}$. Therefore, $m_i|42$ and we get the elliptic curve (26). We now analyse this elliptic curve. In order to put the curve (26) in the Weierstrass form, we perform a couple of transformations. First, we set $v + 6 = x_1$ to get

$$x_1(x_1^2 - 4) = bz_1^2.$$

Next, we multiply both sides by b^3, and set $x = bx_1$ and $y = b^2 z_1$ to get

$$x(x^2 - 4b^2) = y^2; \quad y \neq 0; \quad b \in \mathcal{B} := \{1, 2, 3, 6, 7, 14, 21, 42\}. \tag{27}$$

We used Sage to find all (finitely many) the integral points (x, y) on (27) for each $b \in \mathcal{B}$. Among these, we discarded those solutions (x, y) where, either $y = 0$, $b \nmid x$ or $b^2 \nmid y$. This procedure gave us the following 6 values of x:

$$b = 3, x \in \{-3, 12, 18, 294\}; \quad b = 7, x = 112 \quad \text{and} \quad b = 42, x = 588.$$

We now obtain the values of $x_1 = x/b$ as

$$b = 3, x_1 \in \{-1, 4, 6, 98\}; \quad b = 7, x_1 = 16 \quad \text{and} \quad b = 42, x_1 = 14.$$

Accordingly, we obtain the values of $v = x_1 - 6$ as $v \in \{-7, -2, 0, 92, 10, 8\}$. Recall that only $v > 0$ are being considered here. This leaves us with the possibility that $v \in \{92, 10, 8\}$. It is then easily verified that none of these values of v yields an admissible value for z in (24).

Thus, we have established that if the resolvent cubic of $\mathcal{L}_4^{(\alpha)}(x)$ splits but not completely, then $\mathrm{Gal}(\mathcal{L}_4^{(\alpha)}) = D_4$. Furthermore, this is the case if (see (21))

$$\alpha + 3 \in \{16/(uv^2 - 16), -16/(u^2 v + 16)\},$$

where $u = v + 6$. Setting $v = \lambda$ and $u = \lambda + 6$ if $\alpha + 3 = 16/(uv^2 - 16)$ and, $u = \lambda$ and $v = \lambda - 6$ if $\alpha + 3 = -16/(u^2v + 16)$, we get the two sets (corresponding to $\varepsilon = \pm 1$) of values of α in Theorem 1.2 for which $\mathrm{Gal}(\mathcal{L}_4^{(\alpha)}) = D_4$. The Galois group is S_4 by Theorem 2.1 for all other values of α considered in Theorem 1.2. This concludes the proof of Theorem 1.2. □

Acknowledgements

The authors would like to express their sincere gratitude to all the referees for providing their valuable feedback that certainly helped us to make a better presentation of the material.

References

[1] Banerjee, P. (2014). On Galois groups of Laguerre polynomials whose discriminants are squares. *Journal of Number Theory*, 141, 36–58.

[2] Banerjee, P. (2018). On Galois groups of a one-parameter orthogonal family of polynomials. *Acta Arithmetica*, 190, 1–36.

[3] Banerjee, P., Filaseta, M., Finch, C., & Leidy, J. (2013). On classifying Laguerre polynomials which have Galois group the alternating group. *Journal de Théorie des Nombres de Bordeaux*, 25, 1–30.

[4] Conrad, K. (2020). *Galois groups of cubics and quartics (not in characteristic* 2*)*. Available online at `https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf`.

[5] Dumas, D. (1906). Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels. *Journal de Mathématiques Pures et Appliquées*, 2, 191–258.

[6] Hajir, F. (2009). Algebraic properties of a family of generalized Laguerre polynomials. *Canadian Journal of Mathematics*, 61, 583–603.

[7] Hajir, F., & Wong, S. (2006). Specializations of one parameter family of polynomials. *Annales de l'Institut Fourier (Grenoble)*, 56, 1127–1163.

[8] Kappe, L. C. & Warren, B. (1989). An elementary test for the Galois group of a quartic polynomial. *American Mathematical Monthly*, 96, 133–137.

[9] Schur, I. (1929). Einege Satže über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, I. *Sitzungsberichte der Preussischen Akademie der Wissenschaften. Physikalisch-Mathematische Klasse*, 4, 125–136.

[10] Schur, I. (1929). Gleichungen ohne Affekt. *Sitzungsberichte der Preussischen Akademie der Wissenschaften. Physikalisch-Mathematische Klasse*, 14, 443–449.

[11] Schur, I. (1931). Affectlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome. *Journal für die reine und angewandte Mathematik*, 165, 52–58.