Journal of Number Theory 141 (2014) 36–58

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On Galois groups of generalized Laguerre polynomials whose discriminants are squares

Pradipto Banerjee

Indian Statistical Institute, Stat-Math Unit, 203 Barrackpore Trunk Road, Kolkata 700108, India

A R T I C L E I N F O

Article history:
Received 22 March 2013
Received in revised form 10 January 2014
Accepted 10 January 2014
Available online 4 March 2014
Communicated by David Goss

Keywords:
Generalized Laguerre polynomials
Irreducibility of polynomials
Galois groups of cubics, quartics and quintics

A B S T R A C T

In this paper, we compute Galois groups over the rationals associated with generalized Laguerre polynomials $L_n^{(\alpha)}(x)$ whose discriminants are rational squares, where n and α are integers. An explicit description of the integer pairs (n, α) for which the discriminant of $L_n^{(\alpha)}(x)$ is a rational square was recently obtained by the author in a joint work with Filaseta, Finch and Leidy. Among these pairs (n, α), we show that for $2 \leqslant n \leqslant 5$, the associated Galois group of $L_n^{(\alpha)}(x)$ is always A_n, except for the pairs $(4, -1)$ and $(4, 23)$. For $n \geqslant 6$, we show that the corresponding Galois group is A_n if and only if the polynomial concerned is irreducible over the rationals.

1. Introduction

For a real number α, and a positive integer n, the generalized Laguerre polynomial of degree n is defined by

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

In this paper however, we will concern ourselves with the case that α is an integer.

E-mail address: pradipto.banerjee7@gmail.com.

http://dx.doi.org/10.1016/j.jnt.2014.01.009
0022-314X/

The generalized Laguerre polynomials find a wide range of applications in several branches of mathematics. An interest in algebraic and number theoretic aspects of these polynomials was initiated by Schur, in a series of papers [13–15], where he established the irreducibility of $L_n^{(\alpha)}(x)$ for $\alpha \in \{0, 1, -n-1\}$ over the rationals. He also computed their associated Galois groups. In particular, he [14] gave the following remarkable formula for the discriminant $\mathrm{Disc}(n, \alpha)$ of the monic integral polynomial $\mathcal{L}_n^{(\alpha)}(x) = (-1)^n n! L_n^{(\alpha)}(x)$, namely

$$\mathrm{Disc}(n, \alpha) = \prod_{j=2}^{n} j^j (\alpha + j)^{j-1}.$$

Recently, a variety of results concerning the irreducibility and Galois properties of $L_n^{(\alpha)}(x)$ have appeared in the literature. To cite a few, Gow [6] showed that if $n \equiv 2 \pmod 4$ and $n \neq 2$, then $L_n^{(n)}(x)$ has Galois group A_n, the alternating group on n letters, provided it is irreducible. Filaseta, Kidd and Trifonov [4] have established the irreducibility in this case. Hajir [7,9] and Sell [16] have investigated the irreducibility and Galois groups associated with $L_n^{(\alpha)}(x)$ for $\alpha = -n - r$ where r is a positive integer. In particular, Hajir shows that for r large and n sufficiently large depending on r, the polynomial $L_n^{(\alpha)}(x)$ is irreducible and has Galois group S_n, the symmetric group on n letters. Filaseta and Lam [5] showed that if $\alpha \in \mathbb{Q}$ is not a negative integer, then $L_n^{(\alpha)}(x)$ is irreducible for n sufficiently large. Hajir [8] extended their result showing that for α a rational number that is not a negative integer, and n sufficiently large depending on α, the Galois group of $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ is A_n if $\mathrm{Disc}(n, \alpha)$ is a square, and S_n otherwise. In [10], Hajir and Wong consider the case in which $n \geqslant 5$ is fixed and show that for all but finitely many values of α, $L_n^{(\alpha)}(x)$ is irreducible and the Galois group of $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ is A_n if $\mathrm{Disc}(n, \alpha)$ is a square, and S_n otherwise.

More recently, the author in a joint work with Filaseta, Finch and Leidy [1] has explicitly described the set $\mathcal{A}$ of integer pairs (n, α) with $n \geqslant 1$, for which $\mathrm{Disc}(n, \alpha)$ is a nonzero square. Thus the Galois group associated with $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ is A_n only if $(n, \alpha) \in \mathcal{A}$. We shall describe the set $\mathcal{A}$ briefly. In this paper, we attempt to describe the Galois group of $L_n^{(\alpha)}(x)$ for precisely the pairs (n, α) in $\mathcal{A}$.

2. Statements of the main results

We will often denote an *integer square* by $\square$. The greatest prime factor of a natural number $b > 1$ will be denoted by $P(b)$. If $c + d\sqrt{t} = (a + b\sqrt{t}\,)^u$, where c, d, a, b and t are rational numbers with $\sqrt{t}$ irrational and u is a nonnegative integer, then we refer to c as the rational part of $(a + b\sqrt{t}\,)^u$. For a prime p, a positive integer e and an integer n, we will often use the notation $p^e \parallel n$ to denote that $p^e \mid n$, but $p^{e+1} \nmid n$.

Following the notations in [1], we view pairs (n, α) in $\mathcal{A}$ as being in two sets $\mathcal{A}_0$ and $\mathcal{A}_\infty$. As is evident in [1], the set $\mathcal{A}_0$ is finite set of pairs that are effectively computable, and, hence, so are the corresponding Galois groups. In this paper, we will be interested in the Galois group of $L_n^{(\alpha)}(x)$, for precisely the pairs (n,α) in $\mathcal{A}_\infty$.

The set $\mathcal{A}_\infty$ consists of pairs (n,α) satisfying one of the following.

(i) $n = 1$ and α arbitrary
(ii) $\alpha = n$ and $n \equiv 0 \pmod 2$
(iii) $\alpha = 1$ and n is odd or $n+1$ is an odd square
(iv) $\alpha = -1$ and n is even or n is an odd square
(v) $\alpha = -n-1$ and $n \equiv 0 \pmod 4$
(vi) $\alpha = -n-2$ and $n \equiv 1 \pmod 4$
(vii) $\alpha = -2n-2$ and $n \equiv 0 \pmod 4$
(viii) $\alpha = 3$ and $n+2$ is the rational part of $(2+\sqrt{3})^{2k+1}$ for some $k \in \mathbb{N}$
(ix) $\alpha = 3$, $n \equiv 1 \pmod{24}$ and $(n+2)/3$ is a square
(x) $\alpha = 5$ and $n+3$ is the rational part of $(4+\sqrt{15})^{2k+1}$ for some $k \in \mathbb{N}$
(xi) $\alpha = n-6$ and $(2n-5)/3$ is the rational part of $(1+\sqrt{2})^{4k}$ for some $k \in \mathbb{N}$
(xii) $\alpha = n-1$ is even and n is a square
(xiii) $n = 2$ and $\alpha + 2$ is a square
(xiv) $n = 3$, $\alpha \equiv 1 \pmod 3$ and $(\alpha+2)/3$ is a square
(xv) $n = 4$ and $\alpha + 3$ is the rational part of $(2+\sqrt{3})^k$ for some $k \geqslant 3$
(xvi) $n = 5$ and $\alpha + 3$ is the rational part of $(4+\sqrt{15})^k$ for some $k \geqslant 2$
(xvii) $\alpha = n+2$ and $n+1$ is the square of the rational part of $(1+\sqrt{2})^{2k+1}$ for some $k \in \mathbb{N}$
(xviii) $\alpha = n+1$ and $n+1$ is twice a square
(xix) $\alpha = n+3$ is an even square
(xx) $\alpha = -n-3$, $n \equiv 0 \pmod 4$ and $n+1$ is a square
(xxi) $\alpha = -n-4$, $n \equiv 1 \pmod{24}$ and $(n+2)/3$ is a square
(xxii) $\alpha = -n-5$ and $n+2$ is the rational part of $(2+\sqrt{3})^{2k+1}$ for some $k \in \mathbb{N}$
(xxiii) $\alpha = -n-6$ and $n+3$ is the rational part of $(4+\sqrt{15})^{2k+1}$ for some $k \in \mathbb{N}$
(xxiv) $\alpha = -2n+4$ and $(2n-5)/3$ is the rational part of $(1+\sqrt{2})^{4k}$ for some $k \in \mathbb{N}$
(xxv) $\alpha = -2n$ and n is an odd square
(xxvi) $n = 4$ and $-\alpha - 3$ is the rational part of $(2+\sqrt{3})^k$ for some $k \geqslant 3$
(xxvii) $n = 5$ and $-\alpha - 3$ is the rational part of $(4+\sqrt{15})^k$ for some $k \geqslant 2$
(xxviii) $\alpha = -2n-4$ and $n+1$ is the square of the rational part of $(1+\sqrt{2})^{2k+1}$ for some $k \in \mathbb{N}$
(xxix) $\alpha = -2n-2$ and $(n+1)/2$ is the square of an odd number
(xxx) $\alpha = -2n-4$ and $n+3$ is an even square

The main result in [1] is the following.

Theorem 1. *There is a finite set $\mathcal{A}_0$ of pairs (n,α) such that* $\mathrm{Disc}(n,\alpha)$ *is a nonzero square if and only if (n,α) satisfies one of the properties (i)–(xxx) or $(n,\alpha) \in \mathcal{A}_0$.*

In this paper, we investigate as to how often the Galois group associated with $L_n^{(\alpha)}(x)$ is A_n, provided $\mathrm{Disc}(n, \alpha)$ is a square, where n and α are integers and $(n, \alpha) \notin \mathcal{A}_0$. In other words, our goal here is to classify pairs $(n, \alpha) \in \mathcal{A}_\infty$ such that the associated Galois group of $L_n^{(\alpha)}(x)$ is A_n.

Already a fair bit of information exists in the literature on when the Galois group of $L_n^{(\alpha)}(x)$ is A_n, for pairs (n, α) in $\mathcal{A}_\infty$. These results are compiled below, indicating when the Galois group of $L_n^{(\alpha)}(x)$ is A_n, where the pair (n, α) satisfies the indicated property listed among (i)–(xxx). Here we omit the trivial case $n = 1$ from our discussion, and for $n = 2$, we note that the associated Galois group is always A_2 (the trivial group), whenever $(2, \alpha) \in \mathcal{A}_\infty$.

- Case (ii), Filaseta, Kidd, Trifonov [4]
- Cases (iii) and (v), Schur [13–15]
- Cases (vi) and (xxi)–(xxiii), Hajir [7,9]
- Case (xx), Sell [16]
- Cases (viii)–(x), Banerjee, Filaseta, Finch, Leidy [1]

Thus we only need to consider cases (i), (iv), (vii), (xi)–(xix) and (xxiv)–(xxx).

Our main result in this paper is the following.

Theorem 2. *Let the integer pair (n, α) satisfy one of the properties (i)–(xxx) listed above. Then*

(i) *for $2 \leqslant n \leqslant 5$, the Galois group associated with $L_n^{(\alpha)}(x)$ is always A_n except for the cases $(n, \alpha) \in \{(4, -1), (4, 23)\}$. Both, $L_4^{(-1)}(x)$ and $L_4^{(23)}(x)$, have associated Galois group A_3, and*
(ii) *for $n \geqslant 6$, $L_n^{(\alpha)}(x)$ has Galois group A_n if and only if $L_n^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$.*

As a consequence of Theorem 2, the Galois group associated with $L_n^{(\alpha)}(x)$ is always A_n in cases (xiv)–(xvi) and (xxvi)–(xxvii), except when $n = 4$ and $\alpha = 23$ or, $n = 4$ and $\alpha = -1$. It follows from the result of Hajir and Wong [10] that, for all but finitely many α with $(5, \alpha) \in \mathcal{A}_\infty$, the Galois group associated with $L_5^{(\alpha)}(x)$ is A_5. Theorem 2 asserts that this finite set of exceptional values of $\alpha \in \mathbb{Z}$ such that the Galois group of $L_5^{(\alpha)}(x)$ is not A_5, is in fact, the empty set. It also follows from Theorem 2 that, in the remaining cases, $L_n^{(\alpha)}(x)$ has A_n as the Galois group, provided $L_n^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$. For pairs $(n, \alpha) \in \mathcal{A}_\infty$ with $n \geqslant 6$ and $\alpha < 0$, we only consider the values

$$\alpha = -2n - 4, \qquad \alpha = -2n - 2, \qquad \alpha = -2n \quad \text{and} \quad \alpha = -2n + 4.$$

As indicated in the list preceding Theorem 2, in the remaining cases (cases (vi) and (xx)–(xxiii)), Hajir [7,9] and Sell [16] have described the respective Galois groups.

Conditions (ii)–(xxx) in [1] were achieved by solving the Diophantine equation

$$\mathrm{Disc}(n,\alpha)=\prod_{j=2}^{n} j^j(\alpha+j)^{j-1}=\square.$$

After removing the obvious square factors in Schur's discriminant formula, the equation $\mathrm{Disc}(n,\alpha)=\square$ reduces to

$$\Delta(n,\alpha)=\prod_{2k+1\leqslant n}(2k+1)\prod_{2k\leqslant n}(\alpha+2k)=\square. \tag{1}$$

In order to prove part (i) of Theorem 2, we will use (1) for $n=4$ and $n=5$ in cases (xv), (xvi), (xxvi) and (xxvii). It is easy to check that for $n=4$ and $n=5$, (1) is equivalent to

$$(\alpha+2)(\alpha+4)=\begin{cases}3\,\square & \text{if } n=4\\ 15\,\square & \text{if } n=5.\end{cases} \tag{2}$$

Apart from cases (xv), (xvi), (xxvi) and (xxvii), $n=4$ and $n=5$ appear in the list above in pairs $(4,4)$ (case (ii)), $(5,1)$ (case (iii)), $(4,-1)$ (case (iv)), $(4,-5)$ (case (v)), $(5,-7)$ (case (vi)) and $(4,-10)$ (case (vii)). We have verified with Sage (Mathematical Software System) that, except for the pair $(4,-1)$, the Galois group associated with $L_n^{(\alpha)}(x)$ is A_n. The polynomial $L_4^{(-1)}(x)$ has Galois group A_3.

The proof of Theorem 2 will make use 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 $f(x)=\sum_{j=0}^{n}a_jx^j\in\mathbb{Q}[x]$ with $a_na_0\neq 0$, and let p be a prime. Let S be the set of points in the extended plane given by

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

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 $NP_p(f)$.

Newton polygons are extremely useful in studying algebraic properties of polynomials with rational coefficients. For $n\geqslant 3$, a polynomial in $\mathbb{Q}[x]$ must necessarily be irreducible in order for it to have A_n as the Galois group. We will refer to the following version of the celebrated Dumas criterion [3] in order to establish the irreducibility of $L_n^{(\alpha)}(x)$ for $n\geqslant 3$ in part (i) of Theorem 2.

Theorem 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.*

Observe that if a polynomial $f(x)$ with integer coefficients factors in $\mathbb{Z}[x]$ into polynomials of degrees $\geqslant 1$, then Theorem 3 tells us that for some factor $h(x) \in \mathbb{Z}[x]$, $h(0)$ must appear as the ordinate of some lattice point, different from the endpoints, on $NP_p(f)$, for any prime p. 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 over $\mathbb{Q}$. We will often exploit this fact in order to establish the irreducibility part in Theorem 2. As will be evident from Theorem 4 due to Hajir [8], the theory of Newton polygons also serves as an important tool in studying Galois groups of polynomials in $\mathbb{Q}[x]$. Before stating Hajir's theorem, we first need to introduce the notion of the Newton index of a polynomial.

Definition 1. Given $f(x) \in \mathbb{Q}[x]$, let $\mathcal{N}_f$, be called the *Newton index* of $f(x)$, be the least common multiple of the denominators (in lowest terms) of all slopes of $NP_p(f)$ as p ranges over all primes.

It is easy to see that for a given $f(x) \in \mathbb{Q}[x]$ the denominator of any slope of $NP_p(f)$ is 1 for all but finitely many primes p. That is to say that the Newton index is well defined.

Theorem 4 *(Hajir). Given an irreducible polynomial $f(x) \in \mathbb{Q}[x]$, $\mathcal{N}_f$ divides the order of the Galois group of $f(x)$. Moreover, if $\mathcal{N}_f$ has a prime divisor p in the range $(n/2, n-2)$, where n is the degree of $f(x)$, then the Galois group of $f(x)$ contains A_n. In that case, the Galois group of $f(x)$ is A_n if the discriminant of $f(x)$ is a rational square, and S_n otherwise.*

In other words, Theorem 4 implies that if $f(x) \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ and of degree n and that a prime in $(n/2, n-2)$ divides the slope of an edge of a Newton polygon of $f(x)$, then the Galois group of $f(x)$ over $\mathbb{Q}$ is A_n or S_n depending on whether the discriminant of $f(x)$ is a square in $\mathbb{Q}$ or not, respectively.

If a polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n \geqslant 3$ has associated Galois group A_n, then it is necessarily irreducible over $\mathbb{Q}$. In [9], Hajir, among other things, completely describes the irreducibility of $L_n^{(\alpha)}(x)$ for $n \in \{3,4\}$, and where $\alpha \in \mathbb{Q}$. We deduce from [9] that for $\alpha \in \mathbb{Q}$, $L_3^{(\alpha)}(x)$ is reducible over $\mathbb{Q}$ if and only if α is of the form

$$\alpha = \frac{m^3 - 9m - 6}{3m + 2}, \quad m \in \mathbb{Q},$$

and $L_4^{(\alpha)}(x)$ is reducible if and only if $\alpha \in \{-4, -3, -2, -1, 5, 23\}$. We will however establish the irreducibility of $L_3^{(\alpha)}(x)$, where $(n, \alpha) \in \mathcal{A}_\infty$, via a direct argument. For $n = 4$, we find that $(4, -1)$ and $(4, 23)$ are the only pairs listed in $\mathcal{A}_\infty$ for which $L_4^{(\alpha)}(x)$ is reducible, and these are the only exceptional pairs appearing in part (i) of Theorem 2. It is easily verified (using technology or otherwise) that the corresponding Galois group in these exceptional cases is in fact A_3.

We conclude this section with the discussion of the cases where $|\alpha| \leqslant 5$ and $(n, \alpha) \in \mathcal{A}_\infty$. From the list preceding Theorem 2, we already know for precisely when the Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ is A_n for $0 \leqslant \alpha \leqslant 5$. Also, for $\alpha < 0$, it follows from the identity

$$\mathcal{L}_n^{(\alpha)}(x) = x^{-\alpha}\mathcal{L}_{n+\alpha}^{(-\alpha)}(x), \quad |\alpha| \leqslant n$$

that the Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ is not A_n if $|\alpha| \leqslant n$. Thus, for $|\alpha| \leqslant 5$ and $n \geqslant 5$, the Galois group associated with $\mathcal{L}_n^{(\alpha)}(x)$ is not A_n. Furthermore, it can be verified that $\mathcal{L}_4^{(-5)}(x)$ has Galois group A_4 (see [14]). We have thus completely described the instances where the Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ is A_n for $|\alpha| \leqslant 5$, and where $(n, \alpha) \in \mathcal{A}_\infty$. Henceforth, we will assume $|\alpha| \geqslant 6$. Moreover, from the last identity, it follows that for pairs (n, α) satisfying condition (iv) in the list, that is, for $\alpha = -1$, the Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ is never A_n. This is the only exceptional case among (i)–(xxx), where the Galois group is never A_n. In fact, for $\alpha = -1$, one has

$$\mathcal{L}_n^{(-1)}(x) = x\mathcal{L}_{n-1}^{(1)}(x).$$

It now follows from Schur's work [14] that the Galois group associated with $\mathcal{L}_n^{(-1)}(x)$ is A_{n-1}, whenever $(n, -1) \in \mathcal{A}$.

In the next three sections to follow, we investigate in detail the Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ for $n = 3$, $n = 4$ and $n = 5$, respectively, and where $|\alpha| \geqslant 6$. We will only consider cases (xiv), (xv), (xvi), (xxvi) and (xxvii). Apart from these cases, the pair (n, α) with $n \in \{3, 4, 5\}$ and $|\alpha| \geqslant 6$, appears in $\mathcal{A}_\infty$ in cases (vi) (the pair $(n, \alpha) = (5, -7)$) and (vii) (the pair $(n, \alpha) = (4, -10)$). We easily find that the corresponding Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ is A_n in both cases. In Section 6, we will give a proof of part (ii) of Theorem 2.

3. Galois group in the case $n = 3$

It is well known that the Galois group over $\mathbb{Q}$ of a cubic in $\mathbb{Q}[x]$ is A_3 if and only if the cubic is irreducible over $\mathbb{Q}$ and its discriminant is a square in $\mathbb{Q}$. We already have for $(n, \alpha) \in \mathcal{A}_\infty$ that $\mathrm{Disc}(\mathcal{L}_n^{(\alpha)})$ is a square in $\mathbb{Z}$. Therefore in order to achieve our result in the case $n = 3$, it is enough to show that the polynomial $\mathcal{L}_3^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$.

For $n = 3$, we have

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

Setting $g(x) = \mathcal{L}_3^{(\alpha)}(x + \alpha + 3)$, we obtain

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

Now, for any prime divisor $p \neq 2$ of $\alpha+3$, $NP_p(g)$ has only one edge, joining the endpoints $(0, 0)$ and $(3, \nu_p(\alpha+3))$. Thus, in order that $g(x)$ is reducible, it follows from Theorem 3 that there must be at least one lattice point, other than the endpoints, on $NP_p(g)$. For this to be the case, one necessarily has $\nu_p(\alpha + 3) \equiv 0 \pmod 3$. Since this is the case for any prime divisor, except possibly for $p = 2$, we deduce that $\alpha+3 = \varepsilon 2^l t^3$, where $l \geqslant 0$, t are integers with $2 \nmid t$, and $\varepsilon \in \{1, -1\}$. Since $\varepsilon^3 = \varepsilon$, for any choice of ε, we may assume without loss of any generality that $\alpha + 3 = 2^l t^3$. Also, we have $t \neq 0$ as $|\alpha| \geqslant 6$ here. If we set $g_1(x) = g(tx)/t^3$, we have

$$g_1(x) = x^3 - 3 \cdot 2^l tx - 2^{l+1}.$$

For the monic cubic $g_1(x)$ to be reducible over $\mathbb{Q}$, it must have an integer root. One easily verifies that any integer root of $g_1(x)$ is of the form $\varepsilon 2^m$, where $0 \leqslant m \leqslant l + 1$ is an integer, and $\varepsilon \in \{1, -1\}$. Clearly, 1 is not a root of $g_1(x)$, and -1 is a root if and only if $t = 1$ and $l = 0$. But this gives $\alpha = -2$. Since we are interested in $|\alpha| \geqslant 6$, we may as well ignore the last solution. Next, we consider $m \geqslant 1$. Noting that $\varepsilon^3 = \varepsilon$, in this case, we have $\varepsilon 2^{3m} - 3\varepsilon t 2^{l+m} - 2^{l+1} = 0$. Since t is odd, one easily checks that the last equation holds only if either, $3m = l + 1$, $m = 1$ or, $3m = l + m$. In the case that $3m = l + 1$, we have $\varepsilon 2^{3m} - 3\varepsilon t 2^{4m-1} - 2^{3m} = 0$. After factoring 2^{3m}, one obtains

$$\varepsilon\bigl(1 - 3t2^{m-1}\bigr) = 1,$$

which clearly does not hold if $t \neq 0$, and that is the case here. If $m = 1$, then

$$2^3\varepsilon - 3\varepsilon t 2^{l+1} - 2^{l+1} = 0. \tag{3}$$

One readily sees that for (3) to hold, l must necessarily be in the set $\{0, 1, 2\}$. After solving (3) for these values of l, we find that $(\varepsilon, l, t) = (1, 0, 1)$ and $(\varepsilon, l, t) = (-1, 1, 1)$ are the only solutions to (3) corresponding to $t \neq 0$. None of these solutions yields any value in $|\alpha| \geqslant 6$, and we discard these solutions. Finally, in the case that $3m = l + m$, we have $\varepsilon 2^{3m} - 3\varepsilon t 2^{3m} - 2^{2m+1} = 0$. After factoring 2^{2m+1}, we have

$$\varepsilon 2^{m-1}(1 - 3\varepsilon t) = 1.$$

It is now easy to verify that there are no integral solutions to the last equation if $t \neq 0$.

Therefore we conclude that for $|\alpha| \geqslant 6$, $\mathcal{L}_3^{(\alpha)}(x)$ is irreducible, and, in particular, $\mathcal{L}_3^{(\alpha)}(x)$ has Galois group A_3, whenever $(3, \alpha) \in \mathcal{A}_\infty$.

4. Galois group in the case $n = 4$

For $n = 4$, the polynomial we are interested in is

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

where α satisfies the quadratic equation (2), that is,

$$(\alpha+2)(\alpha+4) = 3\,\square. \tag{4}$$

As noted in Section 2, we will concern ourselves with $|\alpha| \geqslant 6$ and $\alpha \neq 23$. For convenience, we will work with the translated polynomial $g(x) = f(x + \alpha + 4)$. Thus

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

Let the integers β and r be defined as

$$\beta := \begin{cases} \alpha & \text{if } \alpha > 0 \\ -\alpha & \text{if } \alpha < 0 \end{cases} \quad \text{and} \quad r := \begin{cases} 3 & \text{if } \alpha > 0 \\ -3 & \text{if } \alpha < 0. \end{cases}$$

Then from (4), we deduce that $\beta + r$ is the rational part of $(2 + \sqrt{3}\,)^k$, where k is some integer bigger than 2. Thus

$$\beta + r = \begin{cases} 2^k + \binom{k}{2}2^{k-2}\cdot 3 + \cdots + 3^{k/2} & \text{if } k \equiv 0 \pmod 2 \\ 2^k + \binom{k}{2}2^{k-2}\cdot 3 + \cdots + \binom{k}{k-1}2\cdot 3^{(k-1)/2} & \text{if } k \equiv 1 \pmod 2. \end{cases}$$

From this description of $\beta + r$, we immediately deduce that, if k is odd, then $2 \parallel (\beta + r)$ and $\beta \equiv -1 - r \pmod 3$. If k is even, then $\beta \equiv 1 - r \pmod 3$ and that 2 exactly divides one of $\beta + r + 1$ and $\beta + r - 1$ while 4 divides the other. Based on this information, we have from (4) the following.

Lemma 1. *Let the integers β and r be as described above. Then there are integers y and z such that*

(i) *if β is odd, then $(\beta + r - 1, \beta + r + 1) = (y^2, 3z^2)$, where $y \equiv z \equiv 1 \pmod 2$, and*
(ii) *if β is even, then $(\beta + r - 1, \beta + r + 1) = (6y^2, 2z^2)$, where $y \not\equiv z \pmod 2$.*

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, define the resolvent cubic $R_h(x)$ to be 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 [11] 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

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

Resolvent cubics are particularly useful in computing Galois groups of quartic polynomials over number fields. In order to show that the Galois group of $g(x)$ is A_4, we will first need to establish the irreducibility of $g(x)$. As noted in Section 2, Hajir has already established the irreducibility of $L_4^{(\alpha)}(x)$ for pairs $(4, \alpha) \in \mathcal{A}_\infty$ with $|\alpha| \geqslant 6$ and $\alpha \neq 23$.

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

$$R'_g(x) = x^3 - 6(\alpha + 4)(\alpha + 3)x - 4(\alpha + 4)^2(\alpha + 3).$$

For Galois group computations, we will refer to the following result of Kappe and Warren [11].

Theorem 5 *(Kappe–Warren). Let $k(x)$ be an irreducible quartic polynomial in $\mathbb{Q}[x]$, and $R_k(x)$ be its resolvent cubic. Then, the Galois group of $k(x)$ over $\mathbb{Q}$ is A_4 if and only if $R_k(x)$ is irreducible over $\mathbb{Q}$, and the discriminant of $k(x)$ (which is equal to the discriminant of $R_k(x)$) is a square in $\mathbb{Q}$.*

In the following lemma, we establish the irreducibility of $R'_g(x)$.

Lemma 2. *For every integer α satisfying (4), the polynomial $R'_g(x) = x^3 - 6(\alpha + 4)(\alpha + 3)x - 4(\alpha + 4)^2(\alpha + 3)$ is irreducible over $\mathbb{Q}$.*

Proof. If $R'_g(x)$ is reducible over $\mathbb{Q}$, then it has an integer root. Let $a \in \mathbb{Z}$ be a root of $R'_g(x)$. As noted earlier, $2 \parallel (\alpha + 3)$ whenever α is odd and satisfies (4). Thus, for odd α, the Newton polygon $NP_2(R'_g)$ has only one edge, joining the endpoints $(0, 0)$ and $(3, 3)$. Now, from Dumas criterion, we deduce that the sole edge of $NP_2(x - a)$ has slope equal to 1. This, in other words, means that $2 \parallel a$. Furthermore, from $h(a)/8 = 0$, we have

$$(a/2)^2 - 3(\alpha + 4)\big((\alpha + 3)/2\big)(a/2) - (\alpha + 4)^2\big((\alpha + 3)/2\big) = 0.$$

But this is impossible as an odd number of terms on the left hand side above are odd.

In the case that α is even, we let p denote a prime divisor of $\beta + r$. Clearly, $p \neq 2$. Also, $p \neq 3$ as $\beta \equiv 1 - r \pmod 3$ with $r \in \{3, -3\}$. Therefore $NP_p(R'_g)$ has just one edge, that joining the endpoints $(0, 0)$ and $(3, \nu_p(\beta + r))$. Once again, we deduce from Dumas criterion that $\nu_p(\beta + r) \equiv 0 \pmod 3$ in order for $R'_g(x)$ to be reducible over $\mathbb{Q}$. Since this is the case for every prime divisor of $\beta + r$, we conclude that $\beta + r = t^3$ for some odd integer t. We also have from Lemma 1 that $\beta + r + 1 = 2z^2$ for some integer z.

Now, from the identity $(\beta+r+1)-(\beta+r)=1$, it follows that (t,z) is an integral point on the elliptic curve

$$2Z^2 = T^3 + 1. \tag{5}$$

Cohn [2] has shown that, apart from the trivial solutions $(T,Z)=(-1,0)$ and $(T,Z)=(1,\pm 1)$, $(T,Z)=(23,\pm 78)$ are the only other integral points on (5). It is easy to check that $T=\pm 1$ do not yield positive values in $\beta=|\alpha|\geqslant 6$. Since 3 does not divide $\beta+r+1=2z^2$, we may as well ignore $(T,Z)=(23,\pm 78)$. Thus we have proved the assertion of our lemma. $\square$

This concludes the proof of Theorem 2 in the case $n=4$.

5. Galois group in the case $n = 5$

For $n=5$ and $\alpha\in\mathbb{Z}$, the n-th normalized Laguerre polynomial is given by

$$\begin{aligned} f(x) = \mathcal{L}_5^{(\alpha)}(x) = x^5 &- 5(\alpha+5)x^4 + 10(\alpha+5)(\alpha+4)x^3 \\ &- 10(\alpha+5)(\alpha+4)(\alpha+3)x^2 \\ &+ 5(\alpha+5)(\alpha+4)(\alpha+3)(\alpha+2)x \\ &- (\alpha+5)(\alpha+4)(\alpha+3)(\alpha+2)(\alpha+1), \end{aligned}$$

where α satisfies (2), that is,

$$(\alpha+2)(\alpha+4) = 15\,\square. \tag{6}$$

As noted earlier, we need only consider $|\alpha|\geqslant 6$. Sometimes, we will work with the translated polynomial $g(x)=f(x+\alpha+5)$ instead, that is, work with the following polynomial.

$$g(x) = x^5 - 10(\alpha+5)x^3 - 20(\alpha+5)x^2 + 15(\alpha+5)(\alpha+3)x + 4(\alpha+5)(5\alpha+19).$$

Similarly to the case $n=4$, we define

$$\beta := \begin{cases} \alpha & \text{if } \alpha > 0 \\ -\alpha & \text{if } \alpha < 0, \end{cases} \quad \text{and} \quad r := \begin{cases} 3 & \text{if } \alpha > 0 \\ -3 & \text{if } \alpha < 0. \end{cases}$$

Then $\beta+r$ is the rational part of $(4+\sqrt{15}\,)^k$, where k is some integer bigger than 2, that is,

$$\beta + r = \begin{cases} 4^k + \binom{k}{2}4^{k-2}\cdot 15 + \cdots + 15^{k/2} & \text{if } k \equiv 0 \pmod 2 \\ 4^k + \binom{k}{2}4^{k-2}\cdot 15 + \cdots + \binom{k}{k-1}4\cdot 15^{(k-1)/2} & \text{if } k \equiv 1 \pmod 2). \end{cases}$$

From the above description of $\beta + r$, we deduce that $\beta \equiv 1 - r \pmod 3$. Furthermore, for odd β (i.e., for even k), we have $\beta \equiv -1 - r \pmod 5$ and that $4 \parallel (\beta + r)$, while 2 exactly divides $\beta + r \pm 2$. In the case that β is even, one has $\beta \equiv 1 - r \pmod 5$ and it is easily seen that 4 divides one of $\beta + r \pm 1$, and 2 exactly divides the other. Based on this information and Eq. (6), we have the following.

Lemma 3. *Let the integers β and r be as described above. Then there are integers y and z such that*

(i) *if β is odd, then $(\beta + r - 1, \beta + r + 1) = (3y^2, 5z^2)$, where $y \equiv z \equiv 1 \pmod 2$, and*
(ii) *if β is even, then $(\beta + r - 1, \beta + r + 1) = (30y^2, 2z^2)$, where $y \not\equiv z \pmod 2$.*

We also set

$$s = \begin{cases} 5 & \text{if } \alpha > 0 \\ -5 & \text{if } \alpha < 0. \end{cases}$$

Observe that

$$\beta + r \equiv 1 + 3k + \frac{15k(k-1)}{2} \equiv 1 + 3k^2 \pmod 9.$$

Thus, if $\alpha > 0$, then $\beta + s = \beta + r + 2$, which is 3 or 6 mod 9; and $3 \nmid (\beta + s)$ if $\alpha < 0$. Moreover, if β is odd, then $2 \parallel (\beta + s)$ and that $\beta + s$ is odd if β is even.

Suppose that $f(x)$ is reducible over $\mathbb{Q}$, and $h(x) \in \mathbb{Q}[x]$ is an irreducible factor of $f(x)$. Without loss of any generality, we may assume $h(x) \in \mathbb{Z}[x]$ and is monic. Let $p \notin \{2, 3\}$ be a prime divisor of $\beta + s$. Then we find that the Newton polygon $NP_p(f)$ of $f(x)$ with respect to p has only one edge, joining the endpoints $(0, 0)$ and $(5, \nu_p(\beta + s))$. By Dumas criterion, $h(0)$ $(\in \mathbb{Z})$ must appear as the ordinate of some lattice point on $NP_p(f)$. In order for this to be the case, we must have $\nu_p(\beta + s) \equiv 0 \pmod 5$. Therefore, assuming reducibility of $f(x)$, we have the following description of $\beta + s$.

$$\beta + s = \begin{cases} 6\,x^5 & \text{if } \beta \equiv 1 \pmod 2 \text{ and } \alpha > 0 \\ 3\,x^5 & \text{if } \beta \equiv 0 \pmod 2 \text{ and } \alpha > 0 \\ 2\,x^5 & \text{if } \beta \equiv 1 \pmod 2 \text{ and } \alpha < 0 \\ x^5 & \text{if } \beta \equiv 0 \pmod 2 \text{ and } \alpha < 0 \end{cases} \tag{7}$$

for some odd integer x. Observe that for the y and z appearing in Lemma 3 and the x above, one has $\gcd(x, y) = \gcd(y, z) = \gcd(z, x) = 1$.

We next show that the polynomial $f(x) = \mathcal{L}_5^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$ under the assumptions of Lemma 3 on β. We will make use of the description of $\beta + s$ above, in order to arrive at a contradiction.

5.1. Irreducibility of $\mathcal{L}_5^{(\alpha)}(x)$

We consider different cases depending on various signs and parities of α.

Case (i) $\alpha > 0$ is odd: In this case, observing that $(\beta + s) - (\beta + r - 1) = 3$, we have from Lemma 3 and (7) that $6x^5 - 3y^2 = 3$, which after factoring 3 reduces to

$$2x^5 - y^2 = 1. \tag{8}$$

Working in $\mathbb{Z}[i]$, we show that $(x, y) = (1, \pm 1)$ are the only solutions to Eq. (8). Rewriting (8), we have

$$(1 + i)(1 - i)x^5 = (y + i)(y - i).$$

Now, $1 + i$ being a prime in the unique factorization domain (UFD) $\mathbb{Z}[i]$, it must divide $y + i$ or $y - i$. Without loss of any generality, let us assume $1 + i$ divides $y + i$ (otherwise one can replace y by $-y$) and $1 - i$ divides $y - i$. Since x and y are odd in this case with $\gcd(x, y) = 1$, we have $\gcd(\frac{y+i}{1+i}, \frac{y-i}{1-i}) = 1$. Also, if ε in $\mathbb{Z}[i]$ is a unit, then $\varepsilon = \varepsilon^5$. Thus in the UFD $\mathbb{Z}[i]$, both $\frac{y+i}{1+i}$ and $\frac{y-i}{1-i}$ are 5-th powers. Therefore there are integers a and b such that

$$\frac{y + i}{1 + i} = \frac{y + 1 + (y - 1)i}{2} = (a + bi)^5 = a^5 - 10a^3b^2 + 5ab^4 + \left(5a^4b - 10a^2b^3 + b^5\right)i.$$

Comparing the real and imaginary parts on either side, we have from the identity $(y + 1)/2 - (y - 1)/2 = 1$ that

$$\left(a^5 - 10a^3b^2 + 5ab^4\right) - \left(5a^4b - 10a^2b^3 + b^5\right) = 1,$$
$$\text{i.e., } (a - b)\left(a^4 - 4a^3b - 14a^2b^2 - 4ab^3 - b^4\right) = 1.$$

Since a and b are integers, we deduce that $a - b = \pm 1$. It is easy to check that $(a, b) = (1, 0)$ and $(a, b) = (0, -1)$ are the only solutions to the above equation, giving us $y = 1$ and $y = -1$, respectively. These values of y correspond to $\alpha = 1$, which maybe ignored since we are interested in $|\alpha| \geqslant 6$.

Case (ii) $\alpha > 0$ is even: Similarly to the previous case, we consider $(\beta + s) - (\beta + r - 1) = 3$. This, by Lemma 3 and (7), gives us the following equation.

$$x^5 - 10y^2 = 1. \tag{9}$$

Working in the ring $R = \mathbb{Z}[\sqrt{-10}\,]$, we will show that the affine algebraic curve (9) has no nontrivial integral points on it. Here, we note that, although R is not a UFD, there is always a unique factorization of ideals of R into products of prime ideals. Writing $\delta = \sqrt{-10}$, we have from (9) the following ideal factorization in R.

$$(x)^5 = (1 + y\delta)(1 - y\delta).$$

Here, (x), $(1 + y\delta)$ and $(1 - y\delta)$ are the principal ideals generated by the respective elements in R. Since both x and y are odd, the ideals $(1 + y\delta)$ and $(1 - y\delta)$ have no common prime ideal factor in R. It follows from unique factorization of ideals in R that both $(1+y\delta)$ and $(1-y\delta)$ are 5-th powers of some ideals in R. Thus $(1+y\delta) = I^5$, for some ideal I of R. Since the ideal class group of R is cyclic of order 2 (see for example [17]), we deduce that the ideal classes of $I^5 = I^2 \cdot I^2 \cdot I$ and I, are the same. Since $I^5 = (1+y\delta)$ is principal, so is I. Let $I = (c + d\delta)$, where c and d are integers. Since ± 1 are the only units in R, and $-1 = (-1)^5$, we may assume without loss of generality that

$$1 + y\delta = (c + d\delta)^5 = c^5 - 100c^3d^2 + 500cd^4 + \big(5c^4d - 100c^2d^3 + 100c^5\big)\delta.$$

Comparing the rational parts on both sides above, we get the following.

$$c\big(c^4 - 100c^2d^2 + 500d^4\big) = 1.$$

Since c and d are integers, we deduce that the only possible values of c satisfying the above equation are $c = \pm 1$. $c = 1$ gives $d = 0$, and, hence, $y = 0$. Therefore we may discard this solution since from $y = 0$, one obtains $\alpha + 2 = 0$, whereas we are concerned with $\alpha > 0$ here. $c = -1$ does not give a valid (integral) solution for d, and, as such in y. Since the α under consideration is positive, we conclude that $\mathcal{L}_5^{(\alpha)}(x)$ is irreducible in this case.

Thus we have established the irreducibility of $\mathcal{L}_5^{(\alpha)}(x)$ over $\mathbb{Q}$ in the case $\alpha > 0$.

Case (iii) $\alpha < 0$ is odd: Working similarly to the previous cases, we consider the identity $(\beta + r + 1) - (\beta + s) = 3$. This, by Lemma 3 and (7), gives us the quintic curve $5z^2 - 2x^5 = 3$. We will show that $(x, z) = (1, \pm 1)$ are the only integral points on this curve that correspond to a possibly reducible $\mathcal{L}_5^{(\alpha)}(x)$. One verifies that $(x, z) = (1, \pm 1)$ correspond to $\beta = 7$. A quick inspection of the Newton polygon of $\mathcal{L}_5^{(-7)}(x)$ with respect to 2, and then using the rational root test (or otherwise), one can easily verify that $\mathcal{L}_5^{(-7)}(x)$ is irreducible over $\mathbb{Q}$. In the case that $(x, z) \neq (1, \pm 1)$, let us write 3 as $5 - 2$. After rearranging terms on both sides of $5z^2 - 2x^5 = 3$, we have

$$5\big(z^2 - 1\big) = 2(x - 1)(x - \omega)\big(x - \omega^2\big)\big(x - \omega^3\big)\big(x - \omega^4\big), \tag{10}$$

where $\omega = \zeta_5$ is the fifth root of unity. Since the prime $1 - \omega$ divides 5 in the UFD $\mathbb{Z}[\omega]$, the ring of integers in $\mathbb{Q}[\omega]$, $1 - \omega$ divides the right hand side of (10). Now, $1 - \omega$ being a prime in $\mathbb{Z}[\omega]$, divides $x - \omega^j$ for some $j \in \{0, 1, 2, 3, 4\}$. Also, from $x - \omega^k = x - \omega^j + \omega^j(1 - \omega^{k-j})$, we see that $1 - \omega$ divides $x - \omega^j$ for any $j \in \{0, 1, 2, 3, 4\}$. Therefore $(1 - \omega)^5$ divides the right hand side of (10). After taking norms, we find that $z^2 \equiv 1 \pmod 5$. Thus

$$\beta + r + 1 = 5z^2 \equiv 5 \pmod{25},$$

that is, $5 \parallel (\beta + r + 1)$. Thus, for $\alpha > 0$, $5 \parallel (\alpha + 4)$; and $5 \parallel (\alpha + 2)$ if $\alpha < 0$. Hence, the Newton polygon $NP_5(f)$ of $f(x) = \mathcal{L}_5^{(\alpha)}(x)$ has just one edge, joining points $(0, 0)$ and $(5, 1)$. As there are no lattice points on this edge other than the terminal points, we conclude from Theorem 3 that the polynomial $f(x)$ is irreducible.

Case (iv) $\alpha < 0$ is even: In this case, we begin by considering the identity $(\beta + r - 1) - (\beta + s) = 1$. From Lemma 3, (7) and the last identity, we have in this case the following hyper-elliptic curve.

$$30y^2 = x^5 + 1 = (x + 1)(x + \omega)\bigl(x + \omega^2\bigr)\bigl(x + \omega^3\bigr)\bigl(x + \omega^4\bigr), \tag{11}$$

where $\omega = \zeta_5$ is the fifth root of unity. As in the previous case, we deduce that $1 - \omega$ divides $x + \omega^j$, for $j \in \{0, 1, 2, 3, 4\}$. Furthermore, 6 does not divide $(x + \omega)(x + \omega^2)(x + \omega^3)(x + \omega^4) = x^4 - x^3 + x^2 - x + 1$ for any $x \in \mathbb{Z}$. Thus, we have

$$x + \omega^j = \varepsilon_j(1 - \omega)u_j^2, \quad \text{for } 1 \leqslant j \leqslant 4,$$

where ε_j is a unit in $\mathbb{Z}[\omega]$, and $u_j \in \mathbb{Z}[\omega]$. We note that for $\omega = \zeta_5$, the units in $\mathbb{Z}[\omega]$ are of the form $\pm\omega^h(1 + \omega)^k$, where $0 \leqslant h \leqslant 4$, and $k \in \mathbb{Z}$. Since ω^i is a square in $\mathbb{Z}[\omega]$ for every $i \in \mathbb{Z}$, and since $(1 + \omega)^{-1} = (1 + \omega) \cdot \frac{1}{(1+\omega)^2}$ with $\frac{1}{(1+\omega)^2} \in \mathbb{Z}[\omega]$ ($1 + \omega$ being a unit in $\mathbb{Z}[\omega]$), we may assume without loss of generality that

$$\varepsilon_1 = \varepsilon \quad \text{or} \quad \varepsilon_1 = \varepsilon(1 + \omega); \quad \text{where } \varepsilon \in \{1, -1\}.$$

First, let us deal with the case that $\varepsilon_1 = \varepsilon$. In this case, we have

$$x + \omega = \varepsilon(1 - \omega)u_1^2. \tag{12}$$

Let $u_1 = a + b\omega + c\omega^2 + d\omega^3$, where a, b, c and d are integers. Then

$$\begin{aligned} u_1^2 = {} & a^2 + 2cd - c^2 - 2bd + \bigl(d^2 + 2ab - c^2 - 2bd\bigr)\omega \\ & + \bigl(b^2 + 2ac - c^2 - 2bd\bigr)\omega^2 + \bigl(2ad + 2bc - c^2 - 2bd\bigr)\omega^3. \end{aligned}$$

Applying the automorphism $\omega \to \omega^2$ to (12) and denoting the image of u_1 under this map by U_1, one has

$$x + \omega^2 = \varepsilon\bigl(1 - \omega^2\bigr)U_1^2. \tag{13}$$

Subtracting (13) from (12), we obtain

$$\varepsilon\omega(1 - \omega) = (1 - \omega)\bigl(u_1^2 - (1 + \omega)U_1^2\bigr),$$

that is,

$$\varepsilon\omega = u_1^2 - (1+\omega)U_1^2.$$

If we write $u_1^2 = A + B\omega + C\omega^2 + D\omega^3$ with A, B, C, $D \in \mathbb{Z}$, then it is easy to verify that under the action $\omega \to \omega^2$, one has

$$U_1^2 = A + D\omega + B\omega^2 + C\omega^4,$$

and, hence,

$$(1+\omega)U_1^2 = A + (D - C + A)\omega + (B - C + D)\omega^2 + (B - C)\omega^3.$$

Thus

$$\varepsilon\omega = u_1^2 - (1+\omega)U_1^2 = (B + C - A - D)\omega + (2C - B - D)\omega^2 + (D + C - B)\omega^3.$$

Writing A, B, C and D in terms of a, b, c and d, and comparing the coefficients of 1, ω, ω^2, and ω^3 on either side, we have

$$d^2 + b^2 - a^2 + 2ab + 2ac - 2bc - 2ad - 2cd = \varepsilon, \tag{14}$$

$$2b^2 - d^2 + 4ac - 2ab - 2ad - 2bc = 0, \tag{15}$$

and

$$b^2 - c^2 - d^2 + 2ac + 2ad + 2bc - 2ab - 2bd = 0. \tag{16}$$

Adding (14) and (16), we have

$$2b^2 - a^2 - c^2 + 4ac - 2cd - 2bd = \varepsilon.$$

From (15), we find that d is even, and from the last equation, we deduce that a and c have opposite parities.

Note that x in (12) is odd. Now, working mod 2 in $\mathbb{Z}[\omega]$, we have from (12) that

$$1 + \omega \equiv (1+\omega)\bigl(a^2 + c^2 + c^2\omega + \bigl(1 + c^2\bigr)\omega^2 + c^2\omega^3\bigr) \pmod 2. \tag{17}$$

First, we consider the case where c is even and a is odd. Then from (17), we find that

$$1 + \omega \equiv (1+\omega)\bigl(1+\omega^2\bigr) \pmod 2, \quad \text{i.e.,} \quad \omega^2(1+\omega) \equiv 0 \pmod 2.$$

But this is impossible as ω^2 and $1+\omega$ are units in $\mathbb{Z}[\omega]$, and 2 is not a unit. Similarly, if c is odd and a is even, one has from (17) that

$$1 + \omega \equiv (1+\omega)\bigl(1+\omega+\omega^3\bigr) \pmod 2, \quad \text{i.e.,} \quad \omega(1+\omega)\bigl(1+\omega^2\bigr) \equiv 0 \pmod 2.$$

This is a contradiction as ω, $1+\omega$ and $1+\omega^2$ are all units in $\mathbb{Z}[\omega]$.

Next, we consider the case that $\varepsilon_1 = \varepsilon(1+\omega)$. The equation we are interested in is

$$x + \omega = \varepsilon(1-\omega)(1+\omega)u_1^2. \tag{18}$$

Under $\omega \to \omega^2$, we obtain from (18) that

$$x + \omega^2 = \varepsilon\bigl(1-\omega^2\bigr)\bigl(1+\omega^2\bigr)U_1^2 = -\varepsilon(1-\omega)\omega^4 U_1^2. \tag{19}$$

Working mod $1-\omega$, we find from $u_1 = a + b\omega + c\omega^2 + d\omega^3$ that

$$u_1^2 \equiv (a+b+c+d)^2 \pmod{1-\omega}.$$

Also,

$$U_1^2 = \bigl(a + b\omega^2 + c\omega^4 + d\omega\bigr)^2 \equiv (a+b+c+d)^2 \pmod{1-\omega}.$$

Therefore $u_1^2 \equiv U_1^2 \pmod{1-\omega}$. Subtracting (19) from (18) and after dividing throughout by $1-\omega$, we have

$$\varepsilon\omega = (1+\omega)u_1^2 + \omega^4 U_1^2.$$

In the ring $\mathbb{Z}/(5) \cong \mathbb{Z}[\omega]/(1-\omega)$, the above equation is

$$3\,u^2 \equiv \varepsilon \pmod 5,$$

where u^2 is the image of $u_1^2 = U_1^2$ (considered as elements of $\mathbb{Z}[\omega]/(1-\omega)$) in $\mathbb{Z}/(5)$. Thus

$$u^2 \equiv 2\varepsilon \pmod 5,$$

which is impossible, since squares mod 5 are, 0 and ε. Therefore, we conclude that Eq. (11) has no nontrivial integral solution. It is easily seen that the trivial solution $(x,y) = (-1,0)$ gives $\beta = 5$, which we may ignore, since we are only considering $\beta \geqslant 6$ here.

5.2. Galois group of $\mathcal{L}_5^{(\alpha)}(x)$

Now that we have already shown $\mathcal{L}_5^{(\alpha)}(x)$ is irreducible, whenever $(5,\alpha) \in \mathcal{A}_\infty$, our next task is to establish that the Galois group of $\mathcal{L}_5^{(\alpha)}(x)$ is always A_5 in these cases. We achieve this by showing that 3 divides the Newton index $\mathcal{N}_{\mathcal{L}_5^{(\alpha)}}$, whenever the pair $(5,\alpha)$ is in $\mathcal{A}_\infty$. Hence, as a consequence of Theorem 4, 3 divides the order of the Galois group of $\mathcal{L}_5^{(\alpha)}(x)$. Let us denote this Galois group by G. Since $\mathcal{L}_5^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$, G must be a transitive subgroup of S_5, the symmetric group on 5 letters. Thus 15 divides $|G|$. We claim that $|G| \geqslant 60$, and, as such, $G = A_5$ or $G = S_5$. Otherwise,

$|G| = 30$ or $|G| = 15$. If $|G| = 30$, we note that G is not a subgroup of A_5. This is because for $n \geqslant 5$, A_n is simple and $|A_5|/|G| = 2$. But then there is subgroup H of order 15 of G (the kernel of the signature map of G to $\{\pm 1\}$, the multiplicative cyclic group of order 2). A straightforward application of Sylow's theorem shows that H is abelian, generated by a 3-cycle and a 5-cycle. On the contrary, in S_5, a 3-cycle σ and a 5-cycle τ do no commute. To see this, let $k \in \{1,2,3,4,5\}$ be such that $\sigma(k) \neq k$ Now, consider the element $\sigma(k) \in \{1,2,3,4,5\}/\{k\} = \{\tau^i(k)\colon\ 1 \leqslant i \leqslant 4\}$. Let $\sigma(k) = \tau^j(k)$ for some $1 \leqslant j \leqslant 4$. If σ and τ commute, we have

$$k = \sigma^3(k) = \sigma^2\tau^j(k) = \tau^j\sigma^2(k) = \tau^j\sigma\sigma(k) = \tau^j\sigma\tau^j(k) = \tau^{2j}\sigma(k) = \tau^{3j}(k).$$

Since τ is a 5-cycle, we deduce that $j \equiv 0 \pmod 5$, whereby we get a contradiction. Therefore $|G| \neq 30$. With exactly similar reasoning, we further deduce that $|G| \neq 15$. Thus the only possibility is that $|G| = 60$ or $|G| = 120$. Consequently, $G = A_5$ or $G = S_5$. Thus $\mathcal{L}_5^{(\alpha)}(x)$ has Galois group A_5, whenever the pair $(5, \alpha)$ is in $\mathcal{A}_\infty$.

First, let us investigate the case that α is a positive integer. We show that 3 divides the Newton index $\mathcal{N}_g$ of the polynomial $g(x) = f(x + \alpha + 5)$, defined at the beginning of the section. Let us consider the Newton polygon $NP_3(g)$. For $\alpha > 0$, it follows from the discussion preceding Lemma 3 that, $\alpha + 2 = \beta + r - 1 \equiv 0 \pmod 3$, so that $5\alpha + 19 = 5(\alpha + 2) + 9 \equiv 0 \pmod 3$. Let us set $\nu_3(5\alpha + 19) = l \geqslant 1$. As noted earlier, we have in this case that $\alpha + 5 = \beta + s$, which is 3 or 6 mod 9. In any case, we have that $\nu_3(\alpha + 5) = 1$. Thus the Newton polygon $NP_3(g)$ has two edges, the first edge joining $(0,0)$ and $(3,1)$, and the other edge joining $(3,1)$ and $(5, l+1)$. Clearly, 3 divides the denominator of the slope of the edge joining $(0,0)$ and $(3,1)$. This concludes our proof for $\alpha > 0$.

As for computing the Galois group in the case $\alpha < 0$, we note that for any prime divisor $p \neq 2$ of $\beta + r$ $(-(\alpha + 3))$, $NP_p(f)$ has two edges, one joining points $(0,0)$, $(2,0)$, and the other joining $(2,0)$, $(5, \nu_p(\beta + r))$.

Thus, if $3 \nmid \nu_p(\beta + r)$, then the slope of the edge of $NP_p(f)$, joining $(2,0)$ and $(5, \nu_p(\beta + r))$, has 3 in the denominator. It now follows from Theorem 4, that 3 divides the order of the Galois group of $f(x)$, and, thereby allowing us to conclude that $f(x)$ has A_5 as the Galois group. Otherwise, if $3 \mid \nu_p(\beta + r)$ for every prime divisor $p \neq 2$ of $\beta + r$, then from Lemma 3, we have

$$\beta + r = \begin{cases} 4t^3 & \text{if } \beta \equiv 1 \pmod 2 \\ t^3 & \text{if } \beta \equiv 0 \pmod 2, \end{cases}$$

for some odd integer t. If β is odd, then from $(\beta + r) - (\beta + r - 1) = 1$ and Lemma 3, we obtain that

$$4t^3 - 3y^2 = 1. \tag{20}$$

Putting $T = 48\,t$ and $Y = 288\,y + 4$, we have the following (isomorphic) minimal Weierstrass model for (20).

$$Y^2 + Y = T^3 - 7.$$

The last elliptic curve has conductor 27, and a quick glance at the Cremona's table reveals that the group of rational points on this curve has rank 0, and its torsion part is cyclic of order 3. Therefore, we conclude that the only integer points on our affine curve (20) are $(1, \pm 1)$. These points correspond to $\beta = 7$. We verified with Maple (mathematical software system) that $\mathcal{L}_5^{(-7)}(x)$ has Galois group A_5.

For the case where β is even, we have from $(\beta + r) - (\beta + r - 1) = 1$ and Lemma 3, the elliptic curve

$$t^3 - 2z^2 = -1. \tag{21}$$

One verifies that $(t, z) = (-1, 0)$, $(t, z) = (1, \pm 1)$ and $(t, z) = (23, \pm 78)$ (see [2] for details) are the only integral solutions to (21). We can discard the last two solutions, $(23, \pm 78)$ as we have already noted that 3 does not divide

$$\beta + r - 1 = 2z^2$$

in the discussion preceding Lemma 3. The equation $(t, z) = (-1, 0)$ gives $\beta = 2$, and $(t, z) = (1, \pm 1)$ yields $\beta = 4$. We may ignore these values of β as well, since only $\beta \geqslant 6$ are being considered here.

6. Galois group in the case $n \geqslant 6$

As noted in Section 2, we only need to consider cases (i), (iv), (vii), (xi)–(xix) and (xxiv)–(xxx). We further recall from Section 2 that we may assume $|\alpha| \geqslant 6$. Since we are interested in $n \geqslant 6$ in this section, we restrict ourselves to cases (vii), (xi)–(xii), (xvii)–(xix), (xxiv)–(xxv) and (xxviii)–(xxx). Let us denote the set of pairs (n, α) listed in these cases by $\mathcal{A}'_\infty$. We first consider the case that $\alpha > 0$. Set

$$g(x) = \mathcal{L}_n^{(\alpha)}(x) = \sum_{j=0}^{n} b_j x^j,$$

where

$$b_j = (-1)^{n+j} \binom{n}{j} (n + \alpha)(n - 1 + \alpha) \cdots (j + 1 + \alpha).$$

Let us denote $(n + \alpha)(n - 1 + \alpha) \cdots (j + 1 + \alpha)$ by a_j. Thus $b_j = (-1)^{n+j} \binom{n}{j} a_j$. First, we derive a criteria for $\mathcal{L}_n^{(\alpha)}(x)$ to have the associated Galois group containing A_n in the case that $\alpha > 0$, and where $(n + \alpha)/3 < 1 + \alpha$.

Lemma 4. *Let n and α be positive integers with $n < 2\alpha + 3$ such that there is a prime in the interval $((n+\alpha)/3, 1+\alpha)$. Then the Galois group of $\mathcal{L}_n^{(\alpha)}(x)$ over $\mathbb{Q}$ contains A_n, provided that $\mathcal{L}_n^{(\alpha)}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Let us set $g(x) = \mathcal{L}_n^{(\alpha)}(x)$. We show that if there is prime p in the interval $((n+\alpha)/3, 1+\alpha)$, then the Newton polygon $NP_p(g)$ of $g(x)$ with respect to p has two edges with p dividing the denominator of the slope of one of these edges. Since this p is in the interval $(n/2, n-2)$, it follows from Theorem 4 in Section 2 that $g(x)$ has Galois group A_n, provided $g(x)$ is irreducible over $\mathbb{Q}$.

Suppose that there is a prime $p \in ((n+\alpha)/3, 1+\alpha)$. Clearly, p does not appear as one of the factors in the expression for a_j. Also, from $3p > n+\alpha$, we find that $3p$ does not appear as a factor in the expression for a_j either. Thus $\nu_p(a_j) \leqslant 1$ for all $j = 0, 1, \ldots, n$. Also, $\nu_p(a_j) = 1$, whenever $2p$ appears as one of the factors in the expression for a_j. This is the case if $2p \geqslant j + 1 + \alpha$, that is, when $j \leqslant 2p - 1 - \alpha$. It is easy to check that $\binom{n}{j} \equiv 0 \pmod{p}$ if and only if $n - p + 1 \leqslant j \leqslant p - 1$. In fact, for the p under consideration, $\nu_p\big(\binom{n}{j}\big) = 1$ for $n - p + 1 \leqslant j \leqslant p - 1$.

For our choice on the size of p, we have

$$n - p < 2p - 1 - \alpha < p - 1 < n.$$

From the above discussion, it follows that

$$\nu_p(b_j) = \begin{cases} 1 & \text{if } 0 \leqslant j \leqslant n-p \\ 2 & \text{if } n-p < j \leqslant 2p-1-\alpha \\ 1 & \text{if } 2p-1-\alpha < j \leqslant p-1 \\ 0 & \text{if } p \leqslant j \leqslant n. \end{cases}$$

Thus $NP_p(g)$ has two edges, one joining $(0,0)$ and $(n-p,0)$, and the other joining $(n-p,0)$ and $(n,1)$. Clearly, the latter edge has slope $1/p$, and, hence, p divides the denominator of the slope of this edge of $NP_p(g)$, which is what we claimed. $\square$

For $n \geqslant 6$ and $\alpha > 0$, $(n,\alpha) \in \mathcal{A}'_\infty$ if and only if $\alpha \in \{n-6, n-1, n, n+1, n+2, n+3\}$. Thus n and α satisfy the condition in Lemma 4. Furthermore, if we take the prime p in the interval $(2/3n+2, n-7]$, then p is also as in Lemma 4. The conclusion in Theorem 2 for $n \geqslant 6$ and $\alpha > 0$ now follows from Lemma 4. In order to ensure the existence of a prime in the interval $(2/3n+2, n-7]$, we make use of explicit estimates on $\pi(x)$ (the number of primes less than or equal to a real number $x \geqslant 1$) from [12].

Lemma 5. *For $n \geqslant 36$, the interval $(2/3n+2, n-7]$ contains a prime.*

Proof. Let $S(n) = \pi(n-7) - \pi(2n/3+3)$. From [12], we have the following estimates.

$$\pi(x) > \frac{x}{\log x - 0.5} \quad \text{for } x \geqslant 67,$$
$$\pi(x) < \frac{x}{\log x - 1.5} \quad \text{for } x \geqslant e^{1.5},$$

where the logarithms appearing above are natural logarithms. Thus, as long as $n \geqslant 74$, we have

$$\begin{aligned} S(n) &> \frac{n-7}{\log(n-7) - 0.5} - \frac{2n/3+3}{\log(2n/3+3) - 1.5} \\ &> \frac{n-7}{\log n - 0.5} - \frac{2n/3+3}{\log n + \log(2/3) - 1.5} \\ &> \frac{n-7}{\log n - 0.5} - \frac{2n/3+3}{\log n - 1.906}. \end{aligned}$$

After combining the fractions, we find that $S(n) > 0$ if

$$T(n) = \frac{n \log n}{3} - \frac{5n}{3} - 10 \log n + 14.842 > 0.$$

A simple calculation verifies that $T(x)$ is increasing for $x \geqslant e^5$ and $T(250) > 0$. Thus $S(n) > 0$ for $n \geqslant 250$. This proves Lemma 5 for $n \geqslant 250$. For $36 \leqslant n \leqslant 249$, we used Sage to verify the conclusion of Lemma 5. $\square$

Thus the conclusion of Theorem 2 for $n \geqslant 36$ follows from Lemmas 4 and 5. One easily verifies that for $6 \leqslant n \leqslant 35$ and $\alpha > 0$, the only pairs (n, α) which appear in the list for $\mathcal{A}'_\infty$ are $(28, 22)$ (case (xi)); $(9, 8)$, $(25, 24)$ (case (xii)); $(7, 8)$, $(17, 18)$, $(31, 32)$ (case (xviii)); and $(13, 16)$, $(33, 36)$ (case (xix)). For pairs $(n, \alpha) \in \{(7, 8), (9, 8), (13, 16), (17, 18)\}$, we used Sage to compute the corresponding Galois groups (Sage can compute Galois groups of all irreducible polynomials having degree $\leqslant 23$). The Galois group always turns out to be A_n. In the event that $(n, \alpha) \in \{(25, 24), (28, 22), (31, 32), (33, 36)\}$, we verified the irreducibility of $L_n^{(\alpha)}(x)$ with Sage. Now we conclude from Lemma 4 that the corresponding Galois group is A_n in these cases.

The treatment in the case that $\alpha < 0$ is not much different either. For the sake of convenience, we use Hajir's notations as in [9] and write $\alpha = -1 - n - r$. We define $\mathcal{L}_n^{\langle r \rangle}(x)$ as

$$\mathcal{L}_n^{\langle r \rangle}(x) := \mathcal{L}_n^{(-1-n-r)}(x) = \mathcal{L}_n^{(\alpha)}(x) = \sum_{j=0}^{n} c_j x^j.$$

Here, $c_j = (-1)^{n+j} \binom{n}{j} d_j$, where $d_j = (r+1)(r+2) \cdots (r+n-j)$. Following a similar approach as in the previous case, we first derive a criteria for the Galois group of $\mathcal{L}_n^{\langle r \rangle}(x)$ to contain A_n.

Lemma 6. *Let n and r be positive integers with $n < 2r + 3$ such that there is a prime in the interval $((n + r)/3, 1 + r)$. Then the Galois group of $\mathcal{L}_n^{\langle r \rangle}(x)$ over $\mathbb{Q}$ contains A_n, provided that $\mathcal{L}_n^{\langle r \rangle}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Let us write $f(x) = \mathcal{L}_n^{\langle r \rangle}(x)$. Working similarly to the previous case, one finds that $\nu_p(d_j) \leqslant 1$ for all $0 \leqslant j \leqslant n$, and that $\nu_p(d_j) = 1$, for $j \leqslant 2n - 2p - 5$. Thus

$$\nu_p(c_j) = \begin{cases} 1 & \text{if } 0 \leqslant j \leqslant n - p \\ 2 & \text{if } n - p < j \leqslant 2n - 2p - 5 \\ 1 & \text{if } 2n - 2p - 5 < j \leqslant p - 1 \\ 0 & \text{if } p \leqslant j \leqslant n. \end{cases}$$

Therefore $NP_p(f)$ has two edges, joining points $(0, 0)$, $(n - p, 0)$, and $(n - p, 0)$, $(n, 1)$, respectively. As in the case $\alpha > 0$, p divides the denominator of the slope of the edge joining $(0, n - p)$ and $(n, 1)$. Therefore we conclude from Theorem 4 that $\mathcal{L}_n^{\langle r \rangle}(x)$ has Galois group A_n, provided it is irreducible over $\mathbb{Q}$. □

As indicated at the beginning of this section, for $n \geqslant 6$ and $\alpha < 0$, we only need to consider pairs $(n, \alpha) \in \mathcal{A}'_\infty$ in which α assumes values in the set $\{-2n - 4, -2n - 2, -2n, -2n + 4\}$ (cases (vii), (xxiv)–(xxv) and (xxviii)–(xxx)). Thus the only values of r that we need to consider are in the set $\{n - 5, n - 1, n + 1, n + 3\}$. As in the case $\alpha > 0$, we deduce from Lemma 5 that, for $n \geqslant 36$ and $r \in \{n - 5, n - 1, n + 1, n + 3\}$, there is a prime in the interval $((n + r)/3, 1 + r)$. Thus, by appealing to Lemma 6, the conclusion in Theorem 2 follows for $n \geqslant 36$ and $\alpha < 0$.

For $6 \leqslant n \leqslant 35$ and $\alpha < 0$, the pairs $(n, \alpha) \in \mathcal{A}'_\infty$ are $(8, -18)$, $(12, -26)$, $(16, -34)$, $(20, -42)$, $(24, -50)$, $(28, -58)$, $(32, -66)$ (case (vii)); $(28, -52)$ (case (xxiv)); $(9, -18)$, $(25, -50)$ (case (xxv)); $(17, -36)$ (case (xxix)); and $(13, -30)$, $(33, -70)$ (case (xxx)). For $6 \leqslant n \leqslant 20$, we verified with Sage that the corresponding Galois group is indeed A_n. For the remaining pairs, that is, for pairs $(24, -50)$, $(25, -50)$, $(28, -58)$, $(28, -52)$, $(32, -66)$ and $(33, -70)$, it follows from Lemma 6 that the corresponding Galois group is A_n, provided $\mathcal{L}_n^{(\alpha)}(x)$ is irreducible for these values of n and α. The irreducibility in these cases was established using Sage. Based on these various evidences, we believe that for $\alpha \neq -1$, $(4, 23)$ is the only pair in $\mathcal{A}_\infty$ for which the Galois group associated with $\mathcal{L}_n^{(\alpha)}(x)$ is not A_n. We conclude this paper with the following.

Conjecture 1. *For $\alpha \neq -1$, the only pair $(n, \alpha) \in \mathcal{A}_\infty$ for which the Galois group associated with $L_n^{(\alpha)}(x)$ is not A_n, is $(4, 23)$.*

Acknowledgment

The author is grateful to his doctoral dissertation advisor Professor Michael Filaseta for engaging him in projects related to investigation of algebraic properties of generalized

Laguerre polynomials and for various insightful discussion on the topic. The author is also thankful to the anonymous referee for carefully analyzing the article and for giving kind and thoughtful remarks on an earlier version of the paper.

References

[1] P. Banerjee, M. Filaseta, C. Finch, J. Leidy, On classifying Laguerre polynomials which have Galois group the alternating group, J. Théor. Nombres Bordeaux 25 (2013) 1–30.

[2] J.H.E. Cohn, The Diophantine equation $X^3 = NY^2 \pm 1$, Quart. J. Math. Oxford 42 (1991) 27–30.

[3] G. Dumas, Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, J. Math. Pures Appl. (9) 2 (1906) 191–258.

[4] M. Filaseta, T. Kidd, O. Trifonov, Laguerre polynomials with Galois group A_m for each m, J. Number Theory 132 (2012) 776–805.

[5] M. Filaseta, T.Y. Lam, On the irreducibility of generalized Laguerre polynomials, Acta Arith. 105 (2002) 177–182.

[6] R. Gow, Some generalized Laguerre polynomials whose Galois groups are the alternating groups, J. Number Theory 31 (1989) 201–207.

[7] F. Hajir, Some A_n-extensions obtained from generalized Laguerre polynomials, J. Number Theory 50 (1995) 206–212.

[8] F. Hajir, On the Galois group of generalized Laguerre polynomials, J. Theor. Nombres Bordeaux 17 (2) (2005) 517–525.

[9] F. Hajir, Algebraic properties of a family of generalized Laguerre polynomials, Canad. J. Math. 61 (3) (2009) 583–603.

[10] F. Hajir, S. Wong, Specializations of one parameter family of polynomials, Ann. Inst. Fourier (Grenoble) 56 (4) (2006) 1127–1163.

[11] L.-C. Kappe, B. Warren, An elementary test for the Galois group of a quartic polynomial, Amer. Math. Monthly 96 (1989) 133–137.

[12] J.B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64–94.

[13] I. Schur, Gleichungen ohne Affekt, in: Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse, 1930, pp. 443–449.

[14] I. Schur, Affectlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, J. Reine Angew. Math. 165 (1931) 52–58.

[15] I. Schur, Gesammelte Abhandlungen, Band III, Springer-Verlag, Berlin, 1973, Herausgegeben von Alfred Brauer und Hans Rohrbach.

[16] E.A. Sell, On a certain family of generalized Laguerre polynomials, J. Number Theory 107 (2) (2004) 266–281.

[17] M. Watkins, Class numbers of imaginary quadratic fields, Math. Comp. 73 (2004) 907–938.