isid/ms/2015/13
October 12, 2015
http://www.isid.ac.in/~statmath/index.php?module=Preprint

On the Galois groups of generalized Laguerre Polynomials

Shanta Laishram

Indian Statistical Institute, Delhi Centre
7, SJSS Marg, New Delhi–110 016, India

ON THE GALOIS GROUPS OF GENERALIZED LAGUERRE POLYNOMIALS

SHANTA LAISHRAM

Abstract. For a positive integer n and a real number α, the generalized Laguerre polynomials are defined by

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

These orthogonal polynomials are solutions to *Laguerre's Differential Equation* which arises in the treatment of the harmonic oscillator in quantum mechanics. Schur studied these Laguerre polynomials for its interesting algebraic properties. In this short article, it is shown that the Galois groups of Laguerre polynomials $L_n^{(\alpha)}(x)$ is S_n with $\alpha \in \{\pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{4}, \pm\frac{3}{4}\}$ except when $(\alpha, n) \in \{(\frac{1}{4}, 2), (-\frac{2}{3}, 11), (\frac{2}{3}, 7)\}$. The proof is based on ideas of $p-$adic Newton polygons.

1. Introduction

For a positive integer n and a real number α, the generalized Laguerre polynomials are defined by

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

These orthogonal polynomials has a wide range of applications in several areas of mathematics. Not long after its appearance in the literature early in the twentieth century, it became evident, in the hands of Schur, that the generalized Laguerre polynomials also enjoys algebraic properties of great interest. In fact the irreducibility of these polynomials is connected to finding explicit examples as solutions to Hilbert's *Inverse Galois Problem.* We refer to [FKT12] for more details.

It was shown that $L^{(\alpha)}(x)$ is irreducible for $\alpha \in \{\pm\frac{1}{2}\}$ in [Sch29] and [Sch31] and for $\alpha \in \{\pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{4}, \pm\frac{3}{4}\}$ in [LaSh, Theorem 1] except when $\alpha = \frac{1}{4}, n = 2$. By using these results of irreducibility, it was shown in [SaSh15, Theorem 1.4] that the Galois group of $L^{(\alpha)}(x)$ is S_n for $n \geq n_0$ where $n_0 = 182, 876, 1325$ if $q \in \{\pm\frac{1}{2}\}, q \in \{\pm\frac{1}{3}, \pm\frac{2}{3}\}$ and $q \in \{\pm\frac{1}{4}, \pm\frac{3}{4}\}$, respectively. In this short note, we give a complete result for all n. Here S_n is the Symmetric Group on n symbols and A_n is the Alternating Group on n symbols. We prove

2000 Mathematics Subject Classification: Primary 11A41, 11B25, 11N05, 11N13, 11C08, 11Z05.
Keywords: Irreducibility, Hermite-Laguerre Polynomials, Newton Polygons, Arithmetic Progressions, Primes.

Theorem 1. *Let $\alpha \in \{\pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{4}, \pm\frac{3}{4}\}$. The Galois group of Laguerre polynomials $L_n^{(\alpha)}(x)$ is S_n for every $n \geq 1$ except when $(\alpha, n) \in \{(\frac{1}{4}, 2), (-\frac{2}{3}, 11), (\frac{2}{3}, 7)\}$ where it is A_n for $(\alpha, n) \in \{(-\frac{2}{3}, 11), (\frac{2}{3}, 7)\}$ and S_1 for $(\alpha, n) = (\frac{1}{4}, 2)$.*

We give a proof of Theorem 1 in Section 3. The proof of Theorem 1 is an application of a result of Hajir [Haj05] based on $p-$adic Newton polgons, see Lemmas 2.1 and 2.2. The new ingredient in this paper is the clever use of Lemma 2.1 as Lemma 2.2 instead of [SaSh15, Lemma 3.3]. In fact the proof of [SaSh15, Theorem 1.4] can be much shortened by using Lemma 2.2.

2. Preliminaries

Hajir [Haj05] gave a criterion for an irreducible polynomial to have large Galois group using Newton polygons. We restate the result which is [Haj05, Lemma 3.1].

Lemma 2.1. *Let $f(x) = \sum_{j=0}^{m} \binom{m}{j} c_j x^j \in \mathbb{Q}[X]$ be an irreducible polynomial of degree m. Let p be a prime with $\frac{m}{2} < p < m-2$ such that*

(i) $ord_p(c_0) = 1$,
(ii) $ord_p(c_j) \geq 1$ for $0 \leq j \leq m-p$,
(iii) $ord_p(c_p) = 0$.

Then p divides the order of Galois group of f over $\mathbb{Q}$. In fact, this Galois group is A_m if $disc(f) \in \mathbb{Q}^{*2}$ and S_m otherwise.

We will be applying the above lemma to following polynomial. Let $\alpha = \frac{u}{v}$ with $u, v \in \mathbb{Z}$, $\gcd(u, v) = 1$ and $v > 0$. Let

$$\begin{aligned} G(x,u,v) :&= v^n n! L^{(\frac{u}{v})}(\frac{-x}{v}) \\ &= \sum_{j=0}^{n} \binom{n}{j} (u+vn)(u+v(n-1)) \cdots (u+v(j+1)) x^j. \end{aligned} \tag{1}$$

In [Sch31], Schur showed that its discriminant is given by

$$D_n^{(u,v)} := Disc(G(x,u,v)) = \prod_{j=2}^{n} j^j (\frac{u}{v} + j)^{j-1}.$$

We write $D_m^{(u,v)} = bY^2$, $Y \in \mathbb{Q}$ with

$$b = \begin{cases} \frac{3 \cdot 5 \cdots n \cdot (u+2v)(u+4v) \cdots (u+(n-1)v}{v^\delta} & \text{if } n \equiv 1, 3 (\text{mod } 4) \\ \frac{3 \cdot 5 \cdots (n-1) \cdot (u+2v)(u+4v) \cdots (u+nv}{v^\delta} & \text{if } n \equiv 0, 2 (\text{mod } 4) \end{cases} \tag{2}$$

where $\delta = 0$ if $n \equiv 0, 1(\text{mod } 4)$ and 1 if $n \equiv 2, 3(\text{mod } 4)$.

We now apply Lemma 2.1 to $G(x, u, v)$. We prove

Lemma 2.2. *Let* $1 \le r < v$, $\gcd(r, v) = 1$ *and* p *be a prime with*

$$p > v, p \equiv r^{-1}u(\text{mod } v) \text{ and } \frac{u+v+nv}{r+v} \le p \le n-3. \tag{3}$$

Let $G(x, u, v)$ *be given by* (1) *be an irreducible polynomial of degree* n. *Assume that* $|u| < v$. *Then the Galois group of* $G(x, u, v)$ *is* A_n *or* S_n *according as* b *(given by* (2)*) is a square or not an square of an integer.*

Proof. We apply Lemma 2.1 with

$$c_j = (u + vn)(u + v(n-1)) \cdots (u + v(j+1)).$$

Since $1 \le r < v$, we have $\frac{u+v+nv}{r+v} > \frac{n}{2}$ and hence $\frac{n}{2} < p < n-2$ is valid. It suffices to check conditions $(i) - (iii)$ of Lemma 2.1.

Since $p \equiv r^{-1}u(\text{mod } v)$, we get $p|(u + iv)$ for some i. Let i_0 be the least positive integer i with this property. Then $1 \le i_0 < p$. Further let $u + i_0v = pr_0$. Then $r_0 \equiv r(\text{mod } v)$. We claim that $r_0 < v$. Suppose not. Then $u + i_0v = pr_0 \ge pv \ge (i_0 + 1)v$ since $i_0 < p$ contradicting $|u| < v$. Thus $r_0 < v$. This with $r_0 \equiv r(\text{mod } v)$ and $1 \le r < v$ implies $r = r_0$. Since $\frac{u+v+nv}{r+v} \le p$, we have

$$u + v + (n-p)v \le rp = r_0p = u + i_0v$$

giving $i_0 > n-p$. Thus $n-p < i_0 < p$. This gives $i_0-p < 0$ and $i_0+p > n$ and hence $u+i_0v$ is the only multiple of p in $\{u, u+v, \cdots, u+nv\}$. Further $u+i_0v = pr < pv < p^2$ implying $p||(u + i_0v)$. Hence conditions $(i) - (iii)$ of Lemma 2.1 are valid and the assertion follows. □

The above Lemma contains [SaSh15, Lemma 3.3]. We also need the following result on b being a square or not.

Lemma 2.3. *Let* $2 \le n \le 1325$,

$$\alpha = \frac{u}{v} \in \{\pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{1}{4}, \pm\frac{3}{4}\}$$

and b *be given by* (2). *Then* b *is square only when* $(u, v, n) \in \{(-2, 3, 3), (-2, 3, 11), (2, 3, 7)\}$.

Proof. First we check that for $2 \le n \le u + 2v$, the assertion is valid. Hence we now take $n > u + 2v$. Let

$$n_1 = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Assume $u \ne \pm 2$ if $v = 3$. Then we see that b is divisible by every prime $p \equiv u(\text{mod } 2v)$ with $n < p \le u + 2vn_1$ to the first power. Hence if there is such a prime, b cannot be a square. For $u + 2v < n \le 1325$, we check that this is true. Thus we now take $v = 3, u = \pm 2$. Let $u_1 = \frac{u}{2}$. Then

$$(u + 2v) \cdots (u + 2n_1v) = 2^{n_1}(u_1 + v)(u_1 + 2v) \cdots (u_1 + n_1v)$$

and hence b is not an square if there is a prime p with $n < p \le u_1+n_1v$ and $p \equiv u_1(\text{mod } v)$ where $v = 3$. We check that this is the case for $u + 2v < m \le 1325$ except when

$u=-2, m \in \{5,6,7,11\}$ and $u=2, m=19$. For $u=-2, m\in\{5,6,7,11\}$ and $u=2, m=19$, we check that b is not a square except when $u=-2, m=11$. Hence the assertion follows. □

3. Proof of Theorem 1

Let

$$\alpha=\frac{u}{v}\in\{\pm\frac{1}{2},\pm\frac{1}{3},\pm\frac{2}{3},\pm\frac{1}{4},\pm\frac{3}{4}\}.$$

As mentioned before, it was shown that $L^{(\alpha)}(x)$ is irreducible for $\alpha\in\{\pm\frac{1}{2}\}$ in [Sch29] and [Sch31] and in [LaSh] for $\alpha\in\{\pm\frac{1}{3},\pm\frac{2}{3},\pm\frac{1}{4},\pm\frac{3}{4}\}$ except when $\alpha=\frac{1}{4}, n=2$ and hence same is true for $G(x,u,v)$. For $n\le 13$, we check in *SAGE* for $n\le 11$ and *MAGMA* for $n=12,13$ that the assertion of Theorem 1 is valid.

Hence we may suppose that $n>13$. Further we can take $n\le 1325$ by [SaSh15, Theorem 1.4]. It suffices to prove that $G(x,u,v)$ has Galois group S_n. We use Lemmas 2.2 and 2. It suffice to find a prime p with

$$p>v, p\equiv r^{-1}u(\text{mod } v) \text{ and } \frac{u+v+nv}{r+v}\le p\le n-3.$$

for some $r, 1\le r<v$, $\gcd(r,v)=1$. Let $\alpha=\frac{u}{v}\in\{\pm\frac{1}{2}\}$. We check that there is a prime p with $\frac{2n+2+u}{3}\le p\le n-3$ except when $u=1, n=19$. We check that for $n=19$, the Galois group of $L^{(\frac{1}{2})}(x)$ is S_n.

Let $\alpha=\frac{u}{v}\in\{\pm\frac{1}{3},\pm\frac{2}{3}\}$. Since $1\le r<3$, we need to find a prime p with

$$\frac{3n}{4}+\frac{3+u}{4}\le p\le n-3, p\equiv u(\text{mod } 3)$$

or

$$\frac{3n}{5}+\frac{3+u}{5}\le p\le n-3, p\equiv 2u(\text{mod } 3).$$

Hence it suffices to find a prime p with $\frac{3n}{4}+\frac{3+u}{4}\le p\le n-3$ or

$$\frac{3n}{5}+\frac{3+u}{5}\le p<\frac{3n}{4}+\frac{3+u}{4}, p\equiv 2u(\text{mod } 4).$$

We check that this is the case except when

$$\begin{aligned} u=-1 &: n=15\\ u=-2 &: n\in=19\\ u=1 &: n\in\{18,19\}\\ u=2 &: n\in\{14,15,31\}.\end{aligned}$$

For these values of $\frac{u}{3}$ and n, we check in *MAGMA* that Galois group of $L^{(\frac{u}{3})}(x)$ is S_n.

Let $\alpha=\frac{u}{v}\in\{\pm\frac{1}{4},\pm\frac{3}{4}\}$. Since $r\in\{1,3\}$, we need to find a prime p with

$$\frac{4n}{5}+\frac{4+u}{5}\le p\le n-3, p\equiv u(\text{mod } 4)$$

or

$$\frac{4n}{7}+\frac{4+u}{7}\leq p\leq n-3, p\equiv 3u(\text{mod } 4).$$

Hence it suffices to find a prime p with $\frac{4n}{5}+\frac{4+u}{5}\leq p\leq n-3$ or

$$\frac{4n}{7}+\frac{4+u}{7}\leq p<\frac{4n}{5}+\frac{4+u}{5}, p\equiv 3u(\text{mod } 4).$$

We check that this is the case except when

$$\begin{aligned}u=-1 :&n\in\{14,15,30,31\}\\ u=-3 :&n\in\{20,21,23\}\\ u=1 :&n\in\{19,20,21\}\\ u=3 :&n\in\{14,29,30,31\}.\end{aligned}$$

For these values of $\frac{u}{4}$ and n, we check check in *MAGMA* that Galois group of $L^{(\frac{u}{4})}(x)$ is S_n. This completes the proof of Theorem 1. □

Acknoweldgements

We thank the anonymous referee for the remarks in an earlier version of this paper. We also thank DST for supporting this work under the Fast Track Project.

References

[FKT12] M. Filaseta, T. Kidd and O. Trifonov, *Laguerre polynomials with Galois group A_m for each m*, J. Number Theory, **132** (2012), no. 4, 776805.

[Haj05] F. Hajir, *On the Galois group of generalized Laguerre polynomials*, J. Théor. Nombres Bordeaux, **17**(2) (2005), 517–525.

[LaSh] S. Laishram and T. N. Shorey, *Irreducibility of generalized HermiteLaguerre polynomials III*, Submitted.

[SaSh15] N. Saradha and T. N. Shorey, *Squares in blocks from an arithmetic progression and Galois group of Laguerre polynomials*, Int. Jour. of Number Theory, **11**(1) (2015), 233–250.

[Sch29] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, II*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., **14** (1929), 370–391.

[Sch31] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermitschen Polynome*, J. Reine Angew. Math., **165** (1931), 52–58.

Stat-Math Unit, India Statistical Institute, 7, S. J. S. Sansanwal Marg, New Delhi, 110016, India

E-mail address: shantalaishram@gmail.com