

ON THE GALOIS GROUP OF GENERALIZED LAGUERRE POLYNOMIALS

FARSHID HAJIR

JUNE 22, 2004 – 12:47

ABSTRACT. Using the theory of Newton Polygons, we formulate a simple criterion for the Galois group of a polynomial to be “large.” For a fixed $\alpha \in \mathbb{Q} - \mathbb{Z}_{<0}$, Filaseta and Lam have shown that the n th degree Generalized Laguerre Polynomial $L_n^{(\alpha)}(x) = \sum_{j=0}^n \binom{n+\alpha}{n-j} (-x)^j / j!$ is irreducible for all large enough n . We use our criterion to show that, under these conditions, the Galois group of $L_n^{(\alpha)}(x)$ is either the alternating or symmetric group on n letters, generalizing results of Schur for $\alpha = 0, 1$.

ABSTRAIT. En utilisant la théorie des polygones de Newton, on obtient un critère simple pour montrer que le groupe de Galois d’un polynôme soit “large.” Si on fixe $\alpha \in \mathbb{Q} - \mathbb{Z}_{<0}$, Filaseta et Lam ont montré que le Polynôme Généralisé de Laguerre $L_n^{(\alpha)}(x) = \sum_{j=0}^n \binom{n+\alpha}{n-j} (-x)^j / j!$ est irréductible quand le degré n est assez grand. On utilise notre critère afin de montrer que, sous ces hypothèses, le groupe de Galois de $L_n^{(\alpha)}(x)$ est soit le groupe alterné, soit le groupe symétrique, de degré n , généralisant des résultats de Schur pour $\alpha = 0, 1$.

À Georges Gras, à l’occasion de son 60ème anniversaire

1. INTRODUCTION

It is a basic problem of algebra to compute the Galois group of a given irreducible polynomial over a field K . If we order the monic degree n polynomials over \mathbb{Z} by increasing height, then the proportion which consists of irreducible polynomials with Galois group S_n tends to 1; for a more precise statement, see for example Gallagher [G]. Nevertheless, to prove that the Galois group of a given polynomial is S_n can be difficult if n is large. The algorithmic aspects of Galois group computations have witnessed a number of recent advances, for which an excellent reference is the special issue [MMY] of the Journal of Symbolic Computation, especially the foreword by Matzat, McKay, and Yokoyama. Currently, for rational polynomials of degree up to 15, efficient algorithms are implemented, for instance, in GP-PARI and MAGMA. An important piece of any such algorithm is the collection of data regarding individual elements of the Galois group, for which the standard method is to factor the polynomial modulo various “good” primes (i.e. those not dividing its discriminant), obtaining the cycle-type of the corresponding Frobenius conjugacy classes in the Galois group.

Our first goal in this paper is to formulate a criterion which exploits the properties of “bad” primes for proving that the Galois group of a given polynomial is large. The criterion is especially efficacious if one suspects that a “medium size” prime (roughly between $n/2$ and

2000 *Mathematics Subject Classification*. Primary 11R32; Secondary 11R09, 12F10.

Key words and phrases. Galois group, Generalized Laguerre Polynomial, Newton Polygon.

This work was supported by the National Science Foundation under Grant No. 0226869.

n) is wildly ramified in the splitting field of the polynomial. The criterion we give (Theorem 2.3) follows quite simply from the theory of p -adic Newton Polygons; it is used in slightly less general form in Coleman [C] and is reminiscent of, but distinct from, a criterion of Schur [Sc1, §1].

Our second goal is to illustrate the utility of the criterion by using it to calculate the Galois group for a certain family of polynomials, which we now introduce. In the second volume of their influential and classic work [PS], Pólya and Szegő define the Generalized Laguerre Polynomial (GLP)

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

The special case $\alpha = 0$ had appeared much earlier in the work of Abel [A, p. 284] and Laguerre [L], and the general case can in fact be found in Sonin [So, p. 41]. Shortly after the publication of [PS], the study of the algebraic properties of this family of orthogonal polynomials was initiated by Schur [Sc1], [Sc2].

For instance, for the discriminant of the monic integral polynomial $(-1)^n n! L_n^{(\alpha)}(x)$, we have the following formula of Schur [Sc2]:

$$(1) \quad \Delta_n^{(\alpha)} = \prod_{j=2}^n j^j (\alpha + j)^{j-1}.$$

In particular, if α is not in $[-n, -2] \cap \mathbb{Z}$, $L_n^{(\alpha)}(x)$ has no repeated roots. For $\alpha = 0, 1$, Schur [Sc1], [Sc2] established the irreducibility of all $L_n^{(\alpha)}(x)$ over \mathbb{Q} , and also showed that their Galois groups are as large as possible, namely A_n if $\Delta_n^{(\alpha)}$ is a rational square, and S_n otherwise.

A number of recent articles on the algebraic properties of GLP have appeared, including Feit [F], Coleman [C], Gow [Go], Filaseta-Williams [FW], Filaseta-Lam [FL], Sell [S], Hajir [H1], [H2], and Hajir-Wong [HW]. In particular, we have the following theorem of Filaseta and Lam [FL] on the irreducibility of GLP.

Theorem. (Filaseta-Lam) *If α is a fixed rational number which is not a negative integer, then for all but finitely many integers n , $L_n^{(\alpha)}(x)$ is irreducible over \mathbb{Q} .*

In this paper, we provide a complement to the theorem of Filaseta and Lam by computing the Galois group of $L_n^{(\alpha)}(x)$ when n is large with respect to $\alpha \in \mathbb{Q} - \mathbb{Z}_{<0}$. Namely, we prove the following result.

Theorem 1.1. *Suppose α is a fixed rational number which is not a negative integer. Then for all but finitely many integers n , the Galois group of $L_n^{(\alpha)}(x)$ is A_n if $\Delta_n^{(\alpha)}$ is a square and S_n otherwise.*

Remarks. 1. The hypothesis that α not be a negative integer is necessary, as in that case, $L_n^{(\alpha)}(x)$ is divisible by x for $n \geq |\alpha|$. For a study of the algebraic properties of $L_n^{(\alpha)}(x)$ for $\alpha \in \mathbb{Z}_{<0}$, $n < |\alpha|$, see [H1], [S] and [H2].

2. Using a different set of techniques, the following companion to Theorem 1.1 is proved in [HW]: If we fix $n \geq 5$ and a number field K , then for all but finitely many $\alpha \in K$, $L_n^{(\alpha)}(x)$ is irreducible and has Galois group A_n or S_n over K . For each $n \leq 4$, infinitely many

reducible specializations exist, and for $n = 4$, there are infinitely many specializations which are irreducible but have D_4 -Galois group, cf. [H2, Section 6].

3. For integral α , some cases where $\Delta_n^{(\alpha)}$ is a square (giving Galois group A_n) are

- $\alpha = 1$ and $n \equiv 1 \pmod{2}$ or $n + 1$ is an odd square ([Sc2]),
- $\alpha = n$, and $n \equiv 2 \pmod{4}$ ([Go], it is not yet known if all of these polynomials are irreducible [FW]),
- $\alpha = -1 - n$, and $n \equiv 0 \pmod{4}$ ([Sc1], [C]),
- $\alpha = -2 - n$, and $n \equiv 1 \pmod{4}$ ([H1]).

See [H2, §5] as well as the above-cited papers for more details.

4. The proofs of the Filaseta-Lam Theorem in [FL] and of Theorem 1.1 are both effective.

2. A CRITERION FOR HAVING LARGE GALOIS GROUP

2.1. Newton Polygons. Let K be a field equipped with a discrete valuation v and a corresponding completion K_v . We assume v is normalized, i.e. $v(K^*) = \mathbb{Z}$, and employ the same letter v to denote an extension of this valuation to an algebraic closure $\overline{K_v}$ of K_v .

For a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in K[x]$ with $a_0 a_n \neq 0$, the v -adic Newton Polygon of $f(x)$, denoted $NP_v(f(x))$, is defined to be the lower convex hull of the set of points

$$S_v(f) = \{(0, v(a_0)), (1, v(a_1)), \dots, (n, v(a_n))\}.$$

It is the highest polygonal line passing on or below the points in $S_v(f)$. The points where the slope of the Newton polygon changes (including the rightmost and leftmost points) are called the *corners* of $NP_v(f)$; their x -coordinates are the *breaks* of $NP_v(f)$.

For the convenience of the reader, we recall the main theorem about v -adic Newton Polygons; for a proof see, for instance, Gouvêa [Gou]. A very nice survey of the uses of the Newton Polygon for proving irreducibility is Mott [Mo]. For generalizations to several variables, see Gao [Ga] and references therein.

Theorem 2.1 (Main Theorem of Newton Polygons). *Let $(x_0, y_0), (x_1, y_1), \dots, (x_r, y_r)$ denote the successive vertices of $NP_v(f(x))$. Then there exist polynomials f_1, \dots, f_r in $\mathbb{Q}_p[x]$ such that*

- i) $f(x) = f_1(x)f_2(x) \cdots f_r(x)$,
- ii) the degree of f_i is $x_i - x_{i-1}$,
- iii) all the roots of f_i in $\overline{K_v}$ have v -adic valuation $-(y_i - y_{i-1})/(x_i - x_{i-1})$.

2.2. Newton Index. We now suppose that K is a global field, i.e. K is a finite extension of \mathbb{Q} (number field case) or of $\mathbb{F}(T)$, where \mathbb{F} is a finite field (function field case). A global field K enjoys the property that for a given element $\alpha \in K$, $v(\alpha) = 0$ for all but finitely many valuations v of K .

Definition 2.2. *Given $f \in K[x]$, the Newton Index of f \mathcal{N}_f is defined to be the least common multiple of the denominators (in lowest terms) of all slopes of $NP_v(f)$ as v ranges over all normalized discrete valuations of K .*

Note that 0 is defined to have denominator 1, so slope 0 segments of $NP_v(f)$ do not contribute to \mathcal{N}_f . On the other hand, for all but finitely many v , the coefficients of f all have v -adic valuation 0 so $NP_v(f)$ consists of a single slope 0 segment. Hence, \mathcal{N}_f is well-defined and effectively computable (for monic v -integral polynomials, we need only compute

the Newton Polygon for those valuations that do not vanish on the constant coefficient). It is clear that \mathcal{N}_f is a divisor of $\text{lcm}(1, 2, \dots, n)|n!$ where n is the degree of f ; the latter property in fact holds for an arbitrary field K , so the Newton index is well-defined for any field K , though possibly not in the sense that it is necessarily effectively computable.

We now formulate a criterion for an irreducible polynomial to have “large” Galois group. The key idea appears in Coleman’s computation [C] of the Galois group of the n th Taylor polynomial of the exponential function, which incidentally is the GLP $(-1)^n L_n^{(-1-n)}(x)$.

Theorem 2.3. *Suppose K is a global field and $f(x)$ is an irreducible polynomial in $K[x]$. Suppose $g(x) = f(x - \mu)$ for some $\mu \in K$. Then \mathcal{N}_g divides the order of the Galois group of f over K . Moreover, if \mathcal{N}_g has a prime divisor q in the range $n/2 < q < n - 2$, where n is the degree of f , then the Galois group of f contains A_n .*

Proof. Suppose v is a valuation of K and q is an arbitrary divisor of the denominator of some slope s of the v -adic Newton polygon of g . Clearly, f and g have the same splitting field and the same Galois group. It suffices to show that q divides the order of the Galois group of g over \mathbb{Q} . By the main theorem of Newton polygons 2.1, there exists a root $\alpha \in \overline{K}_v$ of g with valuation $-s$. Since q divides the denominator of s , q divides the ramification index e of $K_v(\alpha)/K_v$. But e divides the degree $[K_v(\alpha) : K_v]$, which in turn divides the order of the Galois group of g over K_v , hence also over K . If q is a prime in the interval $(n/2, n - 2)$, then the Galois group of g contains a q -cycle, so it must contain A_n by a theorem of Jordan [J] (or see, for instance, Hall’s book [Ha, Thm 5.6.2 and 5.7.2]). \square

Remark. Schur proved a similar result ([Sc1, §1, III]), namely, if the discriminant of a number field K of degree n is divisible by p^n , then the Galois closure L of K has degree $[L : \mathbb{Q}]$ divisible by p . In general, if p divides the discriminant of an irreducible polynomial f , it is not easy to determine the p -valuation of the discriminant of the stem field $\mathbb{Q}[x]/(f)$; thus, each of Theorem 2.3 and Schur’s criterion can be useful depending on whether we have information about the discriminant of the field or that of the defining polynomial. Neither criterion is useful when the discriminant of f is square-free, for example, since in that case, all the non-trivial ramification indices are 2. On the other hand, over base field \mathbb{Q} , irreducible polynomials with square-free discriminant also have Galois group S_n see e.g. Kondo [K]; the proof of this fact uses the triviality of the fundamental group of \mathbb{Q} .

3. PROOF OF THEOREM 1.1

We now let $K = \mathbb{Q}$. For a prime p , we write NP_p in place of NP_v where $v = \text{ord}_p$ is the p -adic valuation of \mathbb{Q} .

Lemma 3.1. *Let $f(x) = \sum_{j=0}^n \binom{n}{j} c_j x^j \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n over \mathbb{Q} . Suppose there exists a prime p satisfying*

- i) $n/2 < p < n - 2$,
- ii) $\text{ord}_p(c_j) \geq 0$ for $0 \leq j \leq n$,
- iii) $\text{ord}_p(c_j) = 1$ for $1 \leq j \leq n - p$,
- iv) $\text{ord}_p(c_p) = 0$.

Then the Galois group of f over \mathbb{Q} contains A_n .

Proof. It is easy to check that $\binom{n}{j}$ is divisible by p if and only if $n - p + 1 \leq j \leq p - 1$. The given assumptions then guarantee that $(0, 1)$ and $(p, 0)$ are the first two corners of $NP_p(f)$. Therefore, $-1/p$ is a slope of $NP_p(f)$, hence $p | \mathcal{N}_f$ and we are done by Theorem 2.3. \square

We are now ready to prove the Main Theorem.

Proof of Theorem 1.1. We write $\alpha = \lambda/\mu$ in lowest terms, i.e. with $\gcd(\lambda, \mu) = 1$ and $\mu \geq 1$. By assumption, α is not a negative integer. We will work with the normalized (monic, integral) polynomial

$$f(x) := \mu^n n! L_n^{(\lambda/\mu)}(-x/\mu) = \sum_{j=0}^n \binom{n}{j} (n\mu + \lambda)((n-1)\mu + \lambda) \cdots ((j+1)\mu + \lambda) x^j.$$

We wish to apply Lemma 3.1 to it, so we let

$$(2) \quad c_j = \prod_{k=j+1}^n (k\mu + \lambda), \quad 0 \leq j \leq n,$$

and seek a suitable prime p satisfying the conditions of the Lemma.

By a suitably strong form of Dirichlet's theorem on primes in arithmetic progressions, there exists an effective constant $D(\mu)$ such that if $x \geq D(\mu)$ and $h \geq x/(2 \log^2 x)$, the interval $[x - h, x]$ contains a prime in the congruence class $\lambda \pmod{\mu}$ (see Filaseta-Lam [FL, p. 179]). Taking $x = n - 3 \geq D(\mu)$, we find that for some integer $\ell \in [1, n]$, $p = \mu\ell + \lambda$ is a prime satisfying

$$(3) \quad \frac{n\mu + \mu + \lambda}{\mu + 1} \leq p \leq n - 3,$$

as long as

$$\frac{1 - 3/n}{2 \log^2(n - 3)} + \frac{3 + \lambda/(\mu + 1)}{n} \leq \frac{1}{\mu + 1},$$

which clearly holds for all n large enough with respect to λ, μ .

We now fix a prime $p = \mu\ell + \lambda$ satisfying (3). For such a prime p , let us check the hypotheses of Lemma 3.1. We have $(n\mu + \mu + \lambda)/(\mu + 1) > n/2$ if and only if

$$(4) \quad n(\mu - 1) > -2\mu - 2\lambda.$$

Since α is not a negative integer, if $\mu = 1$, then $\lambda \geq 0$, so (4) holds for all n . If $\mu > 1$, we simply need to take $n > -2(\mu + \lambda)/(\mu - 1)$ in order to achieve $n/2 < p < n - 2$, giving us i). Our c_j are integral so ii) holds trivially. Before we discuss iii), let us note that in the congruence class $\lambda \pmod{\mu}$, the smallest multiple of p larger than p is $(\mu + 1)p$, and, similarly, the largest multiple of p in this congruence class which is less than p is $(-\mu + 1)p$. Now we claim that, for n large enough, we have

$$(5) \quad (-\mu + 1)p < \lambda + \mu$$

as well as

$$(6) \quad \lambda + \mu n < (\mu + 1)p.$$

Indeed, if $\mu = 1$, then (5) holds for all n , while for $\mu \geq 2$, $n \geq -2\lambda$ implies (5); moreover, (6) is a direct consequence of (3). We conclude from (5) and (6) that $\text{ord}_p(c_0) = 1$. From (2), we then read off that $\text{ord}_p(c_j) = 1$ for $0 \leq j \leq \ell - 1$, and $\text{ord}_p(c_j) = 0$ for $\ell \leq j \leq n$. One easily checks that (5) and (6) give exactly $p > \ell - 1$ and $n - p < \ell$, i.e. iii) and iv).

By Filaseta-Lam [FL], there is an effectively computable constant $N(\alpha)$ such that $f(x)$ is irreducible for $n \geq N(\alpha)$. Thus, all the conditions of Lemma 3.1 hold, and the proof of the theorem is complete. \square

Remark. Note that the proof simplifies in the case where α is a non-negative integer, giving: If $L_n^{(\alpha)}(x)$ is irreducible and if there is a prime p in the interval $((n + \alpha)/2, n - 2)$, then the Galois group of $L_n^{(\alpha)}(x)$ contains A_n . By [H2, Corollary 3.2], the specified interval contains a prime as long as $n \geq \max(48 - \alpha, 8 + 5\alpha/3)$.

REFERENCES

- [A] N. H. Abel, *Oeuvres Complètes*, Tome 2, Grondahl & Son, Christiania, 1881.
- [C] R. F. Coleman, On the Galois groups of the exponential Taylor polynomials, *Enseign. Math.* (2) **33** (1987), no. 3-4, 183–189.
- [F] W. Feit, \tilde{A}_5 and \tilde{A}_7 are Galois groups over number fields, *J. Algebra* **104** (1986), no. 2, 231–260
- [FL] M. Filaseta and T.-Y. Lam, On the irreducibility of the Generalized Laguerre polynomials, *Acta Arith.* **105** (2002), no. 2, 177–182
- [FW] M. Filaseta and R. L. Williams, Jr., On the irreducibility of a certain class of Laguerre polynomials, *J. Number Theory* **100** (2003), no. 2, 229–250
- [G] P. X. Gallagher, The large sieve and probabilistic Galois theory, in *Analytic number theory*, (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 91–101. Amer. Math. Soc., Providence, R.I., 1973.
- [Ga] S. Gao, Absolute irreducibility of polynomials via Newton polytopes, *J. Algebra* **237** (2001), no. 2, 501–520
- [Gou] F. Q. Gouvêa, *p-adic numbers*, Second edition, Springer, Berlin, 1997
- [Go] R. Gow, Some Generalized Laguerre polynomials whose Galois groups are the Alternating groups, *J. Number Theory* **31** (1989), no. 2, 201–207
- [H1] F. Hajir, Some \tilde{A}_n -extensions obtained from Generalized Laguerre polynomials, *J. Number Theory* **50** (1995), no. 2, 206–212
- [H2] F. Hajir, Algebraic properties of a family of Generalized Laguerre Polynomials, preprint, 2004, 19pp.
- [HW] F. Hajir and S. Wong, Specializations of one-parameter families of polynomials, preprint, 2004, 26pp.
- [Ha] M. Hall, *The theory of groups*. Macmillan, 1959.
- [J] C. Jordan, Sur la limite de transitivité des groupes non alternés, *Bull. Soc. Math. France*, **1** (1872-3), 40–71
- [K] T. Kondo, Algebraic number fields with the discriminant equal to that of a quadratic number field. *J. Math. Soc. Japan* **47** (1995), no. 1, 31–36
- [L] E. Laguerre, Sur l'intégrale $\int_0^\infty \frac{e^{-x} dx}{x}$, *Bull. Soc. math. France* **7** (1879) 72-81. Reprinted in *Oeuvres*, Vol. 1. New York: Chelsea, pp. 428-437, 1971
- [MMY] B. H. Matzat, J. McKay and K. Yokoyama, Algorithmic methods in Galois theory, *J. Symbolic Comput.* **30** (2000), no. 6. Academic Press, Oxford, 2000. pp. 631–872
- [Mo] J. Mott, Eisenstein-type irreducibility criteria, Zero-dimensional commutative rings (Knoxville, TN, 1994), 307–329, *Lecture Notes in Pure and Appl. Math.*, 171, Dekker, New York, 1995
- [PS] G. Pólya and G. Szegő, *Problems and theorems in analysis. Vol. II*, Revised and enlarged translation by C. E. Billigheimer of the fourth German edition, Springer Study Edition, Springer, New York, 1976
- [Sc1] I. Schur, Gleichungen Ohne Affekt, *Gesammelte Abhandlungen. Band III*, Springer, Berlin, 1973, pp. 191-197.
- [Sc2] I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, *Gesammelte Abhandlungen. Band III*, Springer, Berlin, 1973, pp. 227-233.
- [S] E. Sell, On a certain family of Generalized Laguerre Polynomials, *J. Number Theory* (2004), to appear.
- [So] N. J. Sonin, Recherches sur les fonctions cylindriques et le développement des fonctions continues en séries, *Math. Ann.* **16** (1880), 1-80

E-mail address: hajir@math.umass.edu

DEPARTMENT OF MATHEMATICS & STATISTICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MA
01003-9318 USA