Some Generalized Laguerre Polynomials Whose Galois Groups Are the Alternating Groups

R. Gow

Mathematics Department, University College, Belfield, Dublin 4, Ireland

Communicated by H. Zassenhaus
Received December 18, 1987

Following work of I. Schur, we show that the Galois group of the generalized Laguerre polynomial $F_{2n} = e^{x}x^{-2n}(d^{2n}(e^{-x^{2}})/dx^{2n})$ is the alternating group of degree $2n$, provided that $F_{2n}$ is irreducible over the rationals. We show irreducibility when $n = p^{k}$, $p$ a prime greater than 3. These polynomials may fill a gap left in Schur's search for explicit rational polynomials whose Galois group is the alternating group.

In two papers, [2, 3], I. Schur investigated the Galois groups of certain rational polynomials that play an important role in analysis. Of particular interest in this respect are the generalized Laguerre polynomials $L_{n}^{(\alpha)}$, defined as

$$n! e^{-x^{2}}L_{n}^{(\alpha)}(x) = \frac{d^{n}(e^{-x^{2}}+\alpha)}{dx^{n}},$$

where $\alpha$ is a constant. We have then

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

Schur showed that $L_{n}^{(\alpha)}$ is irreducible over the rational numbers $Q$ when $\alpha = 0$ or 1, and the Galois group of $L_{n}^{(0)}$ (the classical Laguerre polynomial) is the symmetric group $S_{n}$. He also showed that the Galois group of $L_{n}^{(1)}$ is the alternating group $A_{n}$ if $n$ is odd or if $n+1$ is an odd square; otherwise the Galois group is $S_{n}$. In addition, Schur showed that the truncated exponential function

$$\sum_{m=0}^{n} \frac{x^{m}}{m!}$$

is irreducible and has Galois group $A_{n}$ if 4 divides $n$. 

201
Schur's results give explicit irreducible polynomials of degree $n$ over $Q$ having Galois group $A_n$ when $n = 4k$ or $2k + 1$ and he remarked in [3] that it would be of interest to realize the missing case when $n = 4k + 2$ in a similar concrete way. The purpose of this paper is to show that when $n$ is even, the polynomial $F_n$ defined by

$$F_n = (-1)^n n! L_{n}^{(n)}$$

has Galois group $A_n$ provided that the polynomial is irreducible over $Q$. We have not been able to prove that the polynomial is irreducible in general, except when $n$ either has the form $2p^k$, $p$ a prime greater than 3, or the form $4p^k$, $p$ a prime greater than 7. We have also verified that the polynomial is irreducible for even values of $n \leq 26$.

1. The Galois Group of $F_n$

The polynomial $F_n$ is monic integral of degree $n$ and is expressible in the form

$$F_n = \sum_{m=0}^{n} \binom{2n}{m} \binom{n}{m} m!(-1)^m x^{n-m}.$$ 

We put $k_j = j(n + j)$, $1 \leq j \leq n$.

(1.1) Lemma. The discriminant $D$ of $F_n$ is a square if $n$ is even.

Proof. Schur shows in [3, Section 2] that

$$D = n! k_2 k_3^2 \cdots k_n^{n-1}.$$ 

Thus if $n = 2m$, working modulo squares, we have

$$D \equiv (2m)! k_2 k_4 \cdots k_{2m}.$$ 

We obtain

$$D \equiv (2m)! 2(2m + 2) 4(2m + 4) \cdots 2m(2m + 2m) \equiv ((2m)!)^2 2^{2m},$$

which proves our contention.

(1.2) Lemma. If $n \geq 14$ or if $n = 10$, there exists a prime $p$ satisfying

$$\frac{2n}{3} < p < n - 2.$$ 

Proof. This follows from [1, Sect. 4(b), p. 120].
(1.3) **Lemma.** Assume that $p$ is a prime satisfying $2n/3 < p < n$. Then $p^n$ divides the discriminant $D$ of $F_n$.

**Proof.** As before, we have

$$D = n! k_1^2 k_2^3 \cdots k_n^{n-1},$$

where $k_j = j(n + j)$. Certainly $p$ divides $n!$ and $p$ also divides $k_j$ when $j = p$ or $2p - n$. Thus the exponent of the power of $p$ that divides $D$ is at least

$$1 + p - 1 + 2p - n - 1 = 3p - n - 1.$$ 

As we are assuming that $p > 2n/3$, we have

$$3p - n - 1 \geq n,$$

which proves the lemma.

(1.4) **Lemma.** Let $p$ be a prime satisfying $2n/3 < p < n$. Then we have

$$F_n = x^n F_{n-p} \pmod p$$

and $p$ does not divide the discriminant of $F_{n-p}$.

**Proof.** We have

$$F_n = x^n - k_n x^{n-1} + \cdots + (-1)^n \frac{k_n k_{n-1} \cdots k_1}{n!},$$

as shown in [3, Sect. 2]. We also know that the coefficient of $x^r$ in $F_n$ is

$$\binom{2n}{n} \frac{n!}{(n-r)!r!}$$

and this is divisible by $p$ if $r < p$. It follows that

$$F_n \equiv x^n - k_n x^{n-1} + \cdots + (-1)^n \frac{k_n \cdots k_{n-p+1}}{(n-p)!} x^p \pmod p.$$ 

Write $m = n - p$. Then we have

$$k_{n-j} \equiv (m-j)(2m-j) \pmod p$$

and thus $k_{n-j} \equiv k_{m-j} \pmod p$. It is now clear that

$$F_n \equiv x^n F_m \pmod p.$$ 

Moreover as $2n < 3p$, we have $p > 2m$ and therefore $k_{m-j} = (m-j)(2m-j)$.
is not divisible by \( p \) for \( 1 \leq j \leq m \). It follows that the discriminant of \( F_m - F_{n-p} \), which is a product of \( m! \) and various powers of the \( k_{m-j} \), is prime to \( p \), as required.

The following lemma is clear.

(1.5) Lemma. Let \( p \) be a prime with \( 2n/3 < p < n \), \( n \geq 4 \). Then the constant term of \( F_n \) is divisible by \( p \) but not by \( p^2 \).

We can now prove our first main result.

(1.6) Theorem. Let \( n \) be an even integer. Then if the polynomial \( F_n \) is irreducible over \( Q \), its Galois group is \( A_n \).

Proof. This follows from our five lemmas and the criterion of Schur given in [2, Sect. 1], provided \( n \neq 4, 6, 8, \) or 12. We defer the proof for the four exceptional cases until the end of the next section.

2. Irreducibility of \( F_n \) in Some Special Cases

It seems to us to be a difficult problem to show the \( F_n \) is irreducible for all even \( n \geq 4 \) and thus Theorem 1.6 is not as decisive as we would wish it to be. While irreducibility can be proved by a variety of special devices for small values of \( n \), we have only obtained one general criterion, which we will describe here.

For a fixed prime \( p \), let \( v(n) \) be the exponent of the exact power of \( p \) that divides the integer \( n \). If we write \( n \) in its \( p \)-adic representation

\[
n = \sum_{j=0}^{k} a_j p^j, \quad 0 \leq a_j \leq p - 1,
\]

we then put

\[
\sigma(n) = \sum_{j=0}^{k} a_j, \quad \sigma(0) = 0
\]

Then, as proved in [1, p. 103], we have

\[
v(n!) = \frac{n - \sigma(n)}{p - 1}.
\]

Now write

\[
F_n = \sum_{m=0}^{n} a_m p^{e_m x^{n-m}},
\]

where \( p \) does not divide \( a_m \).
Assuming this notation, we have the following result of Dumas [1, p. 100].

(2.1) **Lemma.** Suppose that \( e_0 = 0 \) and \( e_m \geq m e_n / n \) for \( 1 \leq m \leq n \). Then the irreducible factors of \( F_n \) have degree of the form \( n t / t \), where \( t = (n, e_n) \) and \( 1 \leq t \leq n \).

It is straightforward to evaluate \( e_m \) for the polynomial \( F_n \).

(2.2) **Lemma.** We have

\[
(p - 1) e_m = m - \sigma(2n) - \sigma(n) + \sigma(2n - m) + \sigma(n - m) + \sigma(m).
\]

We can now prove the technical lemma required to apply Lemma 2.1.

(2.3) **Lemma.** Let \( n = 2p^k \) where \( p \geq 5 \) is a prime. Then \( e_n = (n - 2) / (p - 1) \) and \( t = 2 \). Moreover, \( e_m \geq m e_n / n \) for \( 1 \leq m \leq n \).

**Proof.** As \( p \geq 5 \), we clearly have

\[
\sigma(n) = 2, \quad \sigma(2n) = 4.
\]

The values for \( e_n \) and \( t \) follow immediately from this. We wish now to show that

\[
(p - 1) e_m \geq \frac{m(n - 2)}{n},
\]

which amounts to showing that

\[
\sigma(2n - m) + \sigma(n - m) + \sigma(m) \geq \frac{6n - 2m}{n}.
\]

We can clearly assume that \( 0 < m < n \). Since \( 2n = 4p^k \) and \( m < 2p^k \), we must have

\[
\sigma(2n - m) \geq 3.
\]

Similarly, \( \sigma(n - m) \), \( \sigma(m) \geq 1 \). Moreover, if \( \sigma(m) = \sigma(n - m) = 1 \), we must have \( m = p^k \) and in this case the required inequality holds, as \( 2m/n = 1 \). Otherwise,

\[
\sigma(2n - m) + \sigma(n - m) + \sigma(m) \geq 6
\]

holds, which proves what we want.
We can now find a series of values of $n$ for which $F_n$ is irreducible.

(2.4) **Theorem.** Let $n = 2p^k$, where $p \geq 5$ is a prime. Then $F_n$ is irreducible over $\mathbb{Q}$.

**Proof.** It follows from Lemmas 2.1 and 2.3 that $F_n$ is either irreducible or else it factors into two irreducible polynomials of degree $p^k$. As $n \geq 10$, there exists a prime $q$ with

$$\frac{3n}{2} < q < 2n.$$  

This follows easily from the theorem of R. Breusch, quoted in [1, p. 102]. This prime $q$ divides the coefficient of $x^{n-m}$ for $m > 2n - q$ and moreover $q^2$ does not divide the constant term of $F_n$. It follows that

$$F_n \equiv x^q - G \pmod{q},$$

where $G$ is some integral polynomial of degree $2n - q$. The argument used to prove Eisenstein's irreducibility criterion now shows that $F_n$ must have an irreducible factor of degree at least $q - n$. However, our choice of $q$ shows that $q - n > n/2$ and it follows that $F_n$ is irreducible.

Using the theorem of R. Breusch mentioned above, a slightly more complicated argument proves the following result. We omit the proof.

(2.5) **Theorem.** Let $p \geq 11$ be a prime. Then if $n = 4p^k$, $F_n$ is irreducible.

These ideas can be generalized to the following criterion.

(2.6) **Theorem.** Given a positive integer $r$ and any prime $p > 2r$, there is some integer $n_0$, depending on $r$, such that if $n = rp^k$ and $n > n_0$, $F_n$ is irreducible.

This follows from the prime number and the line of reasoning above. See, for example, [1, p. 102].

### 3. The Galois Group of $F_n$ for Small Values of $n$

Schur's method is not sufficient to calculate the Galois group of $F_n$ for the values 4, 6, 8, and 12 of $n$. We resort to the method of factorizing $F_n$ modulo small primes that do not divide the discriminant to deal with these outstanding cases.
(3.1) Theorem. \( F_n \) is irreducible and has Galois group \( A_n \) for \( n = 4, 6, 8, \) and 12.

Proof. The irreducibility of \( F_n \) for these values is easily shown by ad hoc techniques. Let \( G \) denote the Galois group of \( F_n \). For \( n = 4 \), 4 divides \( |G| \) and 3 also divides \( |G| \) by the discriminant criterion of Schur. Thus \( G \) must be \( A_4 \) in this case.

When \( n = 6 \), 30 divides \( |G| \) by irreducibility and the discriminant criterion. Thus \( G \) is doubly transitive of degree 6. We also have the factorization into irreducibles

\[
F_6 \equiv (x + 6)(x + 14)(x + 30)(x^3 + x^2 + 16x - 23)
\]

mod 41, and it follows that \( G \) contains a 3-cycle, by a theorem of Dedekind. Thus \( G \) must be \( A_6 \), by Jordan’s theorem.

For \( n = 8 \), \( G \) is certainly doubly transitive of degree 8 by the same arguments as above. We have the following factorization

\[
F_8 \equiv (x^5 - 17x^4 + 22x^3 - 29x^2 + 14x - 25)(x^3 - 17x^2 + 17x - 32)
\]

into irreducibles mod 47. Thus \( G \) contains a 3-cycle and again we deduce that \( G \) is \( A_8 \).

For \( n = 12 \), \( G \) is doubly transitive of degree 12. We have the factorization

\[
F_{12} \equiv (x^7 - 6x^6 + 27x^5 - 14x^4 + 34x^3 - 35x^2 - 5x - 4) \\
\times (x^5 - 17x^4 - 2x^3 - 19x^2 + 35x + 5)
\]

into irreducibles mod 53. It is straightforward to see that \( G \) must be \( A_{12} \).

(The factorizations of \( F_8 \) and \( F_{12} \) were obtained by the use of a computer.) This completes the proof.

We mention finally that it is easy to see that if \( n = p + 1 \) or \( 2n = p + 1 \) for a prime \( p \), \( F_n \) is either irreducible or factorizes into irreducibles of degree \( n - 1 \) and 1. By checking \( F_n \) for integral roots, we find that \( F_n \) is irreducible for even \( n \) not exceeding 26.

References