Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

John CULLINAN, Farshid HAJIR et Elizabeth SELL

Algebraic properties of a family of Jacobi polynomials

Tome 21, n^o 1 (2009), p. 97-108.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_1_97_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 97-108

Algebraic properties of a family of Jacobi polynomials

par John CULLINAN, Farshid HAJIR et Elizabeth SELL

Résumé. La famille des polynômes à un seul paramètre $J_n(x,y) = \sum_{j=0}^{n} \binom{y+j}{j} x^j$ est une sous-famille de la famille (à deux paramètres) des polynômes de Jacobi. On montre que pour chaque $n \geq 6$, quand on spécialise en $y_0 \in \mathbf{Q}$, le polynôme $J_n(x, y_0)$ est irréductible sur $\mathbf{Q}$, sauf pour un nombre fini des valeurs $y_0 \in \mathbf{Q}$. Si n est impair, sauf pour un nombre fini des valeurs $y_0 \in \mathbf{Q}$, le groupe de Galois de $J_n(x, y_0)$ est S_n ; si n est pair, l'ensemble exceptionnel est mince.

Abstract. The one-parameter family of polynomials $J_n(x,y) = \sum_{j=0}^{n} \binom{y+j}{j} x^j$ is a subfamily of the two-parameter family of Jacobi polynomials. We prove that for each $n \geq 6$, the polynomial $J_n(x, y_0)$ is irreducible over $\mathbf{Q}$ for all but finitely many $y_0 \in \mathbf{Q}$. If n is odd, then with the exception of a finite set of y_0, the Galois group of $J_n(x, y_0)$ is S_n; if n is even, then the exceptional set is thin.

1. Introduction

For an integer $n \geq 1$ and complex parameters α, β, define the polynomial

$$J_n^{(\alpha,\beta)}(x) := \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \binom{n+\alpha+\beta+j}{j} x^j.$$

It is a slightly renormalized version of the *Jacobi polynomial*

$$P_n^{(\alpha,\beta)}(x) := J_n^{(\alpha,\beta)}\left(\frac{x-1}{2}\right).$$

In terms of the Gauss hypergeometric series

$${}_2F_1(a,b;-,c|z) := \sum_{\nu=0}^{\infty} \frac{(a)_\nu (b)_\nu}{(c)_\nu} \frac{z^\nu}{\nu!}, \qquad (a)_\nu := (a)(a+1)\cdots(a+\nu-1),$$

we have

$$P_n^{(\alpha,\beta)}(x) = {}_2F_1\left(-n, n+\alpha+1+\beta; -, \alpha+1 | \frac{1-x}{2}\right).$$

Mots clefs. Orthogonal polynomials, Jacobi polynomial, Rational point, Riemann-Hurwitz formula, Specialization.

Many important families of polynomials are obtained as specializations of Jacobi polynomials; among them we mention the Tchebicheff polynomials of the first ($T_n(x)$) and second kind ($U_n(x)$), the ultraspherical polynomials $P_n^{(\alpha,\alpha)}(x)$ (also called Gegenbauer polynomials), and the Legendre polynomials $P_n^{(0,0)}(x)$. Jacobi polynomials, together with the Generalized Laguerre polynomials

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

and the Hermite polynomials

$$H_{2n}(x) := (-1)^n 2^{2n} n! L_n^{(-1/2)}(x^2)$$
$$H_{2n+1}(x) := (-1)^n 2^{2n+1} n! x L_n^{(1/2)}(x^2)$$

are the three classical families of orthogonal polynomials. Among all families of orthogonal families, they are distinguished by the fact that their derivatives are also members of the same family. Orthogonal polynomials play a very important role in analysis, mathematical physics, and representation theory.

The systematic study of algebraic properties of families of orthogonal polynomials was initiated by Schur. He showed, for instance, that the Hermite polynomials are irreducible over $\mathbf{Q}$ and determined their Galois groups [13].

The algebraic properties of some of the specializations of $P_n^{(\alpha,\beta)}(x)$ have been known for quite some time (*e.g.* T_n, U_n) whereas for others they appear to be quite difficult to establish (*e.g.* the Legendre polynomials $P_n^{(0,0)}$). Other hypergeometric families related to the theory of modular forms are specializations of Jacobi polynomials. For example, that the polynomials $P_n^{(\pm 1/2, \pm 1/3)}(x)$ are irreducible with Galois group S_n is equivalent to the conjecture introduced and studied by Mahlburg and Ono in [11]; these polynomials are on the one hand related to traces of singular moduli via work of Kaneko-Zagier [9], and, up to simple factors, the supersingular polynomial for a prime p where $n = \lfloor p/12 \rfloor$ ([1], [2]).

In a recent work, Hajir-Wong [7] describe a method for studying the exceptional set for a one-parameter family $F_n^{(t)}(x) \in \mathbf{Q}[x,t]$ of polynomials, *i.e.* the set of $\alpha \in \mathbf{Q}$ for which $F_n^{(\alpha)}(x)$ is reducible. By applying their method, which is a combination of group theory and algebraic geometry, they showed that for each $n \geq 5$, for all but finitely many $\alpha \in \mathbf{Q}$ the generalized Laguerre polynomial $L_n^{(\alpha)}(x)$ is irreducible over $\mathbf{Q}$ and has Galois group S_n.

In the current work, we show a similar result for the polynomial

$$J_n(x,y) = (-1)^n J_n^{(-1-n,y+1)}(-x) = \sum_{j=0}^{n} \binom{y+j}{j} x^j;$$

more precisely:

Theorem 1.1. *Let $n \geq 6$ be an integer and let $J_n(x,y) = \sum_{j=0}^{n} \binom{y+j}{j} x^j$. Then the polynomials $J_n(x,y_0)$ are irreducible over $\mathbf{Q}$ for all but finitely many $y_0 \in \mathbf{Q}$. Moreover, if n is odd then the Galois group of $J_n(x,y_0)$ is equal to S_n for all but finitely many $y_0 \in \mathbf{Q}$. If n is even, then there is a thin set of y_0 for which the Galois group is A_n.*

This result is far from effective, however, since the main tool for obtaining the result is Faltings' theorem. We follow the strategy outlined in Hajir-Wong. We show that, as a polynomial over $\mathbf{Q}(y)$, $J_n(x,y)$ is irreducible with Galois group S_n. We then estimate the genus of the curve defined by the polynomial, as well as other minimal subfields in the Galois closure of its function field, allowing us to apply the theorem of Faltings to obtain the finitude of the exceptional set using a criterion described, for example, in Müller [12]. In addition we also obtain an exact expression for the genus of the curve X_1.

Theorem 1.2. *Let X_1 be the algebraic curve defined by $J_n(x,y)$. Then the genus of the normalization of X_1 is $\binom{n-1}{2}$.*

Acknowledgements. We would like to thank Siman Wong for useful discussions and the referee for many helpful comments and suggestions.

2. The one-parameter family

The linear change of variables

$$r = -1 - n - \alpha$$
$$s = -1 - r + \beta$$

allows us to rewrite the Jacobi polynomials in terms of the parameters r and s:

$$(2.1)\quad P_n^{\langle r,s\rangle}(x) := (-1)^n P_n^{(-1-n-r,r+s+1)}(-x) = \sum_{j=0}^{n} \binom{-1-r}{n-j} \binom{s+j}{j} x^j.$$

Set $r = 0$ to get the one-parameter family (with $s = y$) given by:

$$J_n(x,y) = P_n^{\langle 0,y\rangle}(x) = \sum_{j=0}^{n} \binom{y+j}{j} x^j = \sum_{j=0}^{n} (y+1)\cdots(y+j)\frac{x^j}{j!}.$$

Let $\widehat{P}_n(x,y)$ be the reverse of $J_n(x,y)$ as a polynomial in x, *i.e.*

$$\widehat{P}_n(x,y) := x^n J_n(1/x,y) = \sum_{j=0}^{n} \binom{y+j}{j} x^{n-j}.$$

Clearly $\widehat{P}_n(x,y)$ and $J_n(x,y)$ have the same irreducibility and Galois-theoretic properties. With another linear change of variables we obtain a more convenient form of the polynomial, which we will work with for the rest of the paper:

$$P_n(x,y) := (-1)^n \widehat{P}_n(-x,-y-1) = \sum_{j=0}^{n} \binom{y}{j} x^{n-j}.$$

Fix $n \geq 6$ and define the algebraic curve $X_1 \subset \mathbf{P}^2_{\mathbf{Q}}$ as the projective closure of the zero-set of $P_n(x,y)$. Let X' denote the smooth curve corresponding to the Galois closure K' of $P_n(x,y)$ over $\mathbf{Q}(y)$. Following [7], we will show:

- For each $n \geq 6$, the polynomial $P_n(x,y)$ has an irreducible $\mathbf{Q}$-rational specialization with Galois group S_n.
- The genera of the intermediate subfields $\mathbf{Q}(y) \subset E \subset K'$ are all ≥ 2 with the exception of the fixed-field of A_n when n is even.

In fact, when n is even there will be a thin set of y_0 for which the specialized polynomial $P_n(x,y_0)$ has Galois group A_n. These steps will constitute a proof of Theorem 1.1 following the strategy outlined in [7].

3. Galois properties of $P_n(x,y)$

In this section, we compute the Galois group of our polynomial $P_n(x,y)$ over $\mathbf{Q}(y)$. In a first draft of this paper, we did this by effectively finding an irreducible specialization with Galois group S_n over $\mathbf{Q}$. We give a brief sketch of our original argument. To establish irreducibility, we compare the p-adic Newton polygons (for each $p|n$) of the $P_n(x,y)$ to those of the truncated exponential polynomials $e_n(x)$ which are known to be irreducible [5, lem. 2.7]. Once irreducibility is established, one can show that there exists a prime in the interval $(n/2, n-2)$ such that the ℓ-adic Newton polygons of $P_n(x,y)$ and $e_n(x)$ coincide. By [6, thm. 2.2], the Galois group of $P_n(x,y)$ then contains A_n. To conclude that the Galois group is all of S_n, it suffices to show the discriminant of $P_n(x,y)$ is not a square. Effectivity is not required for the results of the paper, and the details are intricate, so we present a simpler proof. We would like to take this opportunity to thank the referee for providing us with this approach. We start by writing down the discriminant formula for $P_n(x,y)$ as a polynomial in y, which we get easily by specializing the formula for the discriminant of the Jacobi

Polynomial [16, p. 143]:

$$\operatorname{disc}(P_n(x,y)) = \frac{(-1)^{n(n-1)/2}}{(n!)^{n-2}}(y)(y-n)\prod_{j=0}^{n}(y-j)^{n-2}.$$

Proposition 3.1. *For all $n \geq 2$ the polynomial $P_n(x,y)$ is irreducible and has Galois group S_n over $\mathbf{Q}(y)$.*

Proof. It is easy to check that $P_n(x,y) = \sum_{j=0}^{n}\binom{y}{j}x^{n-j}$ is Eisenstein at the place y. This gives irreducibility.

For the Galois group G, the discriminant formula above shows that specialization of $P_n(x,y)$ at $y_0 = 0,\ldots,n$ factors as $P_n(x,y_0) = x^{n-k}(x+1)^k$ for all $k = 0,\ldots,n$. Hence, the inertia subgroup of G contains permutations of cycle type $(n-k,k)$ for all $k = 0,\ldots n$. When $k = 1$, this means G contains an $(n-1)$-cycle and hence is a 2-transitive subgroup of S_n. If n is odd, then the $(n-2)$th power of an element of cycle type $(n-2,2)$ is a transposition. This implies G is all of S_n.

If n is even, let $n = 2^\ell u$ with u and odd integer. If $u = 1$, take $k = 3$, if $u = 3$ take $k = 5$, and if $u \geq 7$, take $k = u-2$. This ensures that, except when $n = 4$ or 6, G contains a k-cycle with k in the range $[2, n/2)$. Thus G contains A_n. Since G contains odd permutations, G is all of S_n.

When $n = 2, 4$ or 6, the specialization $y = 3, 8$, or 11 (for example) yields a polynomial with Galois group S_2, S_4 or S_6, respectively. Since the Galois group of $P_n(x,y_0)$ is a subgroup of the Galois group of $P_n(x,y)$ for all good specializations, this means means $P_2(x,y), P_4(x,y)$ and $P_6(x,y)$ have Galois groups S_2, S_4 and S_6, respectively. This completes the proof. □

4. A genus formula

The goal of this section is to prove Theorem 4.1 below on the genus of the curve X_1. We remark that X_1 is a singular curve, so by abuse of language, we refer to the genus of the normalization of X_1 as the genus of X_1. Let $\iota_n : X_1 \longrightarrow \mathbf{P}^1$ be the projection-to-y map. The discriminant formula above shows that the branch locus of ι_n is given by

$$B_n = \{0,\ldots,n\}.$$

The Riemann-Hurwitz formula implies

$$2g(X_1) - 2 = \deg(\iota_n)(-2) + \sum_{P\in X_1}(e_P - 1).$$

As in the previous section, one checks that $P_n(x,\nu) = x^{n-\nu}(x+1)^\nu$ for all $\nu \in B_n$. Moreover, one checks easily that there is no ramification at infinity (taking note of the fact that $e_n(x) = \sum_{j=0}^{n} x^j/j!$ has discriminant $n!\prod_{j=2}^{n} j^{j-1}$ by [13, p. 229] hence is separable). Thus, there are $2n$ points of X_1 ramified above $\mathbf{P}^1$, with the given ramification indices. The degree of ι_n is n, so altogether this gives

$$g(X_1) = \frac{1}{2}\left(-2n + \frac{n(n+1)}{2} + \frac{n(n+1)}{2} - 2n\right) + 1 = \frac{1}{2}\left(n^2 - 3n + 2\right),$$

and hence:

Theorem 4.1. *Let g_n denote the geometric genus of the normalization of X_1. Then $g_n = \binom{n-1}{2}$.*

5. Genus of maximal subfields

Recall the following notation: K' is the Galois closure of the field $K_1/\mathbf{Q}(y)$ which is the function field of the covering $X_1/\,\mathbf{P}^1$ where X_1 is given by the model $P_n(x, y) = 0$. We have shown in Section 3 that the Galois group of $K'/\mathbf{Q}(y)$ is S_n. We adopt the notation of [7]. Let E be an intermediate field of $K'/\mathbf{Q}(y)$, let $\mathcal{E} = \mathrm{Gal}(K'/E)$, and let X_E be the smooth curve with function field E. Following [7, thm. 3], we will now show that if $P_n(x, y)$ is reducible over E, then the genus of X_E is greater than 1. We will achieve this by showing that the genera of the *minimal* subfields of K' over which $P_n(x, y)$ is reducible (corresponding to maximal subgroups of S_n) are each greater than 1.

Recall the definition of simple branch point from [7, def. 2], and recall our notation: $B_n = \{0, \ldots, n\}$ is the branch locus of the projection-to-y map $\iota_n : X_1 \longrightarrow \mathbf{P}^1$. Consequently:

Lemma 5.1. *The branch points $\nu = 0, 1, (n-1)$, and n are simple of index n, $n-1$, $n-1$, and n, respectively.*

Now we estimate the genera of the intermediate subfields. Our strategy is as follows. We start with the maximal subgroups of S_n other than A_n; they will all be shown to have fixed field of genus exceeding 1. For even n, the fixed field of A_n has genus 0 but it turns out that $P_n(x, y)$ is irreducible over that field. It will then remain to show that the fixed fields of the maximal subgroups of A_n all have genus exceeding 1.

Since the rest of the paper involves computations with the maximal subgroups of S_n, we appeal to the structure theorem of [10]: if G is A_n or S_n, and $\mathcal{E}$ is any maximal subgroup of G with $\mathcal{E} \neq A_n$, then $\mathcal{E}$ satisfies one of the following:

(a) $\mathcal{E} = (S_m \times S_k) \cap G$, with $n = m + k$ and $m \neq k$.
(b) $\mathcal{E} = (S_m \wr S_k) \cap G$, with $n = mk$, $m > 1$ and $k > 1$.
(c) $\mathcal{E} = \mathrm{AGL}_k(\mathbf{F}_p) \cap G$, with $n = p^k$ and p prime.
(d) $\mathcal{E} = (T^k \cdot (\mathrm{Out}\, T \times S_k)) \cap G$, with T a non-abelian simple group, $k \geq 2$ and $n = \#T^{k-1}$.
(e) $\mathcal{E} = (S_m \wr S_k) \cap G$, with $n = m^k$, $m \geq 5$ and $k > 1$, excluding the case where $\mathcal{E}$ is imprimitive.
(f) $T \triangleleft \mathcal{E} \leq \mathrm{Aut}\, T$, with T a non-abelian simple group, $T \neq A_n$, and $\mathcal{E}$ primitive.

For completeness, we recall the notion of a primitive group [4, p. 12]. Let G be a group acting transitively on a set Ω. A non empty subset Δ of Ω is called a *block* for G if for each $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$. The group G is called *primitive* if it has no nontrivial blocks. The groups of type (a) and (b) are imprimitive, while types (c)-(f) are primitive.

Proposition 5.1. *Let $n \geq 6$. If $\mathcal{E}$ is a maximal subgroup of S_n other than A_n, with corresponding fixed-field E, then $g(X_E) > 1$.*

Proof. Let $V = \{0, 1, n-1, n\}$ be the set of simple branch points of $\iota_n : X_1 \longrightarrow \mathbf{P}^1$. Following [7], let $d(k)$ be the least prime divisor of the positive integer k, and define $c_1(\nu)$ as in [7, defn. 1]. Every $\nu \in V$ is simple, so by [7, lem. 6], $c_1(\nu)$ is easily computed:

$$c_1(\nu) = \frac{(\#\text{ of } e_\nu\text{-cycles in } \mathcal{E})}{\#\mathcal{E}} \times e_\nu(n - e_\nu)! < e_\nu(n - e_\nu)!.$$

We now employ the genus estimate of [7, (4.1)]

$$g(X_E) \geq 1 + \frac{[S_n : \mathcal{E}]}{2}\left(-2 + \sum_{\nu \in V}\left(1 - \frac{1}{d(e_\nu)}\right)\right) - \frac{1}{2}\sum_{\nu \in V} c_1(\nu)\left(1 - \frac{1}{d(e_\nu)}\right).$$

For each $\nu \in V$, the ramification index e_ν is either n or $n-1$. In particular, two of the four e_ν are even and for those, $d(e_\nu) = 2$; for the others $d(e_\nu) \geq 3$. Let N be the odd element of the set $\{n, n-1\}$. Then

$$\left(-2 + \sum_{\nu \in V}\left(1 - \frac{1}{d(e_\nu)}\right)\right) = -2 + 4 - \frac{1}{2} - \frac{1}{2} - \frac{2}{d(N)} \geq 1 - \frac{2}{3} = \frac{1}{3}.$$

We now split the rest of the proof into three cases based on the structure of the maximal subgroup $\mathcal{E}$.

Case 1 – imprimitive wreath products

Here we must take $n \geq 4$. The maximal imprimitive wreath products contain no n or $(n-1)$-cycles, hence $c_1(\nu) = 0$ for all $\nu \in V$. The genus estimate for $\mathcal{E} = S_j \wr S_{n/j}$ is therefore

$$g(X_E) \geq 1 + \frac{1}{6} \cdot \frac{n!}{(j!)^{n/j}(n/j)!},$$

which is greater than 1.

Case 2 – intransitive subgroups

Take $n \geq 3$. None of the subgroups $S_j \times S_{n-j}$ will contain an n-cycle, and will only contain an $(n-1)$-cycle when $j = 1$. Hence for $j = 2, \ldots, \lfloor \frac{n-1}{2} \rfloor$, the genus estimate is

$$g(X_E) \geq 1 + \frac{n!}{j!(n-j)!},$$

which is greater than 1. When $j = 1$, the subgroup S_{n-1} of S_n contains $(n-2)!$ cycles of length $(n-1)$. Hence the genus estimate becomes

$$g(X_E) \geq 1 + \frac{1}{6}\frac{n!}{(n-1)!} - \frac{1}{2} \cdot 2 \cdot \frac{(n-2)!}{(n-1)!} \cdot (n-1) \cdot 1!(1 - \frac{1}{3}) = \frac{n}{6} + \frac{1}{3},$$

which is greater than 1 when $n \geq 5$.

Case 3 – primitive subgroups

If $\mathcal{E}$ is a proper primitive subgroup of S_n other than A_n, then Bochert's theorem [4, p. 79] bounds its index in S_n:

$$[S_n : \mathcal{E}] \geq \lfloor \frac{n+1}{2} \rfloor !.$$

The basic estimate $(1 - 1/d(e_\nu)) \leq 1 - 1/n$ gives us

$$\begin{aligned} g(X_E) &\geq 1 + \frac{1}{6} \cdot \lfloor \frac{n+1}{2} \rfloor ! - \frac{1}{2}\left(1 - \frac{1}{n}\right) \sum_{\nu \in V} c_1(\nu) \\ &\geq 1 + \frac{1}{6} \cdot \lfloor \frac{n+1}{2} \rfloor ! - \frac{1}{2}\left(1 - \frac{1}{n}\right)(n + (n-1) + (n-1) + n) \\ &= 1 + \frac{1}{6} \cdot \lfloor \frac{n+1}{2} \rfloor ! - \left(2n - 3 + \frac{1}{n}\right). \end{aligned}$$

This gives $g(X_E) > 1$ when $n \geq 9$. For a more refined estimate, we investigate the primitive subgroups of the symmetric groups.

Let $n = 8$. Then the maximal primitive subgroups of S_8 other than A_8 are $2^3.\mathrm{PSL}_2(\mathbf{F}_7)$ and $\mathrm{PGL}_2(\mathbf{F}_7)$. The group $2^3.\mathrm{PSL}_2(\mathbf{F}_7)$ has order 1344, contains 384 7-cycles, and no 8-cycles. This gives

$$g(X_E) \geq 1 + \frac{1}{6} \cdot \frac{8!}{1344} - \frac{1}{2}\left(1 - \frac{1}{8}\right)\left(0 + 0 + \frac{384}{1344} \cdot 7 \cdot 1! + \frac{384}{1344} \cdot 7 \cdot 1!\right) = \frac{17}{4}.$$

The order of $\mathrm{PGL}_2(\mathbf{F}_7)$ is 336 and it contains 48 7-cycles and 84 8-cycles, hence

$$g(X_E) \geq 1 + \frac{1}{6} \cdot \frac{8!}{336} - \frac{1}{2}\left(1 - \frac{1}{8}\right)\left(2 \cdot \frac{48}{336} \cdot 7 \cdot 1! + 2 \cdot \frac{84}{336} \cdot 8 \cdot 0!\right) = \frac{147}{8}.$$

Now take $n = 7$. There is a unique maximal primitive subgroup of S_7 other than A_7, namely $\mathrm{PSL}_2(\mathbf{F}_7)$, which contains 48 7-cycles and no 6-cycles. Therefore

$$g(X_E) \geq 1 + \frac{1}{6} \cdot \frac{7!}{168} - \frac{1}{2}\left(1 - \frac{1}{7}\right)\left(2 \cdot \frac{48}{168} \cdot 7 \cdot 0!\right) = \frac{30}{7}.$$

The group S_6 has a unique maximal primitive subgroup other than A_6, namely $\mathrm{PGL}_2(\mathbf{F}_5)$. But $\mathrm{PGL}_2(\mathbf{F}_5) \simeq S_5 \simeq S_5 \times S_1$ is an intransitive direct-product subgroup of S_6 and hence was already analyzed. This completes the proof of the Proposition. □

Remark. When $n = 5$, the unique maximal primitive subgroup of S_5 other than A_5 is the Frobenius group F_{20} of order 20. It contains 10 4-cycles and 4 5-cycles. Using the exact values for the $d(e_\nu)$ yields

$$\begin{aligned} g(X_E) \geq 1 &+ \frac{1}{2} \cdot \frac{5!}{20}\left(-2 + 2\left(1 - \frac{1}{d(5)}\right) + 2\left(1 - \frac{1}{d(4)}\right)\right) \\ &- \frac{1}{2}\left(2 \cdot \frac{10}{20} \cdot 4 \cdot 1! \cdot \left(1 - \frac{1}{d(4)}\right) + 2 \cdot \frac{5}{20} \cdot 5 \cdot 0! \cdot \left(1 - \frac{1}{d(5)}\right)\right) = \frac{4}{5}, \end{aligned}$$

so a more detailed analysis would be required determine whether the genus of X_E is greater than 1.

The unique index-2 subgroup A_n of S_n corresponds to the field $\mathbf{Q}(y, \Delta_n)$ where $\Delta_n := \sqrt{\mathrm{disc}(P_n(x, y))}$. We have two different results based on whether n is even or odd.

Lemma 5.2. *Let $\mathcal{C}_n$ be the curve corresponding to the degree-2 field extension $\mathbf{Q}(y, \Delta_n)/\mathbf{Q}(y)$. If n is odd, then $\mathcal{C}_n$ has genus $\lfloor \frac{n-2}{2} \rfloor$; if n is even, then $\mathcal{C}_n$ has genus 0. In particular, for odd $n \geq 7$ and $\mathcal{E} = A_n$, we have $g(X_E) > 1$.*

Proof. Recall the discriminant of $P_n(x, y)$ as a polynomial in y is given by

$$\mathrm{disc}(P_n(x, y)) = \pm \frac{1}{(n!)^{n-2}}(y)(y - n) \prod_{j=1}^{n-1} (y - j)^{n-2},$$

where $\pm = (-1)^{n(n-1)/2}$. When n is even the square-free part of the discriminant is $\pm y(y - n)$, hence a model for $\mathcal{C}$ is given by

$$z^2 = \pm y(y - n),$$

which defines a smooth curve of genus 0. If n is odd, the square-free part of the discriminant is $\frac{\pm 1}{n!}\prod_{j=1}^{n-1}(y-j)$, and a model for $\mathcal{C}_n$ is given by

$$z^2 = \frac{\pm 1}{n!}\prod_{j=1}^{n-1}(y-j).$$

Therefore $\mathcal{C}_n$ is a hyperelliptic curve of genus $\lfloor \frac{n-2}{2} \rfloor$. □

We now take up the case where n is even, so that the genus of the fixed-field of A_n is always 0. By [7, Prop. 3], it suffices to consider the maximal *proper* subgroups of A_n, which are described in the structure theorem above. The groups of type (a) and (b) are imprimitive, while types (c)-(f) are primitive. None of the imprimitive groups are contained in A_n, so their indices in S_n are as follows:

$$[S_n : \mathcal{E} \cap A_n] = \begin{cases} 2 \cdot \binom{n}{k} & \text{if } \mathcal{E} = S_m \times S_k \\ 2 \cdot \frac{n!}{j!^{n/j}(n/j)!} & \text{if } \mathcal{E} = S_j \wr S_{n/j}. \end{cases}$$

Proposition 5.2. *Let $n \geq 6$ be an even integer and $\mathcal{E}$ a maximal proper subgroup of A_n. Then the genus of X_E is greater than 1.*

Proof. As in the proof of Proposition 5.1 we split the proof into three cases according to the structure of $\mathcal{E}$.

Case 1 – imprimitive wreath products

In this case we require $n \geq 4$ and take $\mathcal{E} = (S_j \wr S_{n/j}) \cap A_n$, so that $[S_n : \mathcal{E}] = \dfrac{2 \cdot n!}{j!^{n/j}(n/j)!}$. The subgroup $S_j \wr S_{n/j}$ of S_n contains no n or $(n-1)$-cycles so that $c_1(\nu) = 0$ for all $\nu \in V$. Hence $g(X_E) > 1$.

Case 2 – intransitive subgroups

Here we take $n \geq 4$ (recall n is even) and consider the subgroups $\mathcal{E} = (S_j \times S_{n-j}) \cap A_n$. None of the $\mathcal{E}$ contain an n-cycle, and only $S_1 \times S_{n-1}$ contains an $(n-1)$-cycle. When $j = 1$ we have $\mathcal{E} = (S_1 \times S_{n-1}) \cap A_n \simeq A_{n-1}$. The order of A_{n-1} is $(n-1)!/2$ and it contains $(n-2)!$ $(n-1)$-cycles. Altogether this gives:

$$\begin{aligned} g(X_E) &\geq 1 + \frac{1}{6}\frac{2 \cdot n!}{(n-1)!} - \frac{1}{2}\left(0 + 0 + 2\left(1 - \frac{1}{n}\right)\left(\frac{2(n-2)!}{(n-1)!} \cdot (n-1) \cdot 1!\right)\right) \\ &= 2n - 1 + \frac{2}{n}, \end{aligned}$$

which is greater than 1.

Case 3 – primitive subgroups

If $\mathcal{E}$ is a primitive subgroup of A_n, then it is automatically a primitive subgroup of S_n, and hence is contained in some maximal primitive subgroup of S_n. All the maximal primitive subgroups of S_n (other than A_n) have been analyzed in Proposition 5.1. Moreover, before the proof of this proposition we noted that it suffices to consider the maximal *proper* subgroups of A_n, so we need not estimate the genus of the fixed-field coming from A_n itself. This completes the proof. □

References

[1] S. Ahlgren, K. Ono, *Arithmetic of singular moduli and class polynomials.* Compos. Math. **141** (2005), 283–312.

[2] J. Brillhart, P. Morton, *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial.* J. Number Theory. **106** (2004), 79–111.

[3] R. Coleman, *On the Galois groups of the exponential Taylor polynomials.* L'Enseignement Math. **33** (1987), 183–189.

[4] J.D. Dixon, B. Mortimer, *Permutation Groups.* Springer-Verlag, 1996.

[5] F. Hajir, *Algebraic properties of a family of generalized Laguerre polynomials.* To appear in Canad. J. Math.

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

[7] F. Hajir, S. Wong, *Specializations of one-parameter families of polynomials.* Annales de L'Institut Fourier. **56** (2006), 1127-1163.

[8] M. Hindry, J. Silverman, *Diophantine Geometry, An Introduction.* Springer-Verlag, 2000.

[9] M. Kaneko, D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials.* In Computational perspectives on number theory. AMS/IP Stud. Adv. Math. **7** (1998), 97–126.

[10] M. Liebeck, C. Praeger, J. Saxl, *A classification of the maximal subgroups of the finite alternating and symmetric groups.* J. Algebra **111** (1987), no. 2, 365–383.

[11] K. Mahlburg, K. Ono, *Arithmetic of certain hypergeometric modular forms.* Acta Arith. **113** (2004), 39–55.

[12] P. Müller, *Finiteness results for Hilbert's irreducibility theorem.* Ann. Inst. Fourier **52** (2002), 983–1015.

[13] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermitschen Polynome.* Gesammelte Abhandlungen. Band III, 227–233, Springer, 1973.

[14] I. Schur. Gessammelte Abhandlungen Vol. **3**, Springer, 1973

[15] E. Sell, *On a family of generalized Laguerre polynomials.* J. Number Theory **107** (2004), 266–281.

[16] G. Szegö, *Orthogonal Polynomials*, 4th ed. Providence, RI: Amer. Math. Soc., 1975.

[17] S. Wong, *On the genus of generalized Laguerre polynomials.* J. Algebra. **288** (2005), no. 2, 392–399.

John Cullinan
Department of Mathematics
Bard College
Annandale-On-Hudson, NY 12504
E-mail: cullinan@bard.edu
URL: http://math.bard.edu/cullinan

Farshid Hajir
Department of Mathematics
University of Massachusetts
Amherst MA 01003
E-mail: hajir@math.umass.edu

Elizabeth Sell
Department of Mathematics
Millersville University
P.O. Box 1002
Millersville, PA 17551
E-mail: liz.sell@millersville.edu