2006

Specializations of one-parameter families of polynomials

F Hajir
University of Massachusetts - Amherst, hajir@math.umass.edu

S Wong

SPECIALIZATIONS OF ONE-PARAMETER FAMILIES OF POLYNOMIALS

FARSHID HAJIR AND SIMAN WONG

Abstract. Let K be a number field, and let $\lambda(x,t) \in K[x,t]$ be irreducible over $K(t)$. Using algebraic geometry and group theory, we study the set of $\alpha \in K$ for which the specialized polynomial $\lambda(x,\alpha)$ is K-reducible. We apply this to show that for any fixed $n \geq 10$ and for any number field K, all but finitely many K-specializations of the degree n generalized Laguerre polynomial $L_n^{(t)}(x)$ are K-irreducible and have Galois group S_n. In conjunction with the theory of complex multiplication, we also show that for any K and for any $n \geq 53$, all but finitely many of the K-specializations of the modular equation $\Phi_n(x,t)$ are K-irreducible and have Galois group containing $PSL_2(\mathbf{Z}/n)$.

Contents

1. Introduction

Let K be a number field. Consider a polynomial $\lambda(x,t) \in K[x,t]$ which is non-constant in each of x and t; it can be viewed as a one-parameter family of K-polynomials in x. If λ is irreducible in $K[x,t]$, the Hilbert irreducibility theorem furnishes infinitely many $\alpha \in K$ for which $\lambda(x,\alpha)$ is K-irreducible. It is then natural to study the set of $\alpha \in K$ with reducible specialization. These exceptional sets are thin sets [29, §9.6], and the example $x^n - t$ shows that they can be infinite. Using techniques from diophantine analysis, Fried [10] bounded

1991 *Mathematics Subject Classification.* Primary 12H25; Secondary 11C08, 11G15,11R09, 14H25, 33C45.
Key words and phrases. Branched cover, complex multiplication, Hilbert irreducibility, modular equation, orthogonal polynomial, rational point, Riemann-Hurwitz formula, simple cover, specialization.
Hajir's research is supported in part by NSF Grant No. 0226869.

the number of exceptional specializations of bounded height. Exceptional sets for concrete families have also been examined; for example the irreducibility and Galois group of the Generalized Laguerre polynomial

$$L_n^{(t)}(x) = \sum_{j=0}^{n} (-x)^j \binom{n}{j} \prod_{k=j+1}^{n} (t+k). \tag{1}$$

for various rational values of the parameter t were studied by Schur ([26], [27]); more recently, Feit [9] used them to solve the inverse Galois problem over $\mathbf{Q}$ for certain double covers of the alternating group A_n. See also [14], [15], [28], [16], for other related results. Note that in the papers just cited, the focus is primarily on a related, but different, question from the one we began with, namely that of irreducibility and Galois properties of $L_n^{(\alpha_n)}(x)$ for suitable sequences $\{\alpha_n\}_n$. For example, the case $\alpha_n = -1-n$ corresponds to the truncated exponential polynomial studied by Schur [26]. For the latter type of question, the p-adic Newton polygon is a powerful tool. For example, in Filaseta-Lam [13] it is shown that if we fix $\alpha \in \mathbf{Q} - \mathbf{Z}_{<0}$, then $L_n^{(\alpha)}(x)$ is $\mathbf{Q}$-irreducible for n sufficiently large, while in Filaseta-Trifonov [12], Grosswald's conjecture, to the effect that $L_n^{(-1-2n)}(x)$ (i.e. the n-th degree Bessel polynomial) is $\mathbf{Q}$-irreducible for every n, is proved. The Newton Polygon approach, however, does not appear to be well-suited to the problem under consideration here, namely that of studying exceptional specializations of $L_n^{(t)}(x)$ for n *fixed*.

In this paper we investigate the exceptional set of a given $\lambda(x,t)$ from the algebro-geometric and group-theoretic points of view. First, note that $\lambda(x,t)$ defines a 1-dimensional subvariety $X_\lambda \subset \mathbf{P}^2_K$. To say that the specialization of λ at $t=\alpha$ has a K-rational root is to say that the fiber above α of the projection-to-t map has a K-rational point. Say X_λ is in fact absolutely irreducible; then, by Faltings, at most finitely many K-specializations of λ have a K-rational root if X_λ has genus ≥ 2. More generally, a result of Müller [23] leads to an irreducibility criterion for specializations in terms of the genus of intermediate subfields of $K'/K(t)$ where K' is the Galois closure of $\lambda(x,t)$ over the function field $K(t)$ (cf. also the related results of Dèbes and Fried [6]). In sections 2–5, we develop and refine tools for applying this criterion. In section 6, we apply these to study $L_n^{(t)}(x)$. The recursive properties of $L_n^{(t)}(x)$ allow us to analyze the geometry of the corresponding curve as well as the ramification behavior of the projection-to-t map. By utilizing, in addition, information about maximal subgroups of the symmetric group S_n, we obtain the following result.

Theorem 1. *Let K be a number field.*

(a) *Fix $n \geq 5$. Then for all but finitely many $\alpha \in K$, $L_n^{(\alpha)}(x)$ is K-irreducible and its Galois group (over K) contains A_n. For fixed $n \geq 10$, this Galois group is exactly S_n except for finitely many $\alpha \in K$.*

(b) *Let R be a finitely generated subring of K. If $n \geq 6$, then for all but finitely many $\alpha \in R$, the Galois group over K of $L_n^{(\alpha)}(x)$ is exactly S_n.*

Remark 1. Note that Theorem 1 is optimal in two ways. First, for $6 \leq n \leq 9$, the set of $\alpha \in K$ for which the discriminant of $L_n^{(\alpha)}(x)$ is a square in K turns out to be parameterized by a curve of geometric genus one, so for suitable K there are infinitely many specializations with even Galois group. And when $n = 5$, the square discriminants are parameterized by a curve of geometric genus zero, so there are fields K and finitely generated subrings R of K over which there are infinitely many even specializations. Second, $L_4^{(t)}(x) = 0$ is a model (cf. [16]) of the elliptic curve $384H2$ in Cremona's table. This curve has Mordell-Weil rank 1 over $\mathbf{Q}$, so over any number field K there are infinitely many $\alpha \in K$ for which $L_4^{(\alpha)}(x)$ has a K-rational linear factor. However, the exceptional set in Theorem 1 is captured by rational points on curves of high geometric genus, so it would be difficult to make the Theorem *effective*.

Before we develop the tools necessary for proving Theorem refthm:irr, we illustrate the use of Müller's criterion by applying it to another well-studied polynomial, namely the modular polynomial $\Phi_n(x, j)$. This monic $\mathbf{Z}$-polynomial plays a central role in the theory of elliptic curves; it is determined up to a scalar multiple by the property that two elliptic curves over $\mathbf{C}$ with j-invariants j_1, j_2 are related by a cyclic n-isogeny if and only if $\Phi_n(j_1, j_2) = 0$. It is irreducible over $\mathbf{C}(j)$, and its Galois group over $\mathbf{Q}(j)$ is $PGL_2(\mathbf{Z}/n)$.

For any integer $n > 1$ and any prime p, define

$$\mathbf{Q}_{p,n} = \begin{cases} \text{unique quadratic extension of } \mathbf{Q} \text{ of conductor } p & \text{if } p > 2 \text{ and } p|n, \\ \text{unique biquadratic extension of } \mathbf{Q} \text{ of conductor } 8 & \text{if } p = 2 \text{ and } 8|n, \\ \text{unique quadratic extension of } \mathbf{Q} \text{ of conductor } 4 & \text{if } p = 2 \text{ and } 4||n, \\ \mathbf{Q} & \text{otherwise.} \end{cases}$$

For any number field K and any $n > 1$, denote by $\tilde{K}_n$ the compositum of K with all $\mathbf{Q}_{p,n}$ as p runs over the prime divisors of n; note that this is a finite extension of K.

Theorem 2. *Let $n \geq 53$, and let K be a number field. Then for all but finitely many $\alpha \in \tilde{K}_n$, $\Phi_n(x, \alpha)$ is K-irreducible, and its Galois group over $\tilde{K}_n$ is $PSL_2(\mathbf{Z}/n)$. If n is a prime then it suffices to take $n \geq 23$.*

Remark 2. Theorem 2 is close to optimal in the n-aspect; cf. Remark 3. However, as in the discussion following Theorem 1, it would be difficult to make Theorem 2 effective.

We will describe our strategy via Müller's criterion in section 2, after we establish some notation. To apply this criterion to specializations of Φ_n, in section 3 we investigate the algebraic closure of $\mathbf{Q}$ in the function field defined by Φ_n, and we study the genus of Riemann surfaces defined by congruence subgroups. In sections 4 and 5, we develop the technical tools needed for carrying out the strategy outlined in section 2. In section 6, we implement this plan for the Generalized Laguerre Polynomial after first establishing several geometric properties of the projective plane curve $\mathcal{L}_n$ defined by $L_n^{(t)}(x) = 0$. Specifically, let $\iota_n : \mathcal{L}_n \to \mathbf{P}^1_K$ be the branched cover defined by the projection-to-t map. Then

(i) K is algebraically closed in the splitting field of $L_n^{(t)}$ over $K(t)$;
(ii) the (geometric) Galois group of ι_n is S_n;
(iii) $L_n^{(t)}(x)$, as a polynomial in x, has discriminant which is non-constant in t;
(iv) $\mathcal{L}_n$ has no affine singular points, and
(v) ι_n has several "simple" branch points of index close to n.

In (v), a *simple branch point of index e* is one whose fiber consists of a number (possibly 0) of multiplicity one points together with a single ramified point (of multiplicity e). The cover defined by the degree n Generalized Laguerre Polynomial has one simple branch point of every index between 2 and n: we use the four of highest index, which suffices in our analysis for all $n \geq 6$. As the calculations in section 6 will show, the proof of Theorem 1 extends readily to other one-parameter families of polynomials satisfying properties (i)-(v) (as long as their degree is large with respect to the precise form taken by condition (v)). On the other hand, given an arbitrary $\lambda(x,t)$ which is irreducible over $K(t)$, in general we cannot expect all but finitely many of its K-specializations to be K-irreducible, let alone having the same Galois group as $\lambda(x,t)$ over $K(t)$ — the subvariety X_λ mentioned just before the statement of Theorem 1 could, for example, have genus ≤ 1. In section 7 we will analyze this situation further in the case of "simple branched covers," i.e. where all the branch points are simple of index 2.

2. Rational specializations

We first establish some notation and hypotheses which will be maintained throughout. Let K be a field of characteristic 0, finitely generated over $\mathbf{Q}$. Fix an algebraic closure $\overline{K}$ of K. Denote by K_0 the function field $K(t)$. Fix $\lambda(x,t) \in K[x,t]$ so that λ has degree $n > 0$ in x and is irreducible over K_0. Then $K_1 := K[x]/(\lambda(x,t))$ is a degree n extension of K_0. Let K'/K_0 be a Galois closure of K_1/K_0, and write $G_\lambda = \mathrm{Gal}(K'/K_0)$. By [29, p. 123], the Galois group of $\lambda(x,\alpha)$ over K is a subgroup of G_λ for any $\alpha \in K$, and by [29, Prop. 9.2], there are infinitely many $\beta_0 \in K$ for which this Galois group is exactly G_λ.

From now on, suppose that

(i) K is algebraically closed in K'/K_0.

Then [31, Remark II.2.5] implies that every intermediate subfield E of K'/K_0 is the function field of a smooth projective curve X_E over K, and if $E \subset E'$ are two such subfields, then there exists a K-morphism $X_{E'} \to X_E$ of degree $[E' : E]$. We write $g(X_E)$ for the genus of X_E. By Galois theory, intermediate fields E of K'/K_0 are in bijective correspondence with subgroups $\mathcal{E} = \mathrm{Gal}(K'/E)$ of G_λ. To simplify the exposition, we abbreviate the phrase 'all but finitely many $\alpha \in K$' by $\alpha \in_{\mathrm{af}} K$.

Proposition 1. *Let K'/K_0 be as above, and consider a polynomial $f \in K[x,t]$ which is irreducible over K_0 but splits completely into linear factors over K'. Suppose for every intermediate subfield E of K'/K_0 such that f is reducible over E, we have $g(X_E) > 1$. Then $f(x,\alpha)$ is K-irreducible for $\alpha \in_{af} K$.*

Proof. This is probably well-known to the expert; for a convenient reference see Müller [23, Prop. 4.20]. A method of proof is also indicated in 5.2. □

For any $\alpha \in K$, the Galois group of $\lambda(x,\alpha)$ over K is a subgroup of G_λ, and we are interested in finding conditions on α under which $\lambda(x,\alpha)$ is not only K-irreducible, but also has Galois group coinciding with the full G_λ. Here is our strategy: suppose the splitting field of some "test-polynomial" $f(x,t) \in K[x,t]$ is contained in K'; then the splitting field of $f(x,\alpha)$ over K is contained in that of $\lambda(x,\alpha)$. So if $f(x,\alpha)$ is K-irreducible, then the degree of the splitting field of $\lambda(x,\alpha)$ over K would be divisible by the degree of $f(x,\alpha)$. By running through an appropriate collection of f (e.g. the polynomials Λ_j introduced in 5), we can then hope to show that $\#G_\lambda$ divides the degree of the splitting field of $\lambda(x,\alpha)$ over K, whence the Galois group of $\lambda(x,\alpha)$ over K must be G_λ. To study the irreducibility of the specializations $f(x,\alpha)$ we use Proposition 1, which reduces the problem to estimating the genus of X_E as we run through intermediate subfields E of K'/K_0.

3. Modular equations

By [20, p. 55], the modular polynomial $\Phi_n(x,j) \in \mathbf{Z}[x,j]$ is irreducible over $\mathbf{C}(j)$. We now apply the strategy developed in the last section to study specializations of Φ_n. Denote by L_n the splitting field of Φ_n over $\mathbf{Q}(t)$. Recall the definition of $\mathbf{Q}_{p,n}$ and $\tilde{K}_n$ immediately preceding the statement of Theorem 2.

Lemma 1. *The algebraic closure of* $\mathbf{Q}$ *in* $L_n/\mathbf{Q}(t)$ *is* $\tilde{\mathbf{Q}}_n$.

Proof. As a coarse moduli scheme, the open modular curve $Y_0(n)$ classifies isomorphism classes $(E \to E')$ of pairs of elliptic curves related via a cyclic n-isogeny. Over the complex numbers, such a pair is completely determined by the j-invariants of E and E'. Thus the *complex* points of $Y_0(n)$ are canonically identified with the *complex* points of the affine plane curve defined by $\Phi_n(x,j)=0$. Under this identification, the projection-to-j map from this complex plane curve corresponds precisely to the branched cover $\pi_0(n): Y_0(n) \to Y_0(1)$ coming from the inclusion $\Gamma_0(n) \subset SL_2(\mathbf{Z})$. The smallest regular branched cover containing $\pi_0(n)$ is then the cover $\pi(n): Y(n) \to Y(1) = Y_0(1)$ corresponding to the inclusion $\Gamma(n) \subset SL_2(\mathbf{Z})$. In particular, the deck transformation group of $\pi(n)$ is

$$PSL_2(\mathbf{Z})/(\Gamma(n)/\pm I) \simeq PSL_2(\mathbf{Z}/n).$$

It follows that the *geometric* Galois group of Φ_n is $PSL_2(\mathbf{Z}/n)$. But Macbeath [22] showed that $\mathrm{Gal}(L_n/\mathbf{Q}(t)) \simeq PGL_2(\mathbf{Z}/n)$, so the algebraic closure of $\mathbf{Q}$ in $L_n/\mathbf{Q}(t)$ is the compositum of $\mathbf{Q}(t)$ with a Galois extension $L(n)/\mathbf{Q}$ with Galois group

$$\begin{aligned} PGL_2(\mathbf{Z}/n)/PSL_2(\mathbf{Z}/n) &\simeq \prod_{p|n} PGL_2(\mathbf{Z}/p^{e_p})/PSL_2(\mathbf{Z}/p^{e_p}) \qquad \text{where } p^{e_p}||n \\ &\simeq \prod_{\substack{p|n\\ p>2}} (\mathbf{Z}/2) \times \left\{ \begin{array}{ll} \mathbf{Z}/2 \times \mathbf{Z}/2 & \text{if } 8|n \\ \mathbf{Z}/2 & \text{if } 4||n \\ \{1\} & \text{otherwise} \end{array} \right\}. \end{aligned} \tag{2}$$

If $m|n$ then $L_m \subset L_n$, hence $L(m) \subset L(n)$, so to prove the Lemma we are reduced to showing that for any prime power $p^e > 1$,

$$L(p^e) = \mathbf{Q}_{p,p^e}. \tag{3}$$

For any $\alpha \in \mathbf{Q}$ and any $n > 1$, the splitting field of $\Phi_n(x,\alpha)$ over $\mathbf{Q}$ also contains $L(n)$. Take $\alpha \in \mathbf{Q}$ to be one of the thirteen j-invariants over $\mathbf{Q}$ corresponding to CM elliptic curves over $\mathbf{Q}$, say $\alpha = j(\tau)$. Denote by $k_\alpha/\mathbf{Q}$ the corresponding complex quadratic field. By the 'First Main Theorem' of complex multiplication [4, Thm. 11.1], $k_\alpha(j(n\tau))$ is the ring class field of k_α of conductor n, hence $L(n) \subset k_\alpha(j(n\tau))$. In particular, $L(n)/\mathbf{Q}$ is unramified outside of the prime divisors of n and of the discriminant of $k_\alpha/\mathbf{Q}$. If $j(\tau') = \alpha' \in \mathbf{Q}$ is another CM j-invariant over $\mathbf{Q}$, then $L(n) \subset k_\alpha(j(n\tau)) \cap k'_\alpha(j(n\tau'))$. We may choose α' so that k_α and k'_α have coprime discriminants, whereby $L(p^e)/\mathbf{Q}$ is unramified outside p. On the other hand, (2) says that $L(p^e)/\mathbf{Q}$ is quadratic if $p > 2$ or $p^e = 4$, and that it is biquadratic if $8|p^e$. Recalling the definition of $\mathbf{Q}_{p,n}$, we get (3) except when $p^e = 4$. To treat this remaining case we actually need to determine these ring class fields.

Set $\omega = \frac{1+\sqrt{-7}}{2}$, and take $\alpha = j(\omega) \in \mathbf{Q}$, so $k_\alpha = \mathbf{Q}(\omega)$. The conductor of the extension $k_\alpha(\sqrt{-1})/k_\alpha$ clearly divides $4\mathbf{Z}[\omega]$. On the other hand, by [4, Thm. 7.24] the ring class field of k_α of conductor $4\mathbf{Z}[\omega]$ is a quadratic extension of k_α, so this ring class field is precisely $k_\alpha(\sqrt{-1})$. Recalling (2), we see that $L(4)/\mathbf{Q}$ is a quadratic extension in $\mathbf{Q}(\omega, \sqrt{-1})$ unramified outside 2, and (3) follows for $p^e = 4$. □

Rademacher conjectured that there are only finitely many congruence subgroups with corresponding modular curve of genus zero (cf. [19]). Dennin [18] proved the stronger result that for any integer g, there are at most finitely many n for which $PSL_2(\mathbf{Z}/n)$ contains a subgroup of genus $\leq g$. Cummins and Pauli [5] recently tabulated all such subgroups for $g \leq 24$, from which we deduce the following result.

Lemma 2 (Cummins-Pauli)**.** *If $n \geq 53$, then every proper subgroup of $PSL_2(\mathbf{Z}/n)$ has genus ≥ 2. If n is a prime, the same conclusion holds for $n \geq 23$.* □

Proof of Theorem 2. Thanks to Lemma 1, the discussion in section 2 is applicable to Φ_n over $\tilde{K}_n$ for any number field K.

Let π_n be a primitive element for the extension $\tilde{K}_n L_n(t)/\tilde{K}_n(t)$, and let $f_n(x,t)$ be the minimal polynomial of π_n over $\tilde{K}_n(t)$. Then f_n is irreducible over $\tilde{K}_n(t)$, by construction. So if n is as in Lemma 2, then Proposition 1 and this Lemma together imply that for $\alpha \in_{\mathrm{af}} \tilde{K}_n$, the specializations of f_n and of Φ_n at $t = \alpha$ are both $\tilde{K}_n$-irreducible. If we write $F_n(\alpha)$ for the splitting field of $\Phi_n(x,\alpha)$ over $\tilde{K}_n$, then that means $[F_n(\alpha) : \tilde{K}_n]$ is divisible by $\deg f_n = [\tilde{K}_n L_n(t) : \tilde{K}_n(t)] = \#PSL_2(\mathbf{Z}/n)$, and Theorem 2 follows. □

Remark 3. The fact that *every* non-trivial intermediate subfield of $\tilde{K}_n L_n(t)/\tilde{K}_n(t)$ has genus ≥ 2 for $n \geq 53$ significantly simplifies our search for the 'test polynomial' f in Proposition 1. The modular curve $X_0(n)$ has genus ≤ 1 for $n \leq 21$ and for $n \in \{24, 25, 27, 32, 36, 49\}$, so by the discussion immediately preceding Theorem 1, for these n the modular equation has infinitely many reducible specializations over suitable K. To analyze the remaining values of $n \leq 52$ we could search for test polynomials f which remain irreducible over intermediate subfields of genus ≤ 1. We will not pursue this issue here, but in section 5 we will study the same problem for specializations of S_n-extensions by using a family of $[(n-1)/2]$ test polynomials $\Lambda_j(x,t)$.

4. A Riemann-Hurwitz estimate

We now return to the general setup in section 2. To apply Proposition 1, we need to be able to estimate the genus of certain intermediate subfields of K'/K_0. To do that we will apply the Riemann-Hurwitz formula to the cover $\xi_E : X_E \to \mathbf{P}^1_K$ corresponding to the field inclusion $K_0 \subset E$. Since we do not have any explicit model for X_E, we will take an algebraic approach. Thanks to hypothesis (i) in section 2, in order to determine the ramification of the *geometric* cover $X' \to \mathbf{P}^1_K$ it suffices to determine the *algebraic* ramification behavior of integral extensions of Dedekind domains corresponding to this geometric cover.

Denote by $B_\lambda \subset \mathbf{P}^1_K$ the branch locus of the projection-to-t map for λ. Then ξ_E is unramified outside B_λ. Fix affine open sets on X_E and X' which contain every fiber of ξ_E and $X' \to \mathbf{P}^1_K$ above B_λ, and denote by $\mathcal{O}_E$ and $\mathcal{O}'$ their respective affine coordinate rings. Write $\mathcal{O}_0$ for the affine coordinate ring of the affine line in $\mathbf{P}^1_K$. Let $\mathfrak{m}_\nu$ (or just $\mathfrak{m}$ if ν is fixed) be the maximal ideal in $\mathcal{O}_0$ corresponding to a given $\nu \in B_\lambda$. We let $e_\nu = e(\mathfrak{M}/\mathfrak{m})$ be the ramification index of $\mathfrak{M}$ in the Galois cover K'/K_0, where $\mathfrak{M}$ is an arbitrary prime of $\mathcal{O}'$ dividing $\mathfrak{m}\mathcal{O}'$.

Definition 1. (a) *For a positive integer δ and a branch point $\nu \in B_\lambda$ corresponding to an ideal $\mathfrak{m} \in \mathcal{O}_0$, let*

$$c_\delta(\nu) = c_\delta(\mathfrak{m}) = \sum_{\substack{\mathfrak{n} | \mathfrak{m}\mathcal{O}_E \\ e(\mathfrak{n}/\mathfrak{m}) = \delta}} f(\mathfrak{n}/\mathfrak{m}),$$

be the sum of the residual degrees of distinct $\mathcal{O}_E$-primes $\mathfrak{n}$ of ramification index δ over $\mathfrak{m}$.

(b) *For $\nu \in B_\lambda$ corresponding to an ideal $\mathfrak{m} \in \mathcal{O}_0$, let*

$$\Delta(\nu) = \Delta(\mathfrak{m}) = \sum_{\mathfrak{n} | \mathfrak{m}\mathcal{O}_E} (e(\mathfrak{n}/\mathfrak{m}) - 1) f(\mathfrak{n}/\mathfrak{m})$$

be the ν-component of the discriminant of E/K_0.

(c) *For an integer $e > 1$, let $d(e)$ be the least prime divisor of e.*

Lemma 3. *With the notation and hypotheses as in section 2, if E is an intermediate field of K'/K_0 corresponding to a subgroup $\mathcal{E} = \mathrm{Gal}(K'/E)$ of $G_\lambda = \mathrm{Gal}(K'/K_0)$, and V is any subset of B_λ, then*

$$g(X_E) \geq 1 + \frac{[G:\mathcal{E}]}{2}\Big(-2 + \sum_{\nu \in V}\Big(1 - \frac{1}{d(e_\nu)}\Big)\Big) - \frac{1}{2}\sum_{\nu \in V} c_1(\nu)\Big(1 - \frac{1}{d(e_\nu)}\Big). \tag{4}$$

Proof. First, note that

$$\sum_{1 \leq \delta | e_\nu} c_\delta(\nu)\delta = [E:K_0] = [G_\lambda : \mathcal{E}]. \tag{5}$$

For each $\nu \in B_\lambda$, we have from Definition 1,

$$\begin{aligned}
\Delta(\nu) &= \sum_{1\le\delta|e_\nu} c_\delta(\nu)(\delta-1)\\
&= \sum_{1<\delta|e_\nu} c_\delta(\nu)\Big(1-\frac{1}{\delta}\Big)\delta\\
&\ge \Big(1-\frac{1}{d(e_\nu)}\Big)\sum_{1<\delta|e_\nu} c_\delta(\nu)\delta\\
&\ge \Big(1-\frac{1}{d(e_\nu)}\Big)\sum_{1\le\delta|e_\nu} c_\delta(\nu)\delta - \Big(1-\frac{1}{d(e_\nu)}\Big)c_1(\nu)\\
&\ge [G_\lambda:\mathcal{E}]\Big(1-\frac{1}{d(e_\nu)}\Big) - c_1(\nu)\Big(1-\frac{1}{d(e_\nu)}\Big) \qquad \text{by (5).} \qquad (6)
\end{aligned}$$

By Riemann-Hurwitz for E/K_0, [24, Theorem 7.16], we have

$$g(X_E)-1 = [E:K_0](0-1)+\frac{1}{2}\sum_{\nu\in B_\lambda}\Delta(\nu).$$

Since $\Delta(\nu)>0$, we have, for any subset $V\subseteq B_\lambda$,

$$\begin{aligned}
g(X_E) &\ge 1-[G_\lambda:\mathcal{E}]+\frac{1}{2}\sum_{\nu\in V}\Delta_\nu\\
&\ge 1+\frac{[G_\lambda:\mathcal{E}]}{2}\Big(-2+\sum_{\nu\in V}\Big(1-\frac{1}{d(e_\nu)}\Big)\Big)-\frac{1}{2}\sum_{\nu\in V}c_1(\nu)\Big(1-\frac{1}{d(e_\nu)}\Big) \quad \text{by (6).}
\end{aligned}$$

□

Remark 4. Note that the bound (4) is useful only when $c_1(\nu)$ is fairly small for all $\nu \in V$, so in using (4), it's often useful to take V to be a proper subset of B_λ. Moreover, the inequality (4) is in fact strict if V is a *proper* subset of B_λ since $\Delta(\nu)>0$ for $\nu\in V$.

In view of Proposition 1, our task will be to show that the right hand side of (4) is >1 when a given $f(x,t)\in K[x,t]$ is reducible over E. For our application to Generalized Laguerre Polynomials, this will be easy to arrange by taking V to be an appropriately small subset of B_λ.

We now turn to the task of bounding $c_1 = c_1(\nu)$ from above, where, for the remainder of this section, $\nu\in B_\lambda$ is a fixed branch point, with corresponding ideal $\mathfrak{m}=\mathfrak{m}_\nu$ of $\mathcal{O}_0$. Fix also a prime $\mathfrak{M}\subset\mathcal{O}'$ lying over $\mathfrak{m}$, with corresponding decomposition group $D=\{\sigma\in G : \mathfrak{M}^\sigma=\mathfrak{M}\}$, and inertia group $I=I(\mathfrak{M}/\mathfrak{m})$. Let T be a subset of $G=G_\lambda=\mathrm{Gal}(K'/K_0)$ such that

$$G=\coprod_{\tau\in T}\mathcal{E}\tau D \qquad (7)$$

is the decomposition of G into disjoint double cosets, where $\mathcal{E}=\mathrm{Gal}(K'/E)$ is the subgroup fixing E.

As is clear from Lemma 3, it will be important to keep track of the primes $\mathfrak{n}$ of $\mathcal{O}_E$ dividing $\mathfrak{m}$ and especially their ramification indices $e(\mathfrak{n}/\mathfrak{m})$. That these can be described nicely in terms of the double coset decomposition (7) is a useful fact (we learned from Tate) for which we were not able to find a suitable reference, so we give the details. For each $\sigma \in G$, let $\mathfrak{n}_\sigma$ be the prime $\mathfrak{M}^\sigma \cap \mathcal{O}_E$ of $\mathcal{O}_E$ lying under $\mathfrak{M}^\sigma$. Let $I_\sigma \subseteq D_\sigma$ be the inertia and decomposition groups of $\mathfrak{M}^\sigma/\mathfrak{m}$, respectively. They satisfy $D_\sigma = \sigma D \sigma^{-1}$ and $I_\sigma = \sigma I \sigma^{-1}$. In the extension K'/E, the inertia and decomposition groups for $\mathfrak{M}^\sigma/\mathfrak{n}_\sigma$ are simply $I_\sigma \cap \mathcal{E}$ and $D_\sigma \cap \mathcal{E}$, respectively. For the ramification indices of $\mathfrak{M}/\mathfrak{m}, \mathfrak{M}/\mathfrak{n}_\sigma$, and $\mathfrak{n}_\sigma/\mathfrak{m}$, let us put

$$e = e(\mathfrak{M}/\mathfrak{m}), \qquad e'_\sigma = e(\mathfrak{M}/\mathfrak{n}_\sigma), \qquad e_\sigma = e(\mathfrak{n}_\sigma/\mathfrak{m}),$$

and similarly for the residual degrees, we put

$$f = f(\mathfrak{M}/\mathfrak{m}), \qquad f'_\sigma = f(\mathfrak{M}/\mathfrak{n}_\sigma), \qquad f_\sigma = f(\mathfrak{n}_\sigma/\mathfrak{m}).$$

By multiplicativity in towers for these invariants, we have

$$e_\sigma e'_\sigma = e, \qquad f_\sigma f'_\sigma = f. \tag{8}$$

Lemma 4. *With the notation introduced above,*

(a) *The distinct primes of $\mathcal{O}_E$ dividing $\mathfrak{m}$ are those induced by $\mathfrak{M}^\tau$ for $\tau \in T$. In other words, we have $\mathfrak{n}_\sigma = \mathfrak{n}_{\sigma'}$ if and only if $\mathcal{E}\sigma D = \mathcal{E}\sigma' D$.*

(b) *For $\sigma \in G$, we have*

$$e_\sigma f_\sigma = [\sigma D \sigma^{-1} : \mathcal{E} \cap \sigma D \sigma^{-1}], \qquad e_\sigma = [\sigma I \sigma^{-1} : \mathcal{E} \cap \sigma I \sigma^{-1}].$$

Proof. Let w be the valuation of $\mathcal{O}'$ corresponding to $\mathfrak{M}$. For $\alpha \in \mathcal{O}'$, we have $|\alpha|_{\sigma w} = |\sigma^{-1}\alpha|_w$. If $\mathcal{E}\sigma D = \mathcal{E}\sigma' D$, we can write $\sigma' = h\sigma g$, with $h \in \mathcal{E}, g \in D$. For $\alpha \in \mathcal{O}_E$, we compute

$$|\alpha|_{\sigma' w} = |\alpha|_{h\sigma g w} = |\alpha|_{h\sigma w} = |h^{-1}\alpha|_{\sigma w} = |\alpha|_{\sigma w}.$$

Thus, σw and $\sigma' w$ induce the same valuation on $\mathcal{O}_E$, i.e. $\mathfrak{n}_\sigma = \mathfrak{n}_{\sigma'}$. Conversely, suppose $\mathfrak{n}_\sigma = \mathfrak{n}_{\sigma'}$, i.e. the set of primes of $\mathcal{O}'$ lying over $\mathfrak{n}_\sigma$ includes $\mathfrak{M}^{\sigma'}$ as well as $\mathfrak{M}^\sigma$. Since $\mathcal{E} = \mathrm{Gal}(K'/E)$ acts transitively on this set, there exists $h \in \mathcal{E}$ such that $\mathfrak{M}^{h\sigma'} = \mathfrak{M}^\sigma$, i.e. $\sigma^{-1}h\sigma' \in D$. Therefore, $\mathcal{E}\sigma D = \mathcal{E}\sigma' D$. This proves (a). We have $ef = \#I_\sigma f = \#D_\sigma$ and $e'_\sigma f'_\sigma = \#(I_\sigma \cap \mathcal{E}) f'_\sigma = \#(D_\sigma \cap \mathcal{E})$, so we get (b) by multiplicativity in towers (8). □

Define

$$Y = \{\sigma \in G : \sigma I \sigma^{-1} \subset \mathcal{E}\}.$$

For the application to Riemann-Hurwitz, we'll need to estimate c_1. We proceed as follows.

Lemma 5. *If $a \in Y$, then $\{b \in Y : \mathcal{E}aI = \mathcal{E}bI\} = \mathcal{E}a$. We have $c_1 = \#Y/\#\mathcal{E}$.*

Proof. We first make a remark that simplifies the calculation. Note that if we compose our fields $K_0 \subset E \subset K'$ with a finite extension $\tilde{K}$ of the constant field K that splits $\mathfrak{M}$, then $c_\delta(\mathfrak{m})$ remains unchanged, since each prime $\mathfrak{n}_\sigma$ of E of residual degree f_σ splits in $E\tilde{K}$ into f_σ primes of residual degree 1 with the same inertia group $I_\sigma \cap \mathcal{E}$. In fact, the genus calculation we are performing is a purely geometric one, so we could have simply assumed from the outset that the constant field K is algebraically closed.

Either way, we take $\mathfrak{M}/\mathfrak{m}$ as above and assume without loss of generality, that $f(\mathfrak{M}/\mathfrak{m}) = 1$, i.e. $I = D$.

By Lemma 4, for any $\sigma \in G$, $e(\mathfrak{n}_\sigma/\mathfrak{m}) = 1$ if and only if $\sigma I \sigma^{-1} \subset \mathcal{E}$. Thus

$$c_1 = \#\{\mathcal{E}\sigma I : \sigma I \sigma^{-1} \subset \mathcal{E}\}. \tag{9}$$

Note that $\mathcal{E}aI = \mathcal{E}bI$ if and only if $b \in \mathcal{E}aI$. Suppose $b \in Y$ and $b \in \mathcal{E}aI$. Then $ba^{-1} \in \mathcal{E}aIa^{-1} \subset \mathcal{E}$, hence $b \in \mathcal{E}a$. Conversely, suppose $b = ha$ with $h \in \mathcal{E}$. Then

$$bIb^{-1} = haIa^{-1}h^{-1} \subset h\mathcal{E}h^{-1} = \mathcal{E}$$

so $b \in Y$. Finally, clearly $\mathcal{E}a \subset \mathcal{E}aI$ so $b \in \mathcal{E}a$ implies $b \in \mathcal{E}aI$. Therefore, Y is a union of (right) cosets of $\mathcal{E}$, and the number of distinct double cosets $\mathcal{E}aI$ with $a \in Y$ is exactly $\#Y/\#\mathcal{E}$. This completes the proof by (9). □

Since we are working with function fields of characteristic 0, all ramification is tame, so the inertia group I is cyclic. We now specialize to the case where $G = S_n$, and I is generated by a *cycle* (under its natural action on the roots of λ). Of course, if $\#I$ is greater than $n/2$, the latter condition holds automatically.

Lemma 6. *If* $\mathrm{Gal}(K'/K_0) = S_n$ *and* I *is generated by an* m*-cycle, then*

$$c_1 = \frac{(\text{number of } m\text{-cycles in } \mathcal{E})}{\#\mathcal{E}} \times m(n-m)! \tag{10}$$

$$< m(n-m)!. \tag{11}$$

Proof. Just as in the proof of the preceding Lemma, we may assume that $I = D$. Let $J = \{sIs^{-1} \subset \mathcal{E} : s \in G\}$ be the set of subgroups of $\mathcal{E}$ which are G-conjugate to I. Then

$$\#Y = \sum_{I' \in J} \#\{s \in G : sI's^{-1} = I'\}. \tag{12}$$

Any two m-cycles in S_n are S_n-conjugate, so

$$\#J = \text{number of cyclic subgroups of } \mathcal{E} \text{ generated by an } m\text{-cycle} \tag{13}$$

$$= (\text{number of } m\text{-cycles in } \mathcal{E})/\varphi(m). \tag{14}$$

There are $n!/(m(n-m)!)$ m-cycles in S_n, so for any S_n-conjugate $I' \subset \mathcal{E}$ of I,

$$\#\{s \in S_n : sI's^{-1} = I'\} = \frac{n!}{\#\mathrm{orbit}_{S_n}(I')} = \frac{n!}{\frac{n!}{m(n-m)!}/\varphi(m)} = m\varphi(m)(n-m)!. \tag{15}$$

The proof is complete once we combine (12)-(15) with Lemma 5. □

We end this section with an elementary criterion which guarantees the hypothesis of Lemma 6 (on inertia being generated by a cycle) to hold; the criterion will be easily verified for the Generalized Laguerre Polynomial at all its branch points.

Recall that K_1/K_0 is a root field for λ, i.e. $K_1 \simeq K_0[x]/(\lambda)$.

Definition 2. *Let* $\nu \in B_\lambda$ *be a branch point of* λ*, with corresponding maximal ideal* $\mathfrak{m} \subset \mathcal{O}_0$*. Let* $e > 1$ *be an integer. We say that* ν *(or* $\mathfrak{m}$*) is* simple of index e *for* λ *if*

$$\mathfrak{m}\mathcal{O}_{K_1} = \mathfrak{n}_0^e \mathfrak{n}_1 \cdots \mathfrak{n}_s, \tag{16}$$

where $\mathfrak{n}_0, \ldots, \mathfrak{n}_s$ *are pairwise distinct primes of* $\mathcal{O}_{K_1}$*; in other words, in* $\mathcal{O}_{K_1}$*, there is a unique prime dividing* $\mathfrak{m}\mathcal{O}_{K_1}$ *with non-trivial ramification index (equal to* e*).*

Lemma 7. *Suppose* $G = \mathrm{Gal}(K'/K_0) = S_n$*. Let* $\mathfrak{m} \subset \mathcal{O}_0$ *be a maximal ideal corresponding to a branch point* $\nu \in B_\lambda$*, which is simple of index* $e > 1$*. Then, for any* $\mathfrak{M} \subset \mathcal{O}'$ *lying above* $\mathfrak{m}$*, the inertia group* $I = I(\mathfrak{M}/\mathfrak{m})$ *has order* e *and is generated by a cycle of length* e*.*

Proof. Let $\mathcal{E} = \mathrm{Gal}(K'/K_1)$. The index n subgroups in S_n are stabilizers of any one of the n letters. By reordering the roots if needed, we can identify $\mathcal{E} \simeq S_{n-1}$ with the stabilizer of the letter n. Every element in S_n is a product of disjoint, non-trivial cycles. This decomposition is unique once a labelling is fixed, and two elements in S_n are conjugate if and only if they decompose into the same number of cycles of each length.

Returning to the proof of the Lemma, suppose $\mathfrak{M}$ is a prime of $\mathcal{O}'$ whose restriction $\mathfrak{M} \cap \mathcal{O}_{K_1}$ is the unique prime $\mathfrak{n}$ of $\mathcal{O}_{K_1}$ of ramification index $e > 1$ over $\mathfrak{m}$. Let $I = I(\mathfrak{M}/\mathfrak{m})$. We may assume, as in the preceding lemmas, that composing with a suitable finite extension of K, $\mathfrak{M}/\mathfrak{m}$ has degree 1, i.e. $I = D$ (this disturbs neither the identification $G \simeq S_n$ nor the embedding $I \hookrightarrow G$).

Let γ be a generator of the cyclic group I. Write $\gamma = \gamma_1 \cdots \gamma_r$ for its decomposition into disjoint, possibly trivial, cycles. Since the γ_i pairwise commute, we may assume that the letter n occurs in the cycle γ_1. For $1 \leq i \leq r$, let $a_i = \mathrm{ord}(\gamma_i) \geq 1$, and let $a = \min\{m \geq 1 : \gamma^m \in \mathcal{E}\}$. On the one hand, γ^a generates $I \cap \mathcal{E}$, and, on the other hand, we have $a = a_1$ (recalling our convention that $\mathcal{E}$ is the stabilizer of the letter n). By Lemma 4, $e(\mathfrak{n}/\mathfrak{m}) = \#[I/(I \cap \mathcal{E})] = \#[\langle\gamma\rangle/\langle\gamma^a\rangle] = a$, thus γ_1 has order $a = a_1 = e > 1$, since we took $\mathfrak{n}$ to be the unique prime of ramification index $e > 1$ over $\mathfrak{m}$.

It remains to show that the cycles $\gamma_2, \ldots, \gamma_r$ are trivial, i.e. $a_i = 1$ for $i > 1$. We proceed by contradiction. If $a_2 > 1$, say, then, there exists $\sigma \in G$ such that $\sigma\gamma_2\sigma^{-1}$ is a cycle acting non-trivially on the letter n. Then, as before, $e(\mathfrak{n}_\sigma/\mathfrak{m}) = a_2 > 1$, so we get $a_2 = e$ and $\mathfrak{n}_\sigma = \mathfrak{n}$ by the assumption on the simplicity of the ramification. By Lemma 4, therefore, $\sigma \in \mathcal{E}I$, say $\sigma = \eta\theta$ with $\eta \in \mathcal{E}$ and $\theta \in I$. Letting $x' = \sigma x \sigma^{-1}$ for $x \in G$, we have $\gamma' = \gamma'_1\gamma'_2 \cdots \gamma'_r$ is the decomposition of γ' into disjoint cycles since conjugation preserves cycle structure. But we claim that γ'_1 and γ'_2 are not disjoint, as they both act non-trivially on the letter n. To see this, note that $\theta = \gamma^b$ for some integer b, so $\theta\gamma_i\theta^{-1} = \gamma_i$ for $i = 1, \ldots, r$. On the other hand, since $\eta \in \mathcal{E}$, it fixes n, so $\gamma'_1 = \eta\gamma_1\eta^{-1}$ and $\gamma'_2 = \eta\gamma_2\eta^{-1}$ are both e-cycles that act non-trivially on n, hence are not disjoint. This contradiction shows that $\gamma_2, \ldots, \gamma_r$ are all trivial, so $I = \langle\gamma_1\rangle$ is generated by an e-cycle, hence has order e. □

5. Specializations of S_n-covers

In this section, we develop a strategy for applying Proposition 1 to a geometric S_n-cover. Namely, starting with an S_n-extension of function fields K'/K_0 as in section 2, in subsection 5.1 we construct a family of polynomials $\Lambda_j(x,t) \in K[x,t]$ with splitting field contained in K' (to which we will later apply Proposition 1). In 5.2, we will give a geometric interpretation in terms of fiber products for the curves corresponding to these Λ_j which we need for controlling the genus of subfields of K' cut out by a subgroup contained in A_n. A reader who is interested in a proof of Theorem 1 for $n \geq 10$ only, can skip 5.2 entirely, as it will enter the proof only for $6 \leq n \leq 9$.

5.1. **Distinguished subfields in S_n-extensions.**

Let $\lambda(x,t)$ and K'/K_0 be as in section 2; in particular, recall the regularity hypothesis (i) introduced there. Suppose further that

(ii) $G_\lambda \simeq S_n$, and

(iii) λ, as a polynomial in x, has discriminant which is non-constant in t.

These two conditions actually recover the regularity of the cover, at least when n is not too small.

Lemma 8. *Suppose $n \geq 5$. Then*
(a) *K is algebraically closed in K'/K_0, and*
(b) *K'/K_0 has a unique Galois subfield. This subfield is quadratic over K_0.*

Proof. Fix an algebraic closure $\overline{K}$ of K. Then $\overline{K} \cap K'$ is a Galois subfield of the S_n-extension K'/K_0. Since $n \geq 5$, the only non-trivial Galois subfield in K'/K_0 is the unique quadratic subfield generated by the square-root of the discriminant (with respect to x) of $\lambda(x,t)$. Invoke the discriminant condition on λ and we are done. □

The following result is standard.

Lemma 9. *Let X/K be a smooth projective curve, and let $\xi : X \to \mathbf{P}^1_K$ be a non-constant K-morphism. Then X is K-birational to a plane curve $G(x,t) = 0$ such that ξ is the projection-to-t map.* □

We now describe a distinguished collection of subfields in K'/K_0. Fix a labelling of the roots of $\lambda(x,t)$ over K_0, giving an identification of G_λ with the symmetric group S_n. For $1 \leq j < n$, write $S_{n,j}$ for the subgroup $S_j \times S_{n-j} \subset S_n$, where S_j permutes the first j roots, and S_{n-j}, the remaining $n-j$ roots. Denote by

- K_j the subfield of K'/K_0 fixed by $S_{n,j}$,
- X_j the associated smooth projective curve over K, and
- $\tilde{\phi}_{n,j} : X_j \to \mathbf{P}^1_K$ the K-branched cover corresponding to the extension K_j/K_0.

Lemma 9 furnishes a K-birational map taking X_j to a plane curve $\Lambda_j(x,t) = 0$ which is smooth above $t = \beta_0$, and such that $\tilde{\phi}_{n,j}$ is the projection-to-t map. Clearly we can take $\Lambda_1 = \lambda$ and do so. Since X_j is smooth, it is absolutely irreducible, hence so is $\Lambda_j(x,t)$. Thus we can apply Proposition 1 to Λ_j.

Lemma 10. *Fix positive integers n, j satisfying $n \geq 5$ and $j \in [1, n/2]$. Suppose for every intermediate subfield E of K'/K_0 over which $\Lambda_j(x,t)$ is reducible, we have $g(X_E) > 1$. Then for $\alpha \in_{af} K$, the specialization $\lambda(x,\alpha)$ is K-irreducible, and its splitting field has degree divisible by $\binom{n}{j}$.*

Proof. As $\deg \tilde{\phi}_{n,j} = [K_j : K_0] = \#S_n/\#S_{n,j} = \binom{n}{j} \geq n$, and $n \geq 5$, Lemma 8(b) says that K'/K_0 is the Galois closure of K_j; equivalently, K'/K_0 is the splitting field of $\Lambda_j(x,t)$ over K_0. But K' is the splitting field of $\lambda(x,t) = \Lambda_1(x,t)$ over K_0, so by Proposition 1, for $\alpha \in_{\mathrm{af}} K$ the splitting field of $\lambda(x,\alpha)$ contains the roots of $\Lambda_j(x,\alpha)$, and we are done. □

For the proof of Theorem 1, we will employ the following application of Proposition 1.

Theorem 3. *Suppose $n \geq 7$ and $\Lambda_j(x,t)$ satisfies the hypothesis in Lemma 10 for each integer $j \in [1, n/2]$. Then for $\alpha \in_{af} K$, the specialization $\lambda(x,\alpha)$ is K-irreducible and has Galois group containing A_n.*

Proof. First, recall that $\Lambda_1 = \lambda$. By Lemma 10, $\lambda(x, \alpha)$ is K-irreducible for $\alpha \in_{\text{af}} K$, hence its Galois group is a transitive subgroup of S_n. If $n \geq 8$, then there exists a prime q with $n/2 < q < n-2$ [25, p. 370]. Necessarily q divides $\binom{n}{k}$ for some $1 < k < n/2$, so by Lemma 10, for $\alpha \in_{\text{af}} K$ the specialization $\lambda(x, \alpha)$ is K-irreducible, and q divides the degree of its splitting field over K. That means the Galois group of such a $\lambda(x, \alpha)$ is a transitive subgroup of S_n and has order divisible by q; a theorem of Jordan [17, Thm 5.6.2 and 5.7.2] then implies that this Galois group contains A_n.

For $n = 7$, Lemma 10 implies that for $\alpha \in_{\text{af}} K$, the Galois group of $\lambda(x, \alpha)$ is a transitive subgroup of S_7 of size divisible by $\text{LCM}\left(\binom{7}{2}, \binom{7}{3}\right) = 105$. By the classification of transitive subgroups of S_7 [7, p. 60] it follows that this Galois groups contains A_7. □

5.2. **Interpretation in terms of fiber products.**

We continue with the notation of the previous subsection and assume properties (i)-(iii) are satisfied. Fix a labelling $\lambda_1, \dots, \lambda_n$ of the roots of $\lambda = \Lambda_1$ in K', and let $\Sigma = \Sigma_1 = \{\lambda_1, \dots, \lambda_n\}$. For an integer $j \in [1, n-1]$, let Σ_j be the set of roots of Λ_j in K', and let $\Sigma^{(j)}$ be the set of "j-subsets" of Σ (i.e. those of cardinality j). Recall that Λ_j splits into linear factors over K', hence $\#\Sigma_j = \#\Sigma^{(j)} = \binom{n}{j}$. Each of these sets carries a natural action of $\text{Gal}(K'/K_0) \simeq S_n$.

Lemma 11. *For each $j \in [1, n-1]$, there is a bijective correspondence between Σ_j and $\Sigma^{(j)}$ which respects the natural action of $\text{Gal}(K'/K_0)$ on these sets.*

Before proving Lemma 11, let us state two applications of it that we shall need.

Proposition 2. *For $\alpha \in K$, the K-rational roots of $\Lambda_j(x, \alpha)$ are in one-to-one correspondence with the K-rational degree j factors of $\lambda(x, \alpha)$.*

Proof. The K-rational linear factors of $\Lambda_j(x, \alpha)$ are in one-to-one correspondence with the fixed points of G_λ in its action on $\Sigma^{(j)}$. By the Lemma, these are in one- to-one correspondence with the G_λ-invariant subsets of Σ of size j. The roots of a K-rational degree j factor of $\lambda(x, \alpha)$ clearly form such a subset, and conversely, a G_λ-invariant $T \in \Sigma_j$ gives the K-rational degree j factor $\prod_{\theta \in T}(x - \theta)$ of λ. □

Remark 5. Proposition 2 lends some perspective on Proposition 1. Namely, λ has a degree j factor, $1 \leq j \leq n-1$, over some intermediate field $K_0 \subseteq E \subseteq K'$ if and only if Λ_j has a root in E, i.e. if and only if E contains (a conjugate of) K_j. Thus the hypothesis of Proposition 1, namely that $g(X_E) \geq 2$ for every E over which λ is reducible is equivalent to the hypothesis that $g(X_j) \geq 2$ for $1 \leq j \leq n-1$. One then obtains Proposition 1 by applying Proposition 2 in conjunction with Faltings' Theorem.

Proposition 3. *Suppose $1 \leq j \leq n-1$. Then $\Lambda_j(x, t)$ is irreducible over the subfield of K'/K_0 fixed by A_n.*

Proof of Proposition 3. Since A_n is $(n-2)$-transitive, if $2 \leq j \leq n-2$ then A_n, as a subgroup of the group of permutations on the set Σ, acts transitively on the set $\Sigma^{(j)}$. Thanks to Lemma 11, A_n, as a subgroup of $\text{Gal}(K'/K_0)$, then acts transitively on the set of roots of Λ_j in K', establishing the Proposition for this range of j.

Write F for the fixed field of K'/K_0 by A_n. If Λ_1 is reducible over F, then $\mathrm{Gal}(K'/F)$ is contained in $S_l \times S_{n-l}$ for some $1 \le l \le n-1$. Since F/K_0 is quadratic, $\#\mathrm{Gal}(K'/K_0) \le 2 \cdot \#S_l \cdot \#S_{n-l} < \#S_n$, a contradiction. Thus Λ_1 is irreducible over F. Thanks to Lemma 11, that means A_n, as a subgroup of the group of permutations of Σ, acts transitively on $\Sigma^{(1)}$, hence also on $\Sigma^{(n-1)}$. Applying Lemma 11 again, we see that Λ_{n-1} is irreducible over F, as desired. □

We now verify Lemma 11 via a fiber product construction. The Lemma and the construction are probably well-known, but we cannot locate a reference for either one so we give the details here. We begin with a general setup. Recall that K is a field of characteristic 0.

Let $\wp_K^n$ denote the set of equivalence classes of non-zero, degree $\le n$ polynomials in $K[x]$, where two polynomials are identified if they are $K^\times$-multiples of each other. We have a natural bijection between $\wp_K^n$ and the set of K-rational points $\mathbf{P}_K^n(K)$ of projective n-space, via

$$a_0x^n + a_1x^{n-1} + \cdots + a_n \longmapsto [a_0 : \cdots : a_n].$$

In light of this, to give a polynomial $\lambda(x,t) \in K[x,t]$ which is non-constant and of degree $\le n$ in x is to give a non-constant K-morphism $\Lambda : \mathbf{P}_K^1 \to \mathbf{P}_K^n$. Also, for every $1 \le j < n$ the multiplication map $\wp_K^j \times \wp_K^{n-j} \to \wp_K^n$ gives rise to a K-morphism $\phi_{n,j} : \mathbf{P}_K^j \times \mathbf{P}_K^{n-j} \to \mathbf{P}_K^n$, whence a pull-back diagram

$$\begin{array}{ccc} X_j^\circ & \xrightarrow{\Lambda(j)} & \mathbf{P}_K^j \times \mathbf{P}_K^{n-j} \\ {\scriptstyle \tilde{\phi}_{n,j}^\circ}\downarrow & & \downarrow{\scriptstyle \phi_{n,j}} \\ \mathbf{P}_K^1 & \xrightarrow{\Lambda} & \mathbf{P}_K^n \end{array} \quad . \tag{17}$$

Denote by $\phi_n : (\mathbf{P}_K^1)^n \to \mathbf{P}_K^n$ the K-morphism corresponding to the n-fold multiplication map $(\wp_K^1)^n \to \wp_K^n$. Then we have an analogous pull-back diagram

$$\begin{array}{ccc} \overline{X} & \xrightarrow{\overline{\Lambda}} & (\mathbf{P}_K^1)^n \\ {\scriptstyle \overline{\phi}_n}\downarrow & & \downarrow{\scriptstyle \phi_n} \\ \mathbf{P}_K^1 & \xrightarrow{\Lambda} & \mathbf{P}_K^n \end{array} \quad . \tag{18}$$

Any permutation of the n-coordinates of the points of $(\mathbf{P}_K^1)^n$ is a K-morphism which is compatible with ϕ_n. Clearly $\deg \phi_n = n!$, so ϕ_n is a *regular* branched cover with deck transformation group S_n.

Suppose Λ corresponds to a separable, degree n polynomial λ over $K_0 = K(t)$. Then the fiber of $\overline{\phi}_n$ over the generic point of $\mathbf{P}_K^1$ consists of $n!$ pairwise distinct, *ordered* n-tuples of the roots of λ over K_0. Every element of the Galois group G_λ of λ over K_0 permutes these n-tuples, and such a permutation gives rise to a permutation on $(\mathbf{P}_K^1)^n$ making the diagram (18) commute. Having fixed a labelling of the roots of λ, we see that G_λ is canonically identified with a *subgroup* of S_n. Since λ is separable over K_0, these $n!$ n-tuples are pairwise distinct, whence the scheme $\overline{X}$ is reduced. Also,

$$
\begin{aligned}
\overline{X} \text{ is } K\text{-reducible} \quad &\Leftrightarrow \quad \text{the generic fiber of } \overline{\phi}_n \text{ is the disjoint union} \\
&\qquad\ \text{of non-trivial, } G_\lambda\text{-stable subsets} \\
&\Leftrightarrow \quad G_\lambda \text{ does not act transitively on this fiber} \\
&\Leftrightarrow \quad G_\lambda \subsetneq S_n. \qquad (19)
\end{aligned}
$$

The multiplication map $(\wp^1_K)^n \rightarrow \wp^n_K$ naturally factors through every $\wp^j_K \times \wp^{n-j}_K$. That means $\overline{\phi}_n$ factors through $\phi_{n,j}$ for every j; therefore the diagram (18) factors through the diagram (17) for every j, and $\Phi_{n,j}$ is also a regular branched cover with deck transformation group isomorphic to $S_j \times S_{n-j}$:

$$
\begin{array}{ccccc}
 & \overline{X} & \xrightarrow{\ \overline{\Lambda}\ } & (\mathbf{P}^1_K)^n & \\
 & \downarrow{\scriptstyle \tilde{\Phi}_{n,j}} & & \downarrow{\scriptstyle \Phi_{n,j}} & \\
\overline{\phi}_n & X^\circ_j & \xrightarrow{\ \Lambda(j)\ } & \mathbf{P}^j_K \times \mathbf{P}^{n-j}_K & \phi_n \\
 & \downarrow{\scriptstyle \tilde{\phi}^\circ_{n,j}} & & \downarrow{\scriptstyle \phi_{n,j}} & \\
 & \mathbf{P}^1_K & \xrightarrow{\ \Lambda\ } & \mathbf{P}^n_K &
\end{array}
$$

Finally, suppose λ satisfies hypotheses (i)-(iii). Then $G_\lambda = S_n$, whence the deck transformation group of $\overline{\phi}_n$ is also S_n. By (19), the scheme $\overline{X}$ is reduced and K-irreducible, and so it makes sense to speak of the function field $K(\overline{X})$. Both $\tilde{\Phi}_{n,j}$ and $\tilde{\phi}_{n,j}$ are surjective, so X°_j is also K-irreducible, and so it makes sense to speak of the function field $K(X^\circ_j)$ as well, and $K(\overline{X})/K(\mathbf{P}^1_K)$ is an S_n-extension of function fields. We have $\deg \tilde{\Phi}_{n,j} = j!(n-j)!$, and the same argument after (18) shows that the deck transformation group of $\tilde{\Phi}_{n,j}$ is isomorphic to a subgroup of, and hence is exactly, $S_j \times S_{n-j}$.

Proof of Lemma 11. First, recall the notations X_j, K_j etc. introduced after Lemma 9, and the fact that X_1 is given by $\lambda = 0$. For any $t_0 \in \mathbf{P}^1_{\overline{K}}$, the $\overline{K}$-rational points on the fibers of $\tilde{\phi}^\circ_{n,1}$ are in bijective correspondence with the $\overline{K}$-linear factors of $\lambda(x, t_0)$, while those on the fibers of $\tilde{\phi}_{n,1}$ are in bijective correspondence with the $\overline{K}$-rational points of the curve $\lambda(x,t) = 0$ with t-coordinates t_0. These two sets are in natural bijective correspondence with each other; the universal property of the pullback diagram (17) then implies that there is a K-isomorphism $\mu_n : X_1 \rightarrow X^\circ_1$ such that $\tilde{\phi}_{n,1} = \mu_n \tilde{\phi}^\circ_{n,1}$. This allows us to identify the two S_n-extensions $K(\overline{X})/K_0$ and K'/K_0. The $S_j \times S_{n-j}$ subgroups in S_n are pairwise conjugate, so we can identify the intermediate subfields $K(X^\circ_j)$ with $K(X_j)$. That means the smooth curve X_j is the canonical desingularization of X°_j, and $\tilde{\phi}_{n,j}$ is the extension of $\tilde{\phi}^\circ_{n,j}$ to X_j, whence the $\mathrm{Gal}(K'/K_0) \simeq S_n$ action on the roots of Λ_j over K_0 is the same as that on the generic fiber of $\tilde{\phi}^\circ_{n,j}$. But the points on this generic fiber are precisely the j-subsets of Σ. $\square$

6. Generalized Laguerre Polynomials

In this section we apply the machinery developed above to study specializations of Generalized Laguerre Polynomials $L^{(t)}_n(x)$ defined in the introduction. In subsection 6.1, we study the singular locus of the plane curve $\mathcal{L}_n$ defined by $L^{(t)}_n(x) = 0$. By analyzing the structure of maximal subgroups of S_n, in subsection 6.2 we compute the genus of the intermediate subfields of K'/K_0 over which Λ_j is reducible. In subsection 6.3 we combine these ingredients to deduce Theorem 1 following the strategy outlined in sections 2 and 5.

From now on, we fix n and take $\lambda(x,t) = L_n^{(t)}(x)$, carrying over all the notation (K_0, K_1, K', $\mathcal{O}_0$, G_λ, B_λ, etc.) from sections 2, 4, 5 to the present setting.

6.1. **The singular locus of $L_n^{(t)}(x)$.**

Fix $n > 2$. Following Schur [27, p. 54], we homogenize $L_n^{(t)}(x)$ by setting

$$\begin{aligned} F_n(x,\nu,\mu) &:= (-1)^n n!\mu^n L_n^{(\nu/\mu)}(x/\mu) \\ &= x^n - \frac{k_n}{1}x^{n-1} + \frac{k_{n-1}k_n}{1\cdots 2}x^{n-2} - \cdots + (-1)^n \frac{k_1\cdots k_n}{1\cdot 2\cdots n}, \end{aligned} \tag{20}$$

where $k_j = j(\nu + j\mu)$. Let $\mathcal{L}_n$ be the plane curve $F_n(x,\nu,\mu) = 0$. To simplify the notation, we write $\partial_x F_j$ for $\partial F_j/\partial x$. Then we have the relations [27, p. 54]

$$x\partial_x F_m = mF_m + k_m F_{m-1}, \qquad (m \geq 1, F_0 := 1); \tag{21}$$

$$F_m = (x - \nu - (2m-1)\mu)F_{m-1} - \mu k_{m-1} F_{m-2}, \qquad (m \geq 2). \tag{22}$$

Setting $\mu = 0$, (20) becomes

$$x^n - nx^{n-1}\nu + \frac{n(n-1)}{2}x^{n-2}\nu^2 - \cdots + (-1)^n\nu^n = (x-\nu)^n.$$

Thus $\mathcal{L}_n$ has exactly one point along the line at infinity, namely $[1:1:0]$. Let $\iota_n : \mathcal{L}_n \to \mathbf{P}^1_K$ be the projection map defined by $[x:\nu:\mu] \mapsto [\nu:\mu]$.

Lemma 12. *Suppose for some integer $j \in [0,n]$ and some point $z = [x(z):\nu(z):\mu(z)] \in \mathbf{P}^2_{\mathbf{C}}$ with $x(z)\mu(z) \neq 0$, we have*

$$F_{n-j}\big|_z = \partial_x F_{n-j}\big|_z = 0 \quad \textit{and} \quad k_{n-j} \neq 0. \tag{23}$$

Then $F_{n-j-1}\big|_z = 0$ and $k_{n-j-1} \neq 0$. Moreover, if $j \leq n-2$, then $\partial_x F_{n-j-1}\big|_z = 0$.

Proof. Since $\mu(z) \neq 0$, without loss of generality we can set $\mu(z) = 1$.

Suppose $n \geq j+1$; then substitute into (21) the first two relations in (23), we get $0 = k_{n-j}F_{n-j-1}\big|_z$, whence

$$F_{n-j-1}\big|_z = 0. \tag{24}$$

Next, suppose $k_{n-j-1} = 0$. When we use the expansion (20) to evaluate (24), we see that $x(z) = 0$, a contradiction. Finally, suppose $n \geq j+2$. Substituting (24) along with the first relation in (23) into (22), we get

$$0 = -\mu(z)k_{n-j-1}F_{n-j-2}\big|_z.$$

Substitute this and (24) back into (21) and we get $x\partial_x F_{n-j-1}\big|_z = 0$. As $x(z) \neq 0$, that means $\partial_x F_{n-j-1}\big|_z = 0$. This completes the proof of the Lemma. □

Lemma 13. *For $n \geq 3$ the curve $\mathcal{L}_n$ has no finite singular point.*

Proof. Using the relations (21) and (22), Schur [27, p. 54] showed that F_n, viewed as a polynomial in x, has discriminant

$$\mu^{\frac{n(n-1)}{2}} n! k_2 k_3^2 \cdots k_n^{n-1}. \tag{25}$$

We are interested in the finite points on $\mathcal{L}_n$, so for the rest of the proof we can set $\mu = 1$. Clearly it suffices to consider only the points on $\mathcal{L}_n$ lying above the branch locus of ι_n.

Suppose $z = (x_0, \nu_0)$ is a finite singular point. By (25) we have $\nu_0 \in \{-2, \ldots, -n\}$, and

$$F_n\big|_z = \partial_x F_n\big|_z = \partial_\nu F_n\big|_z = 0. \tag{26}$$

We claim that $x_0 \neq 0$. Suppose otherwise; set $\partial_\nu F_n = 0$ and then substitute $x = 0$ (recall that $\mu = 1$), to get

$$0 = (-1)^n \frac{\partial}{\partial \nu} \prod_{k=1}^{n} (\nu + k) = (-1)^n \sum_{m=1}^{n} \prod_{\substack{k=1 \\ k \neq m}}^{n} (\nu + k).$$

Set $\nu = \nu_0$ and this becomes

$$\prod_{\substack{k=1 \\ k \neq -\nu_0}}^{n} (\nu_0 + k) = 0,$$

a contradiction. Thus $x_0 \neq 0$. Also, if $k_n = 0$, then from (20) we get $x_0 = 0$, a contradiction. Thus $k_n \neq 0$, i.e. $\nu_0 \neq -n$. That means the hypotheses of Lemma 12 are satisfied for $j = 0$. Applying the lemma, we find the conditions of the lemma hold for $j = 1$ as well as $\nu_0 \neq 1 - n$. Repeating this procedure, we find $\nu_0 \notin \{-2, \cdots, -n\}$, a contradiction. Thus $\mathcal{L}_n$ has no finite singular point. ☐

Lemma 14. *Suppose $n \geq 2$. Then $K(\sqrt{disc\ L_n^{(t)}(x)})$ is a quadratic extension of K_0 corresponding to a smooth curve of genus $\left[\frac{n-2}{4}\right]$.*

Proof. Since $n \geq 2$, (25) says that disc $L_n^{(t)}(x)$ is a polynomial in t whose square-free part has degree $\left[\frac{n}{2}\right]$, and the Lemma follows. ☐

Recall that the notation of section 4, such as $\mathcal{O}_0, \mathcal{O}'$ etc. now applies to the case $\lambda(x,t) = L_n^{(t)}(x)$. For $\nu \in B_\lambda = \{-2, \ldots, -n\} \subset \mathbf{P}_K^1$, denote by $\mathfrak{m}_\nu$ the corresponding maximal ideal in $\mathcal{O}_0$. Denote by $\mathcal{O}_1$ the coordinate ring of an affine open set of X_1 containing all places lying above every ν with respect to the projection map ι_n. Then (25) says that the restriction of ι_n to $\mathcal{O}_0$ is unramified outside the $\mathfrak{m}_\nu$, and Lemma 13 says that the inclusion map $\mathcal{O}_0 \subset \mathcal{O}'$ is an integral extension of Dedekind domains when localized at these $\mathfrak{m}_\nu$. From (20) and (25), we see that $\mathcal{O}_1$ has exactly one ramified maximal ideal lying above $\mathfrak{m}_\nu$:

$$\mathfrak{m}_\nu \mathcal{O}_1 = \mathfrak{n}_0^{|\nu|} \mathfrak{n}_1 \cdots \mathfrak{n}_s, \tag{27}$$

where the $\mathfrak{n}_i$ are pairwise distinct; in other words each branch point ν of $L_n^{(t)}(x)$ is simple of index $|\nu|$. Applying Lemma 7, we deduce the following result.

Lemma 15. *For $\nu \in \{-2, \ldots, -n\}$, let $\mathfrak{M}_\nu \subset \mathcal{O}'$ be a maximal ideal lying above $\mathfrak{m}_\nu$. Then the inertia group $I(\mathfrak{M}_\nu/\mathfrak{m}_\nu)$ is generated by a cycle of length $|\nu|$. In particular,*

$$e_\nu := e(\mathfrak{M}_\nu/\mathfrak{m}_\nu) = |\nu|.$$

□

Proposition 4. *Suppose $n \geq 6$. Then the geometric genus of $\mathcal{L}_n$ is > 1.*

Proof. First, assume $n \geq 7$. Thanks to Lemma 15, we can apply Lemma 3 with $V = \{-n, 1-n, \ldots, 5-n\}$. Since there is a unique prime in $\mathcal{O}_1$ above $\mathfrak{m}_\nu$ with non-trivial ramification index $-nu$, we have $c_1(\nu) = n + \nu$, and (4) becomes

$$g(\mathcal{L}_n) = g(K_1) \geq 1 + \frac{n}{2}\Big(-2 + \sum_{i=0}^{5}\Big(1 - \frac{1}{d(n-i)}\Big)\Big) - \frac{1}{2}\sum_{i=0}^{5}\Big(1 - \frac{1}{d(n-i)}\Big) \cdot i \tag{28}$$

For any six consecutive, positive integers, exactly two of them are prime to 6, another one is odd, and the remaining three are even. Thus the first i-sum in (28) is

$$\geq -2 + 6 - 2 \times \frac{1}{5} - \frac{1}{3} - 3 \times \frac{1}{2} = \frac{53}{30}.$$

Thus (28) yields

$$g(\mathcal{L}_n) \geq 1 + \frac{53n}{60} - \frac{1}{2}\Big(1 - \frac{1}{n}\Big)(0+1+2+3+4+5), \tag{29}$$

which is > 1 if $n > 10$. Using the more refined version (28) we find that in fact $g(\mathcal{L}_n) > 1$ if $n \geq 7$. Using the full Riemann-Hurwitz formula, or the ALGCURVES package in MAPLE, we find that $g(\mathcal{L}_6) = 4$. This completes the proof of the Proposition. □

Remark 6. By analyzing the singularity at infinity, one in fact has a nice formula $g(\mathcal{L}_n) = [(n-2)^2/4]$ valid for all n.

6.2. **Genus of maximal subgroups.**

In this subsection, we carry out the calculations which will be necessary ingredients for the application of Theorem 3 to $L_n^{(t)}(x)$ in the next section. This involves a mixed strategy in the following sense. For $n \geq 10$, we show that every *minimal* intermediate subfield E of K'/K_0 has genus > 1, thanks to Lemma 14 and Proposition 5 below. It then follows from Riemann-Hurwitz that *every* proper intermediate subfield has genus > 1. For $6 \leq n \leq 9$, the quadratic extension inside K'/K_0 has genus 0 or 1, but we have shown in Proposition 3 that Λ_j is not reducible over this field. It remains, then, to check for $6 \leq n \leq 9$ that *proper* subgroups of A_n give fixed fields of genus > 1, and this is the content of Proposition 6. We treat $n = 5$ "by hand."

Proposition 5. *Suppose $n \geq 6$. If $\mathcal{E}$ is a maximal subgroup of G_λ other than A_n, with corresponding fixed field E, then $g(X_E) > 1$.*

Proposition 6. *Suppose $6 \leq n \leq 9$. If $\mathcal{E}$ is a proper maximal subgroup of $A_n \subset G_\lambda$, with corresponding fixed field E, then $g(X_E) > 1$.*

Proof of Proposition 5. Up to conjugation, the maximal subgroups of S_n other than A_n belong to exactly one of the following three types [7, p. 268]:

- imprimitive subgroups: the wreath products $S_j \wr S_{n/j}$ in its imprimitive action[1], for some divisor j of n, $1 < j < n$;
- intransitive subgroups: $S_{n,j}$ for some $1 \leq j < n/2$ (note that if n is even then $S_{n,n/2}$ is contained in $S_{n/2} \wr S_2$);
- a primitive subgroup of S_n.

For each of the three types of $\mathcal{E}$, we use group-theoretic properties of $\mathcal{E}$ plus ramification data of K'/K_0 to bound (4) from below for large n, and then handle the remaining cases individually. Note that among any four consecutive integers ≥ 2, exactly one of them is prime to 6, another one is odd, and the other two are even. Recall the notation $d(e)$ from Definition 1 and we see that for $n \geq 6$,

$$-2 + \sum_{j=0}^{3}\Big(1 - \frac{1}{d(n-j)}\Big) \geq -2 + 4 - \frac{1}{2} - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} = \frac{7}{15}. \tag{30}$$

We will also make repeated use of the following remark. For the rest of this section we will take

$$V = \{3-n, 2-n, 1-n, -n\},$$

so if $n \geq 6$ then Lemma 15 implies that the inertia group of any $\nu \in V$ is generated by a single *cycle*, which will allow us to use Lemma 6 in conjunction with (4).

Case: imprimitive subgroups $S_j \wr S_{n/j}$

First, suppose $n \geq 7$. Since $n - 3 > n/2$, $S_j \wr S_{n/j}$ does not contain any $(n-\mu)$-*cycle* for $0 \leq \mu \leq 3$. That means $c_1(\nu) = 0$ for every $\nu \in V$. Recall (30) and (4) becomes

$$g(X_E) \geq 1 + \frac{7}{30}[S_n : S_j \wr S_{n/j}] > 1.$$

Next, suppose $n = 6$. The same reasoning as above shows that $c_1(\nu) = 0$ if $\nu \leq 2-n$, and if $j = 2$, then $c_1(3-n) = 0$ as well. So as before $g(X_E) > 1$ if $\mathcal{E} \simeq S_2 \wr S_3$. It remains to consider the case $\mathcal{E} \simeq S_3 \wr S_2 \simeq (S_3 \times S_3) \rtimes \mathbf{Z}/2$. A representative of the non-trivial coset of $S_3 \times S_3$ in $(S_3 \times S_3) \rtimes \mathbf{Z}/2$ (as a subgroup of S_6) is $(14)(25)(36)$; from this we check that elements in this non-trivial coset all have even order. Thus the order 3 elements in $(S_3 \times S_3) \rtimes \mathbf{Z}/2$ are all contained in $S_3 \times S_3$. The latter has a unique Sylow 3-subgroup, namely $\mathbf{Z}/3 \times \mathbf{Z}/3$, so $\mathcal{E}$ has four distinct $\mathbf{Z}/3$-subgroups, whence (10) gives $c_1(-3) = \frac{8}{\# S_3 \wr S_2} 3 \cdot 3! = 2$. Thus

$$g(X_E) \geq 1 + \frac{6!/72}{2}\frac{7}{15} - \frac{1}{2} \cdot 2 \cdot \Big(1 - \frac{1}{3}\Big) > 1,$$

as desired.

Case: intransitive subgroups $S_{n,j}$ with $1 \leq j < n/2$

For $j > 3$, $S_{n,j}$ contains no cycle of length $\geq n-3$, so $c_1(\nu) = 0$ for every $\nu \in V$. Thus (4) gives $g(X_E) > 1$.

[1] i.e. the stabilizer of a partition of n letters into n/j disjoint subsets of equal size

Next, suppose $j = 3$, so that we can take $n \geq 7$. Then $c_1(\nu) = 0$ for $|\nu| > n-3$, and (11) gives $c_1(3-n) < 6(n-3)$. Thus (4) becomes

$$g(X_E) \geq 1 + \frac{7}{30}\frac{n!}{3!(n-3)!} - \frac{6n-19}{2}\Big(1 - \frac{1}{d(n-3)}\Big),$$

which is easily seen to be > 1 for $n \geq 7$ (for $n \geq 8$, use the trivial bound $d(n-3) \leq n-3$).

Now, take $j = 2$. Since $n \geq 6$, the only cycles of order $n-2$ and $n-3$ in $S_{n,2} = S_2 \times S_{n-2}$ come from the cycles in S_{n-2} of such order. There are $(n-3)!$ and $(n-2)(n-4)!$ of them, respectively, so by (10),

$$c_1(n-2) = 1 \quad \text{and} \quad c_1(n-3) = 3,$$

whence (4) plus (30) gives

$$g(X_E) \geq 1 + \frac{7}{30}\frac{n(n-1)}{2} - \frac{1}{2}\Big(1 - \frac{1}{d(n-2)}\Big) - \frac{3}{2}\Big(1 - \frac{1}{d(n-3)}\Big).$$

This is > 1 for $n \geq 5$, so we are done.

Finally, consider the case $j = 1$. Then X_E is simply the curve X_1, which we saw right before the statement of Lemma 10 is simply the curve $\mathcal{L}_n$ defined by $L_n^{(t)}(x)$. By Proposition 4, this curve has geometric genus > 1 if $n \geq 6$, so we are done.

Case: primitive subgroups

Let $\mathcal{E} \subset S_n$ be a primitive subgroup other than A_n. By Bochert's theorem [7, p. 79],

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

Using (11) together with the trivial estimate $1 - \frac{1}{d(e_\nu)} \leq 1 - \frac{1}{n}$, (4) becomes

$$\begin{aligned} g(X_E) &\geq 1 + \frac{7}{30}[S_n : \mathcal{E}] - \frac{1}{2}\Big(1 - \frac{1}{n}\Big)((n-1) + (n-2) + (2n-5)) + (6n-19)) \\ &\geq 1 + \frac{7}{30}\Big[\frac{n+1}{2}\Big]! - \Big(1 - \frac{1}{n}\Big)\frac{10n-27}{2} \qquad (31) \\ &\geq 1 + \frac{7\sqrt{\pi n}}{30}\Big(\frac{n}{2e}\Big)^{n/2} - \Big(1 - \frac{1}{n}\Big)\frac{10n-27}{2} \qquad \text{Stirling formula [1, p. 24].} \qquad (32) \end{aligned}$$

From (32) we get that $g(X_E) > 1$ if $n \geq 15$. Using the sharper form (31), we see that in fact $g(X_E) > 1$ if $n \geq 11$. For $n = 9, 10$, if we use the original inequality (4), we also obtain $g(X_E) > 1$. To handle the remaining values of n, i.e. $6, 7, 8$, we make use of classification of primitive groups of small degree [2].

$n = 8$ S_8 has two maximal primitive subgroups other than A_7, namely $PGL(2, \mathbf{F}_7)$ and $2^3 \cdot PSL_2(\mathbf{F}_7)$ (a group with normal subgroup $(\mathbf{Z}/2)^3$ and with quotient $PSL_2(\mathbf{F}_7)$). In particular, both groups contain no element of order 5, so the c_1-term in (4) corresponding to the branched point $\nu = -5$ is zero. For the group $PGL_2(\mathbf{F}_7)$, (4) then becomes

$$1 + \frac{7}{30}\frac{8!}{336} - \frac{1}{2}\Big(7\Big(1 - \frac{1}{2}\Big) + 6\Big(1 - \frac{1}{7}\Big) + 11\Big(1 - \frac{1}{2}\Big)\Big) > 1.$$

To handle the group $2^3 \cdot PSL_2(\mathbf{F}_7)$ we need to refine our estimate for the $c_1(-7)$-term. Sylow theory dictates that $2^3 \cdot PSL_2(\mathbf{F}_7)$ has at most 64 Sylow 7-subgroups, all of order 7, so $2^3 \cdot PSL_2(\mathbf{F}_7)$ has at most $64 \times 6 = 384$ elements of order 7. Substitute this into (10) and we find that $c_1(-7) \leq 2$, whence (4) becomes

$$1 + \frac{7}{30}\frac{8!}{8 \times 168} - \frac{1}{2}\Big(7\Big(1-\frac{1}{2}\Big) + 2\Big(1-\frac{1}{7}\Big) + 11\Big(1-\frac{1}{2}\Big)\Big) > 1.$$

$\boxed{n=7}$ S_7 has a unique maximal primitive subgroup other than A_7, namely $PSL_2(\mathbf{F}_7)$. It has 42 elements of order 4, no element of order 5, and 48 elements of order 7, so $c_1(-4) = \frac{42}{168}4 \cdot 6 = 6$, $c_1(-5) = 0$, and $c_1(-7) = \frac{48}{168} \cdot 7 = 2$, whence (4) becomes

$$g(X_E) \geq 1 + \frac{7}{30}\frac{7!}{168} - \frac{1}{2}\Big(2(1-\frac{1}{7}) + 5\Big(1-\frac{1}{2}\Big) + 6\Big(1-\frac{1}{2}\Big)\Big) > 1.$$

$\boxed{n=6}$ S_6 has a unique maximal primitive subgroup other than A_6, namely $PGL_2(\mathbf{F}_5) \simeq S_5 \simeq S_{6,1}$. For such intransitive groups we already saw that $g(X_E) > 1$, so we are done for $n = 6$. This completes the proof of Proposition 5. $\square$

Proof of Proposition 6. We will make extensive use of the *Atlas* [3] to determine the maximal subgroups of these A_n, and for the number of conjugacy classes of elements A_n and $PSL_2(\mathbf{F}_q)$. For the rest of the proof we take $V = \{-n, 1-n, 2-n, 3-n\}$.

$\boxed{n=9}$ According to the *Atlas*, the maximal subgroups[2] of A_9 are A_8, S_7, plus others of indices ≥ 84 in A_9. First, consider those $\mathcal{E}$ of index ≥ 84 in A_9. Then $[S_9 : \mathcal{E}] \geq 168$, and (4) becomes

$$\begin{aligned} g(X_E) &\geq 1 + \frac{7}{30}168 - \frac{1}{2}\Big(\Big(1-\frac{1}{3}\Big)c_1(-9) + \Big(1-\frac{1}{2}\Big)c_1(-8) + \Big(1-\frac{1}{7}\Big)c_1(-7) + \Big(1-\frac{1}{2}\Big)c_1(-6)\Big) \\ &\geq 1 + \frac{196}{5} - \frac{1}{2}\Big(\frac{2}{3}8 + \frac{1}{2}7 + \frac{6}{7}13 + \frac{1}{2}35\Big) > 1, \end{aligned}$$

which is satisfactory. Next, take $\mathcal{E} = A_8$. Then $[S_9 : \mathcal{E}] = 18$, and A_8 has no *cycles* of order $9, 8$ or 6, so $c_1(-9) = c_1(-8) = c_1(-6) = 0$. There are $8!/7$ elements of order 7 in A_8, so $c_1(-7) = \frac{8!/7}{8!/2}7 \cdot 2 = 4$. Thus

$$g(X_E) \geq 1 + \frac{7 \cdot 18}{30} - \frac{4}{2}\Big(1 - \frac{1}{7}\Big) > 1.$$

Finally, take $\mathcal{E} = S_7$. Then $[S_9 : \mathcal{E}] = 72$ and S_7 has no element of order 9 or 8, so

$$g(X_E) \geq 1 + \frac{7 \cdot 72}{30} - \frac{1}{2}\Big(\Big(1-\frac{1}{7}\Big)13 + \Big(1-\frac{1}{2}\Big)35\Big) > 1.$$

This completes the case $n = 9$.

$\boxed{n=8}$ The maximal subgroups of A_8, along with their indices in A_8, are

$$(A_7, 8);\ \ ((2^3 : PSL_2(\mathbf{F}_7)), 15);\ \ (S_6, 28);\ \ (2^4 : (S_3 \times S_3), 35);\ \ ((A_5 \times 3) : 2, 56).$$

From (11) we get the standard estimates

$$c_1(-8) < 8,\ \ c_1(-7) < 7,\ \ c_1(-6) < 6 \cdot 2!. \tag{33}$$

[2] in what follows we will consider the *isomorphism* classes, and not *conjugacy classes*, of maximal subgroups of these A_n. For the purpose of computing $g(X_E)$ this is sufficient.

The case $\mathcal{E} = 2^3 : PSL_2(\mathbf{F}_7)$ has already been dealt with in the course of proving Prop. 5. For $\mathcal{E} = 2^4 : (S_3 \times S_3)$, it has no element of order 5 or 7, whence $c_1(-5) = c_1(-7) = 0$. We have $[S_n : \mathcal{E}] = 70$, so (4) becomes

$$g(X_E) \geq 1 + \frac{7}{30}70 - \frac{1}{2}\Big(\Big(1 - \frac{1}{2}\Big)8 + \Big(1 - \frac{1}{2}\Big)12\Big) > 1.$$

Next, take $\mathcal{E} = (A_5 \times 3) : 2$, i.e. a split extension with kernel $A_5 \times \mathbf{Z}/3$ and quotient $\mathbf{Z}/2$. The order 5 elements in $\mathcal{E}$ are all in $A_5 \times \mathbf{Z}/3$, and hence there are 4! of them. Thus (10) gives $c_1(-5) = \frac{4!}{360}5 \cdot 3! = 2$. Also, $\mathcal{E}$ has no element of order 7, so $c_1(-7) = 0$. Thus (11) becomes

$$g(X_E) \geq 1 + \frac{7}{30}112 - \frac{1}{2}\Big(\Big(1 - \frac{1}{2}\Big)8 + \Big(1 - \frac{1}{2}\Big)6 + \Big(1 - \frac{1}{5}\Big)2\Big) > 1.$$

For $\mathcal{E} = S_6$, again it has no order 7 elements so $c_1(-7) = 0$. It has $6!/5$ order 5 elements, so $c_1(-5) = \frac{6!/5}{6!}5 \cdot 3! = 6$. Thus (4) becomes

$$1 + \frac{7}{30}56 - \frac{1}{2}\Big(\Big(1 - \frac{1}{2}\Big)8 + \Big(1 - \frac{1}{2}\Big)6 + \Big(1 - \frac{1}{5}\Big)6\Big) > 1.$$

Now take $\mathcal{E} = A_7$. There are no cycles of length 6 or 8 in A_7, so $c_1(-8) = c_1(-6) = 0$. There are 6! order 7 elements and $7!/(5 \cdot 2!)$ order 5 elements in A_7, so $c_1(-7) = c_1(-5) = 1$. Thus

$$g(X_E) \geq 1 + \frac{7}{30}8 - \frac{1}{2}\Big(\Big(1 - \frac{1}{7}\Big) + \Big(1 - \frac{1}{5}\Big)\Big) > 1.$$

$\boxed{n = 7}$ The maximal subgroups of A_7, along with their indices in A_7, are

$$(A_6, 7);\ \ (PSL_2(\mathbf{F}_7), 15);\ \ (S_5, 21);\ \ ((A_4 \times 3) : 2, 35).$$

Note that (11) gives the following estimates

$$c_1(-7) < 7,\ \ c_1(-6) < 6,\ \ c_1(-5) < 5 \cdot 2,\ \ c_1(-4) < 4 \cdot 6.$$

First, take $\mathcal{E} = (A_4 \times 3) : 2$. Then $\mathcal{E}$ has no element of order 7 or 5, so $c_1(-7) = c_1(-5) = 0$. Thus (4) becomes

$$g(X_E) \geq 1 + \frac{7}{30}70 - \frac{1}{2}\Big(\Big(1 - \frac{1}{2}\Big)5 + \Big(1 - \frac{1}{2}\Big)23\Big) > 1.$$

Next, take $\mathcal{E} = S_5 \subset A_7$. Then it has no *cycles* of order 7 or 6, so $c_1(-7) = c_1(-6) = 0$. It has 4! elements of order 5, and $5!/4$ elements of order 4. Thus $c_1(-5) = 2$ and $c_1(-4) = 6$. Thus

$$g(X_E) \geq 1 + \frac{7}{30}42 - \frac{1}{2}\Big(\Big(1 - \frac{1}{5}\Big)2 + \Big(1 - \frac{1}{2}\Big)6\Big) > 1.$$

Now, take $\mathcal{E} = A_6 \subset A_7$. It has no order 7 elements and no *cycles* of order 6 or 4. It has $6!/5$ order 5 elements, so $c_1(-5) = 2$. Thus

$$g(X_E) \geq 1 + \frac{7}{30}14 - \frac{1}{2}\Big(1 - \frac{1}{5}\Big)2 > 1.$$

Finally, take $\mathcal{E} = PSL_2(\mathbf{F}_7)$. It has 42 elements of order 4, none of order 5 or 6, and 48 elements of order 7. Thus $c_1(-4) = \frac{42}{168}4 \cdot 3! = 6, c_1(-5) = c_1(-6) = 0, c_1(-7) = \frac{48}{168}7 = 2$. Then

$$g(X_E) \geq 1 + \frac{7}{30}30 - \frac{1}{2}\Big(\Big(1 - \frac{1}{7}\Big)2 + \Big(1 - \frac{1}{2}\Big)6\Big) > 1.$$

$\boxed{n=6}$ The maximal subgroups of A_6, along with their indices in A_6, are

$$(A_5, 6); \ \ ((\mathbf{Z}/3 \times \mathbf{Z}/3) \rtimes \mathbf{Z}/4, 10); \ \ (S_4, 15).$$

First, take $\mathcal{E} = S_4$. It has six elements of order 4, eight of order 3, and none of order 5 or 6. Thus $c_1(-4) = 2, c_1(-3) = 6, c_1(-6) = c_1(-5) = 0$, whence $g(X_E) > 1$.

Next, take $\mathcal{E} = A_5$. It has twenty-four elements of order 5, twenty elements of order 3, and none of order 6 or 4. Thus $c_1(-5) = 1, c_1(-3) = 3, c_1(-6) = c_1(-4) = 0$, whence $g(X_E) > 1$.

Finally, take $\mathcal{E} = (\mathbf{Z}/3 \times \mathbf{Z}/3) \rtimes \mathbf{Z}/4$. Then $c_1(-5) = 0$. There are 8 elements of order 3, and hence ≤ 27 elements of order 4. Thus $c_1(-3) = 4$ and $c_1(-4) \leq 6$. It follows that $g(X_E) > 1$. This completes the proof of Proposition 6. $\square$

6.3. **Proof of Theorem 1.**

$\boxed{\text{STEP I.}}$ First, we treat the case $n = 5$ using an argument specific to quintics. A separable quintic over K (not necessarily irreducible) has a solvable Galois group if and only if its resolvent sextic has a root in K [8]. Compute the resolvent sextic of $L_5^{(t)}(x)$ using the formula in [8] and set it to $(x - 10A)(x^5 + c_1x^4 + \cdots + c_5)$, obtaining six equations in $t, A, c_1, \ldots, c_5$. Eliminate $c_1, \ldots, c_5$ from the six equations using MAPLE and we arrive at a single equation in t and A:

$$\begin{aligned}
&A^6 + (-12t^2 - 24t)A^5 + (120t^2 + 60t^3)A^4 \\
&\quad + (720t^3 + 2120t^4 + 1600t^5 + 360t^6)A^3 \\
&\quad + (-5040t^4 - 11580t^6 - 4200t^7 - 540t^8 - 13200t^5)A^2 \\
&\quad + (10368t^4 + 39744t^5 + 48864t^6 + 14448t^7 - 12480t^8 - 9360t^9 - 1728t^{10})A \\
&\quad - 3(5832t^5 + 26892t^6 + 50814t^7 + 50645t^8 + 28406t^9 + 8735t^{10} + 1278t^{11} + 54t^{12}).
\end{aligned}$$

Using the ALGCURVES package in MAPLE, we find that this equation is absolutely irreducible and defines a plane curve with geometric genus 3. Thanks to Faltings, that means $L_5^{(\alpha)}(x)$ is K-irreducible and is not solvable for $\alpha \in_{\text{af}} K$. This completes the proof for the case $n = 5$. From now on, assume that $n \geq 6$.

$\boxed{\text{STEP II.}}$ Given a number field K, we claim that if there exists *one* $\beta \in K$ for which $L_n^{(\beta)}(x)$ has S_n-Galois group over K_0, then Theorem 1 holds for this K.

By (25), the discriminant of $L_n^{(t)}(x)$ is not constant. Since $n \geq 5$, Lemma 8 applies so that the existence of this one β yields the necessary hypotheses on K'/K_0. For $n \geq 10$, the genus of the fixed field of every proper maximal subgroup of G_λ is greater than 1 (Proposition 5 and Lemma 14). By Riemann-Hurwitz, since K has characteristic 0, $g(X_E) \leq g(X_{E'})$ whenever $E \subset E'$. Thus, for $n \geq 10$, *every* non-trivial intermediate subfield of K'/K_0 has genus greater than 1. For degrees $n = 6, 7, 8, 9$, we have shown, (a) that *proper* maximal subgroups of A_n and S_n have genus greater than one (Propositions 5 and 6), and (b) over the quadratic subfield of K_0 in K', the polynomials Λ_j are all irreducible (Proposition 3). Thus, for all $n \geq 6$, the hypotheses of Theorem 3 are satisfied.

We therefore obtain the first part of Theorem 1(a) for $n \geq 7$. By Lemma 14, if $n \geq 10$ (resp. $n \geq 6$) then the set of $t \in K$ corresponding to even Galois groups are parameterized by a curve of geometric genus ≥ 2 (resp. ≥ 1). The rest of Theorem 1 for $n \geq 7$ now follows.

For $n = 6$, the argument for Theorem 3 only shows that the degree of the splitting field of all but finitely many $L_n^{(\alpha)}(x)$ over K is divisible by $\mathrm{LCM}\big(\binom{6}{2}, \binom{6}{3}\big) = 60$. To improve this we use a different test function. By Lemma 8(a), the fixed field of K'/K_0 by $S_3 \times \{1\} \subset S_{6,3}$ corresponds to a smooth projective curve $X_{3,0}$ plus a K-morphism $\xi_{3,0} : X_{3,0} \to \mathbf{P}^1_K$. Write $\Lambda_{3,0}(x,t) = 0$ for the corresponding birational plane curve. The same argument as in Lemma 11 shows that the roots of $\Lambda_{3,0}(t)$ over K_0 are in bijective correspondence with triples of roots of $L_6^{(t)}(x)$ over K_0. Argue as in Proposition 3 and we see that $\Lambda_{3,0}(x,t)$ is irreducible over the fixed field of K'/K_0 by A_6. The discussion in subsection 6.2 is now applicable, and we see that for $\alpha \in_{\mathrm{af}} K$, the degree of the splitting field of $L_n^{(\alpha)}(x)$ over K is divisible by $\deg \xi_{3,0} = [S_6 : S_3 \times \{1\}] = 120$. By the classification of transitive subgroups of S_6 [7, p. 60], we are done.

Step III. Schur [26] showed that $L_n^{(0)}(x)$ is $\mathbf{Q}$-irreducible and has S_n Galois group. That means $L_n^{(t)}(x) = 0$ has S_n Galois group over $\mathbf{Q}(t)$. Apply Step II and we get Theorem 1 for $K = \mathbf{Q}$. In particular, $\lambda(x, \alpha)$ has S_n Galois group over $\mathbf{Q}$ for all but finitely many $\alpha \in \mathbf{Z}$. From (25) we see that, for any finite set of primes Σ, infinitely many of these S_n-extensions of $\mathbf{Q}$ must be ramified outside Σ. There are only finitely many number fields of bounded degree which are unramified outside Σ, so for any fixed number field K, there exist infinitely many $\alpha' \in \mathbf{Q}$ so that any root of $L_n^{(\alpha')}(x)$ defines a degree n extension $L_{\alpha'}/\mathbf{Q}$ with S_n-Galois closure and is ramified at a prime which is unramified in $K/\mathbf{Q}$. Since S_n has no subgroup of index $< n$, that means $L_{\alpha'} \cap K = \mathbf{Q}$, whence $L_n^{(\alpha')}(x)$ also has S_n Galois group over K. Apply Step II with $\beta = \alpha'$ and we are done.

7. Simple covers

Let Y be a smooth projective curve defined over a number field K, and let $\pi : Y \to \mathbf{P}^1_K$ be a K-morphism of degree n. We say that π is a *simple cover* if the fiber above every point in $\mathbf{P}^1_{\overline{K}}$ contains at least $n-1$ distinct points. In other words, every branch point of π is simple of index 2. By [11, top of p. 549], the (geometric) Galois group of a simple n-cover is precisely S_n. Say Y has genus g; then the Riemann-Hurwitz formula implies that the number of branch points of π is exactly

$$\#B_\pi = 2g + 2n - 2. \tag{34}$$

Over an algebraically closed field, if $n \geq g+1$ then every smooth projective curve of genus g admits a simple cover of degree n [11, Prop. 8.1].

Suppose $\lambda(x,t) \in K[x,t]$ is irreducible over $K_0 = K(t)$ of degree n and defines a simple cover K_1/K_0 (in the notation of section 2). To simplify the exposition, suppose K is algebraically closed in the splitting field K' of λ over K_0. The following example of Müller shows that we cannot expect all but finitely K-specializations of λ to be K-irreducible, let alone having the same Galois group as λ. Consider the transpositions $g_1 = (1,2), g_2 = (2,3), \ldots, g_{n-2} = (n-2, n-1), g_{n-1} = (n-1, n), g_n = (n-1, n), g_{n+1} = (n-2, n-$

1), ..., $g_{2n-3} = (2,3), g_{2n-2} = (1,2)$. Note that the product of these g_i is 1, and that they generate S_n. So by the Riemann existence theorem [32, Cor. 7.3], there exists a degree n branched cover $X_n \to \mathbf{P}^1_{\overline{K}}$ with exactly $2(n-1)$ branched points over $\overline{K}$, such that the inertia group of the i-th branch point is generated by g_i. By Riemann-Hurwitz, the cover with this description has geometric genus zero and is a simple cover. So taking a finite extension L/K if necessary, there are infinitely many L-rational specializations of this cover with an L-linear factor.

This example shows that there is not an analogue of Theorem 1 which holds for *all* simple covers of sufficiently large degree. But if we start with a simple cover of genus at least 2, then we can reach a similar conclusion, as in Part (b) of the following theorem. Even if we start with a rational or elliptic simple cover, however, Part (a) of the theorem says that all but finitely many specializations are either irreducible or factor as a linear times a degree $n-1$ irreducible factor. We give two proofs of Theorem 4. The first is due to Müller, and uses a classification theorem of Liebeck and Saxl; we thank Müller for suggesting that we include it here, as well as for catching an error in an earlier version of the theorem. The second proof illustrates the usefulness of the interpretation of the curve X_j introduced in section 5 as the variety whose K-rational points parametrize the K-rational degree j factors of λ.

Theorem 4. *Let $\lambda(x,t)$ be an irreducible polynomial over $K(t)$ defining a simple cover $\pi : Y \to \mathbf{P}^1_K$ of degree $n \geq 5$ and geometric genus $g = g_Y \geq 0$. If $g = 0$, assume $n \geq 6$. Then,*

(a) *For $\alpha \in_{af} K$, the specialization $\lambda(x,\alpha)$ has a K-irreducible factor of degree $\geq n-1$.*

(b) *If $g_Y \geq 2$, then for $\alpha \in_{af} K$, the specialization $\lambda(x,\alpha)$ is K-irreducible.*

(c) *If $g_Y \geq 2$ and $n \geq 7$, for $\alpha \in_{af} K$, the Galois group of $\lambda(x,\alpha)$ over K is S_n.*

First Proof. Suppose $\mathcal{E}$ is a subgroup of G_λ with fixed field E. The key step is the following claim.

Claim. If $\mathcal{E}$ is a maximal subgroup of G_λ not conjugate to $S_{n,1}$, then $g_E \geq 2$.

We now give a proof, communicated to us by Müller, of this claim. Suppose $\mathcal{E}$ is a maximal subgroup of S_n which is not conjugate to $S_{n,1}$. Recall that K'/K_0 is the Galois closure of the function field extension K_1/K_0 defined by the simple cover π. This yields an action of $\mathrm{Gal}(K'/K_0) \simeq S_n$ on the generic fiber of π_E. By Galois theory, this action, call it ρ_E, is simply the left-action of S_n on the left cosets of $\mathcal{E}$ in S_n. Since $\mathcal{E} \not\simeq S_{n,1}$, this action is not the natural degree n action of S_n. Let $\mu(\mathcal{E})$ be the largest integer m such that every transposition of S_n moves at least m points in the ρ_E-action. Since π_E is a quotient of the Galois closure of the *simple* cover π, the ramification index of π_E at any maximal ideal $\mathfrak{n}$ of an affine coordinate ring of X_E divides 2 (Lemma 7). By definition of $\mu(\mathcal{E})$, there are $\mu(\mathcal{E})/2$ $\mathcal{O}_E$-primes $\mathfrak{n}$ above $\mathfrak{m}$ with $e(\mathfrak{n}/\mathfrak{m}) = 2$, thus for any $\mathfrak{m} \in B_\pi$, as $\mathfrak{n}$ runs through all maximal ideals of $\mathcal{O}_E$ lying above $\mathfrak{m}$, we have

$$\sum_{\mathfrak{n}/\mathfrak{m}} \big(e(\mathfrak{n}/\mathfrak{m}) - 1\big) f(\mathfrak{n}/\mathfrak{m}) \geq \mu(\mathcal{E})/2.$$

By Lemma 8(b), the branch locus of π_E is exactly B_π. Thus Riemann-Hurwitz gives

$$2(N_E - 1 + g_E) \geq \#B_\pi \times \mu(\mathcal{E})/2. \tag{35}$$

Suppose $g_E \leq 1$. Then (35) and (34) together give

$$\mu(\mathcal{E}) \leq 2N_E/(n + g_Y - 1) \leq 2N_E/(n-1) \tag{36}$$

Recall that ρ_E is transitive, and since $\mathcal{E}$ is maximal, [7, Cor. 1.5A] implies that ρ_E is primitive as well. By [21, Thm. 6.1], either

- $\mu(\mathcal{E}) \geq N_E/2$, or
- S_n contains a normal subgroup isomorphic to H^r, where H is isomorphic to an alternating group A_m for some m, or to a simple group of Lie type over $\mathbf{Z}/2$.

The first option plus (36) implies that $n \leq 4$ for $g_Y \geq 1$ and $n \leq 5$ for $g_Y = 0$, and we are done. Since $n \geq 5$, for the second option we must have $m = n, r = 1$ and $H \simeq A_n$. Furthermore, [21, Thm. 6.1] says that, in this case, ρ_E is in fact the action of S_n on the set of j-subsets of $\{1, \ldots, n\}$ for some $j \in [1, n/2]$, whence $N_E = \binom{n}{j}$, and $\mu(\mathcal{E}) = 2\binom{n-2}{j-1}$. Recall (36) and we get

$$2\binom{n-2}{j-1} \leq \frac{2}{n + g_Y - 1}\binom{n}{j}. \tag{37}$$

This inequality simplifies to $j(n-j) \leq n(n-1)/(n+g-1)$. Since $n \geq 5$, this is only possible if $g_Y \leq 1$ and $j = 1$. Thus, $g_E \geq 2$ for all maximal subgroups $\mathcal{E}$ of G_λ not conjugate to $S_{n,1}$.

Parts (b) and (c) follow immediately from the claim. Indeed, the hypothesis there, namely $g_{K_1} > 1$, ensures that the genus of *every* minimal subfield of K'/K_0 is at least 1. Now we can apply Proposition 1 and Theorem 3 to complete the proof. For part (a), it remains only to combine the claim with Proposition 2. □

Second Proof. Now we give a slightly different approach which is independent of Liebeck-Saxl. Fix $j \in [1, n/2]$ and suppose $\lambda(x, \alpha)$ has a K-rational degree j factor for infinitely many $\alpha \in K$. Then Proposition 2 implies that $g(X_j) \leq 1$. But the function field of X_j is the fixed field $E = K_j$ of $\mathcal{E} = S_{n,j}$, so by Lemma 11 (recall the notation introduced at the beginning of subsection 5.2), we have reduced again to the case where ρ_E is the action of G_λ on the set of j-subsets of $\Sigma = \{\lambda_1, \ldots, \lambda_n\}$. Repeat the argument arising from (37) and we get $g_Y \leq 1$ and $j = 1$, from which Parts (a) and (b) of the Theorem follow. To prove (c), assuming now that $g_Y \geq 2$, and $n \geq 7$, we have already seen that the fixed field of the *intransitive* maximal subgroups $S_{n,j}$ have genus at least 2. Now we consider a *transitive* maximal subgroup $\mathcal{E}$ of G_λ. By [30, Lem. 4.4.4], the only transitive subgroup of S_n that contains a 2-cycle is S_n, so we may assume $\mathcal{E}$ has no transpositions. Recalling that $\#B_\pi = 2g + 2n - 2$, (4) and (10) combine to give $g(X_E) > 1$ in this case as well. Now we can apply Theorem 3 to conclude the proof. □

Remark 7. The argument above plus Theorem 3 shows that if $g_Y \geq 2$ then the Galois group of $\lambda(x, \alpha)$ has order divisible by 60 (if $n = 6$) and by 20 (if $n = 5$) for $\alpha \in_{\mathrm{af}} K$. We do not know if the Galois groups are in fact S_6 and S_5, respectively, for $\alpha \in_{\mathrm{af}} K$.

Acknowledgments. We are grateful to Professor Müller for pointing out an error in the final section of an earlier draft, and for showing us the first proof of Theorem 4. We would also like to thank Professors Boston, Cox, Gunnells and Markman for useful discussions.

References

[1] E. Artin, *The gamma function*. Holt, Rinehart and Winston, 1964.

[2] G. Butler and J. McKay, The transitive subgroups of degree up to eleven. *Comm. in algebra* **11** (1983) 863-911.

[3] J. H. Conway *et al.*, *Atlas of finite groups : maximal subgroups and ordinary characters for simple groups*. Oxford, 1985.

[4] D. Cox, *Primes of the form* $x^2 + ny^2$. Wiley, 1989.

[5] C. J. Cummins and S. Pauli, Congruence subgroups of $PSL(2, \mathbf{Z})$ of genus less than or equal to 24. *Exper. Math.* **12** (2003) 243-255.

[6] P. Dèbes and M. D. Fried, Integral specialization of families of rational functions. *Pacific J. Math.* **190** (1999) 45-85.

[7] J. D. Dixon and B. Mortimer, *Permutation groups*. Springer-Verlag, 1996.

[8] D. Dummit, Solving solvable quintics. *Math. Comp.* **57** (1991) 387-401.

[9] W. Feit, $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields. *J. Algebra* **104** (1986) 231-260.

[10] M. Fried, On Hilbert's irreducibility theorem. *J. Number Theory* **6** (1974) 211-231.

[11] W. Fulton, Hurwitz schemes and irreducibility of moduli of algebraic curves. *Ann. Math.* **90** (1969) 542-575.

[12] M. Filaseta and O. Trifonov, The irreducibility of the Bessel polynomials. *J. Reine Angew. Math.* **550** (2002) 125-140.

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

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

[15] F. Hajir, Some $\tilde{A}_n$-extensions obtained from generalized Laguerre polynomials. *J. Number Theory* **50** (1995) 206-212.

[16] F. Hajir, Algebraic properties of a family of generalized Laguerre polynomials, *preprint*, 17pp.

[17] M. Hall, *The theory of groups*. Macmillan, 1959.

[18] J. B. Dennin, Jr., The genus of subfields of $K(n)$. *Proc. A.M.S.* **51** (1975) 282-288.

[19] M. I. Knopp and M. Newman, Congruence subgroups of positive genus of the modular group. *Ill. J. Math.* **9** (1965) 577-583.

[20] S. Lang, *Elliptic functions*, 2nd ed. Springer-Verlag, 1987.

[21] M. W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc.* **63** (1991) 266-314.

[22] A. M. Macbeath, Extensions of the rationals with Galois group $\mathrm{PGL}(2, \mathbf{Z}_n)$. *Bull. London Math. Soc.* **1** (1969) 332-338.

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

[24] M. Rosen, *Number theory in function fields*. Springer-Verlag, 2002.

[25] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen. II. *Sitzungsberichte der Berliner Akademie* (1929) 370-391.

[26] I. Schur, Gleichungen ohne Affekt. *Sitzungsberichte der Berliner Akademie* (1930) 443-449.

[27] I. Schur, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome. *J. reine und angew. Math.* **165** (1931) 52-58.

[28] E. Sell, On a family of generalized Laguerre polynomials, To appear in *J. Number Theory*, 13pp.

[29] J. P. Serre, *Lectures on the Mordell-Weil theorem*, 2nd ed. Vieweg, 1990.

[30] J. P. Serre, *Topics in Galois theory*. Jones and Bartlett Publ., 1992.

[31] J. H. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[32] H. Volklein, *Groups as Galois groups : an introduction*. Cambridge University Press, 1996.

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

Department of Mathematics & Statistics, University of Massachusetts. Amherst, MA 01003-9318 USA

E-mail address: `siman@math.umass.edu`

Department of Mathematics & Statistics, University of Massachusetts. Amherst, MA 01003-9318 USA