REDUCIBLE SPECIALIZATIONS OF POLYNOMIALS: THE NONSOLVABLE CASE

JOACHIM KÖNIG AND DANNY NEFTIN

Abstract. Given an irreducible polynomial $F \in \mathbb{Q}(t)[x]$, we develop methods for determining the set of exceptions in Hilbert's irreducibility theorem up to a finite set, under nonsolvability assumptions on its Galois group $A = \mathrm{Gal}(F/\mathbb{Q}(t))$. As opposed to previous results, these methods address the case where A is imprimitive. As a consequence, we answer the Davenport–Lewis–Schinzel problem (1959), and the problem of determining the reducibility of fibers of a polynomial $f \in \mathbb{Q}[x]$ over rational points (1971), when the involved polynomials do not factor through x^n, a Chebyshev polynomial, and an indecomposable degree 4 polynomial.

1. Introduction

1.1. **Background.** Reducibility of polynomials, varying through an algebraic family, is a key property in arithmetic geometry appearing at the heart of the Inverse Galois Problem [55], construction of elliptic curves of large rank [45], the solution of Pisot's d-th root conjecture [56], and many other problems. Moreover, the reducibility of separated polynomials $f(x) - g(y) \in \mathbb{Q}[x, y]$ plays a key role in studying the rational points on components of the associated curves $f(x) = g(y)$ [3, 7, 46, 14], a problem with a wide range of applications including to functional equations [48, 18, 42], dynamics [25], and complex analysis [47].

Hilbert's irreducibility theorem [30] asserts in its basic version that, given an irreducible polynomial $F(t, x) \in \mathbb{Q}(t)[x]$, viewed as a family of polynomials that depends on a parameter t, the specialized polynomial $F(t_0, x) \in \mathbb{Q}[x]$ is irreducible for "most" values $t_0 \in \mathbb{Q}$. More precisely, letting $\mathrm{Red}_F = \mathrm{Red}_F(\mathbb{Q})$ denote the set of values $t_0 \in \mathbb{Q}$ where $F(t_0, x)$ is defined and reducible, Hilbert's theorem asserts that Red_F is "thin" [53, §3], that is, up to a finite set[1], it is the union of finitely many value sets $h_i(Y_i(\mathbb{Q}))$ of coverings $h_i : Y_i \to \mathbb{P}^1$ over $\mathbb{Q}$, $i \in I$. However, an explicit description of the infinite value sets $h_i(Y_i(\mathbb{Q}))$ is far from known. In particular, the following are two long standing open problems:

The first is the *fiber reducibility problem* that seeks to determine over which rational values the fiber of $f \in \mathbb{Q}[x]$ is reducible over $\mathbb{Q}$. Equivalently, the problem seeks to

[1] Note that trying to determine the concrete finite set of exceptions would be hopeless for general F, since it would correspond to determining the complete set of rational points for arbitrary curves.

determine the reducibility of $f(x)$ upon varying its free coefficient. More precisely, setting $F(t,x) = f(x) - t \in \mathbb{Q}(t)[x]$, find (explicit) coverings $h_i : Y_i \to \mathbb{P}^1$, $i \in I$ over $\mathbb{Q}$, such that Red_F and the union of the value sets $h_i(Y_i(\mathbb{Q}))$, $i \in I$, differ by a finite set. For example, when $f(x) = x^2$, one has $F(t,x) = x^2 - t$ and, up to including ∞, the set $\mathrm{Red}_F = \mathbb{Q}^2$ is the value set of the covering $f : \mathbb{P}^1 \to \mathbb{P}^1$ given on an affine chart by $f(x) = x^2$.

In the setting of integral specializations, this problem was first studied by Fried [17, 19, 20], cf. [40], showing that $\mathrm{Red}_F \cap \mathbb{Z}$ is the union of the single value set $f(\mathbb{Q}) \cap \mathbb{Z}$ with a finite set, given that f is indecomposable and[2] $\deg f > 5$. Here, a covering $f : X \to \mathbb{P}^1$ (and in particular a polynomial $f \in \mathbb{Q}[x]$) is indecomposable if in every decomposition $f = g \circ h$, either $\deg g = 1$ or $\deg h = 1$.

The fiber reducibility problem also arises in dynamics in the context of eventual stability, arboreal representations, and newly reducible values, cf. [6, §19, §5],[32]. However, it is unknown for which integers $m = m_f \geq 2$ there exists (resp. exist infinitely many) $a \in \mathbb{Q}$ over which the *m-th iterate* $f^{\circ m}$ of f is *newly reducible*, that is, the fiber of $f^{\circ(m-1)}$ over a is irreducible over $\mathbb{Q}$, but the fiber of $f^{\circ m}$ is reducible over $\mathbb{Q}$. Finally, the problem also arises in the context of a prime number theorem in short intervals for function fields [5] as the latter can be viewed as studying the irreducibility of a polynomial upon changing only few of its coefficients. Although studied in various contexts, the fiber reducibility problem remains widely open for decomposable polynomials.

The second problem is the so called *Davenport–Lewis–Schinzel (DLS)* problem which originates in the late 50's [49, 50, 9, 10] and seeks to determine the polynomials $f, g \in \mathbb{C}[x] \setminus \mathbb{C}$ for which $f(x) - g(y) \in \mathbb{C}[x,y]$ is reducible. A trivial case in which $f(x) - g(y)$ is reducible is when f and g have a nontrivial common left composition factor, that is, $f = h \circ f_1, g = h \circ f_2$ for $h, f_1, f_2 \in \mathbb{C}[x] \setminus \mathbb{C}$ with $\deg h > 1$. The problem is to show that this is the only case, up to an explicit list of exceptions. In the case where at least one of f and g is indecomposable, the problem is solved by Fried [16], who gives the possible ramification of f and g. The polynomials themselves are then determined by Cassou-Noguès–Couveignes [8], and more recent progress is described in [4, Theorem 3 and §3], and [21, 24].

Although the DLS problem plays a key role in studying the set of rational points on separated curves $f(x) = g(y)$, the latter problem is more tractable due the implied genus constraints on the curve. As pointed out in [21], although many problems from Schinzel's list [50] have been solved, the DLS problem stands out, and decomposable polynomials are the source of the challenge [21, §7.4.3].

The polynomials $F(t,x) = f(x) - t \in \mathbb{Q}(t)[x]$, which play a central role in the above problems, define (geometrically irreducible smooth projective) curves X_F: $F(t,x) =$

[2] Moreover, counterexamples to this assertion with $\deg f = 5$ were given by Dèbes and Fried [11].

0, of genus 0, whose natural projection $X_F \to \mathbb{P}^1$ to the t-coordinate is given by f. To put these problems in the general setting of absolutely irreducible polynomials $F \in \mathbb{Q}(t)[x]$, consider a curve X_F: $F(t,x) = 0$, of fixed genus $g_{X_F} = g$, and let $n = \deg_x F$ be its degree in x. Furthermore, let $f : X_F \to \mathbb{P}^1$ be the natural projection to the t-coordinate, and $\mathrm{Mon}(f) := \mathrm{Gal}(F, \mathbb{Q}(t))$ its monodromy group viewed as a subgroup of S_n.

In this setting, an extensive study of the set $\mathrm{Red}_F \cap \mathbb{Z}$ was led by Müller [38, 39] who shows, among other results, that $\mathrm{Red}_F \cap \mathbb{Z}$ is finite for $g > 0$ when f is general, that is, $\mathrm{Mon}(f) = S_n$ (in which case f is indecomposable). Further progress in understanding the the entire set Red_F has been made using the vast classification of primitive monodromy groups led by Guralnick [29, 28, 43]: For indecomposable f of sufficiently large degree, the set Red_F differs from the value set $f(X_F(\mathbb{Q}))$ only by a finite set, unless the ramification of f is in an explicit list. However, since the methods underlying the above results are rooted in the structure theory of primitive groups, new methods are required to deal with imprimitve monodromy groups, or equivalently with decomposable coverings f.

1.2. **Main results.** This paper develops the craved method for dealing with decomposable coverings $f = f_1 \circ \cdots \circ f_r$ when the monodromy groups of f_i, $i = 1, \ldots, r$ are nonsolvable. This answers the fiber reducibility problem when $f \in \mathbb{Q}(t)[x]$ has no composition factor which, up to composition with linear polynomials, is x^n, or the (normalized) Chebyshev polynomial T_n, or is indecomposable of degree 4. Here, $T_n \in \mathbb{Z}[x]$ is the degree n polynomial satisfying $T_n(x + 1/x) = x^n + 1/x^n$ for $n \in \mathbb{N}$.

Theorem 1.1. *Let $F(t,x) = f(x) - t \in \mathbb{Q}(t)[x]$ where $f = f_1 \circ \ldots \circ f_r$ for indecomposable $f_i \in \mathbb{Q}[x]$, $i = 1, \ldots, r$ of degree ≥ 5, none of which equals $\mu_1 \circ x^n \circ \mu_2$ or $\mu_1 \circ T_n \circ \mu_2$, for $n \in \mathbb{N}$ and linear $\mu_1, \mu_2 \in \mathbb{C}[x]$. Assume further that $\deg f_1 > 20$. Then Red_F is either the union of $f_1(\mathbb{Q})$ with a finite set, or f_1 is as in Table 1.*

In both cases, Red_F is the union of $\mathrm{Red}_{f_1(x)-t}$ and a finite set.

A surprising part of Theorem 1.1 is that given that the first polynomial $f_1(x) - t_0 \in \mathbb{Q}[x]$ is irreducible, it follows that the rest of the compositions $f_1 \circ \cdots \circ f_i(x) - t_0 \in \mathbb{Q}[x]$, $i = 1, \ldots, r$ remain irreducible for all but finitely many $t_0 \in \mathbb{Q}$. In particular for $m > 1$, it follows that the iterate $f^{\circ m}$ is newly reducible only over finitely many values $a \in \mathbb{Q}$. The assumption $\deg(f_1) > 20$ can be removed at the account of a longer list of exceptions, see Remark 5.3. However, different methods are required when f_i, $i = 1, \ldots, r$ are allowed to be the composition of x^n or T_n with linear polynomials, that is, when $\mathrm{Mon}(f_i)$, $i = 1, \ldots, r$ are allowed to be solvable. Moreover, in such cases Red_F may consist of more than one infinite value set, see Example 2.5.

We also give the following answer to the DLS problem when one avoids composition factor of the form x^n, T_n, and indecomposable degree 4 polynomials:

Theorem 1.2. *Let $f, g \in \mathbb{C}[x]$ be nonconstant polynomials. Assume that $f = f_1 \circ \ldots \circ f_r$ for indecomposable $f_i \in \mathbb{C}[x]$ of degree ≥ 5, none of which is $\mu_1 \circ x^n \circ \mu_2$ or $\mu_1 \circ T_n \circ \mu_2$, for $n \in \mathbb{N}$ and linear $\mu_1, \mu_2 \in \mathbb{C}[x]$. Assume further that $\deg f_1 > 31$. Then $f(x) - g(y) \in \mathbb{C}[x, y]$ is reducible if and only if $g = f_1 \circ g'$ for some $g' \in \mathbb{C}[x]$.*

Note that the common composition factor of f and g necessarily factors through f_1 since, for f_i's as above, the decomposition $f = f_1 \circ \cdots \circ f_r$ is unique, up to composition with linear polynomials by Ritt's theorem, cf. Remark 2.16.

We note that in combination with the monodromy classification, these results are expected to extend more generally to (geometrically irreducible) polynomials $F(t, x)$ defining a curve X_F of fixed genus $g_{X_F} = g$, when the natural projection $f : X_F \to \mathbb{P}^1$ is a composition $f_1 \circ \ldots \circ f_r$ of geometrically indecomposable coverings $f_i : X_i \to X_{i-1}$ of sufficiently large degree, that is, larger than a constant depending only on g.

Finally, when the genus of X_F is arbitrary, and not fixed in advance, quite general "Ritt" decompositions $f = f_1 \circ \cdots \circ f_r$ are possible. Consequently, every indecomposable factor f_i in a decomposition $f = f_1 \circ \cdots \circ f_r$ may contribute an infinite value set, and even two such sets in exceptional cases. Still, for coverings $f_1, \ldots, f_r$ with alternating or symmetric monodromy, we can effectively bound the number of infinite value sets in Red_F:

Theorem 1.3. *There exists $N > 0$ with the following property. Let $f : X_F \to \mathbb{P}^1_{\mathbb{Q}}$ be the projection to t-coordinates from the curve $F(t, x) = 0$ over $\mathbb{Q}$. Suppose that $f = f_1 \circ \cdots \circ f_r$ for geometrically indecomposable coverings f_i of degree $n_i \geq N$, and of monodromy group A_{n_i} or S_{n_i}, $i = 1, \ldots, r$. Then there exists a number field[3] k such that, up to a finite set, $\mathrm{Red}_F(k)$ is the union of at most $2r$ value sets $h_j(Y_j(k))$, $j = 1, \ldots, 2r$ of coverings $h_j : Y_j \to \mathbb{P}^1_k$.*

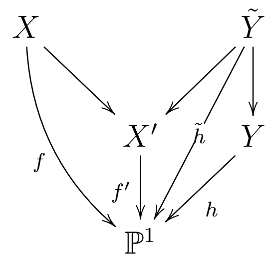
We furthermore show that, up to a finite set, $\mathrm{Red}_F(k)$ equals the union of sets $\mathrm{Red}_G(k)$, where the curves $G(t, x) = 0$, defined by $G \in k(t)[x]$, run through all minimal subcovers of f. These minimal subcovers, and hence the coverings h_j admit a rather explicit description, so that the pullbacks of at most two of the coverings h_j have the same Galois closure as f_i, for each i. The bound $2r$ is in fact sharp, but for typical compositions $f = f_1 \circ \cdots \circ f_r$, the number of infinite values sets in Red_F is at most 1. See Theorem 5.4 for the more complete result, and Remark 5.5 for its expected extensions.

1.3. **Methods.** The underlying problem in determining the set Red_F, up to a finite set, is finding the minimal coverings $h : Y \to \mathbb{P}^1$ of genus ≤ 1 whose fiber product with the projection $f : X_F \to \mathbb{P}^1$ is reducible. Such coverings are necessarily subcovers of the Galois closure $\tilde{f}$ of f, that is, $\tilde{f} = h \circ h'$ for some covering h', by Lemma

[3]In fact $k = \mathbb{Q}$ by upcoming results on arithmetic monodromy groups, cf. Remark 5.5.(1).

2.9. The crux in proving the above theorems is relating the genus ≤ 1 subcovers $h : Y \to \mathbb{P}^1$ of $\tilde{f}$ of nonsolvable monodromy, to the composition factors f_i of f:

Theorem 1.4. *Suppose $f : X \to \mathbb{P}^1$ is a covering with decomposition $f = f_1 \circ \cdots \circ f_r$ for indecomposable coverings $f_i : X_i \to X_{i-1}$ with nonsolvable monodromy groups whose proper quotients are solvable. Suppose $h : Y \to \mathbb{P}^1$ is a minimal subcover of $\tilde{f}$ with nonsolvable monodromy group whose proper quotients are solvable. Then there exists an indecomposable subcover f' of f having the same Galois closure as h.*



The theorem is applicable far more widely than in the above results since it makes no genus assumptions on Y, no reducibility assumptions on the fiber product of h and f, and its stronger version, Theorem 4.1, applies also when the monodromy groups of f_i, $i = 1, \ldots, r$ are allowed to be solvable.

The condition on $\mathrm{Mon}(h)$ to be nonsolvable with solvable proper quotients holds for coverings h that decompose as $h_1 \circ \cdots \circ h_s$ for indecomposable $h_i : Y_i \to Y_{i-1}$ with solvable $\mathrm{Mon}(h_i)$, $i = 1, \ldots, s-1$, and nonsolvable $\mathrm{Mon}(h_s)$ whose proper quotients are solvable, see Lemma 3.7. In particular, the above condition holds under the genus constraint $g_{Y_s} \leq 1$ when $\mathrm{Mon}(h_s)$ is not affine, cf. Lemma 3.10.

The proof of Theorem 1.4 is of group theoretic nature, and rests on a tool kit, developed in Section 3, for studying the monodromy groups of arbitrary length decompositions of coverings f under composition. In particular we provide a new relation between normal subgroups of $\mathrm{Mon}(f)$ and such decompositions, see Lemma 3.4. The combination this relations with Ritt's theorems provides new insight on the structure of $\mathrm{Mon}(f)$ for decomposable f.

By combining the above group theoretic results with Ritt's theorem, and Burnside's theorem on doubly transitive groups with a full cycle, we reduce Theorems 1.1 and 1.2 to determining the genus ≤ 1 subcovers of the Galois closure of the first indecomposable subcover f_1 of f, see Theorem 5.1. It is only in this final step of the proof we apply the primitive monodromy classification theorems for polynomials by Feit and Müller [36], and Guralnick–Shareshian [28], see Corollary 5.2 and the proof of Theorem 1.2. Similarly, in the final step of the proof of Theorem 1.3, we apply the classification of monodromy groups of low genus coverings [43, 44].

The second author was supported by the Israel Science Foundation (grant No. 577/15) and the U.S.-Israel Binational Science Foundation (grant No. 2014173). All computer computations were carried out using Magma.

2. Preliminaries

We start with setting up the relation between coverings, function fields, and groups in Sections 2.1 - 2.7. Sections 2.8-2.10 recall arithmetic preliminaries. Section 2.3 and the classification results from Sections 2.8-2.10 are used only in Section 5.

2.1. **Coverings.** Let k be a field of characteristic 0, and $\overline{k}$ its algebraic closure. An (irreducible branched) *covering* $f : X \to Y$ over k is a morphism of (smooth irreducible projective) curves defined over k. Note that as X may be geometrically reducible (i.e., reducible over $\overline{k}$), and the morphism $f \times_k \overline{k}$ obtained by base change from k to $\overline{k}$ may not be a covering over $\overline{k}$. A covering h is called a *subcover* of f if $f = h \circ h'$ for some covering h'. A covering f defines a field extension $k(X)/k(Y)$ via the injection $f^* : k(Y) \to k(X), h \mapsto h \circ f$. Two coverings $f_i : X_i \to Y$, $i = 1, 2$ over k are called (k-)equivalent if there exists an isomorphism $\mu : X_1 \to X_2$ (over k) such that $f_1 \circ \mu = f_2$. Note that for two k-equivalent coverings, one has $f_1(X_1(k)) = f_2(X_2(k))$ and hence we may consider the value set of a k-equivalence class of coverings.

Recall that there is a correspondence between equivalence classes of coverings of $\mathbb{P}^1_k$ and finite field extensions of $k(t)$, up to $k(t)$-isomorphisms, cf. [12, Section 2.2]. In particular, letting $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ denote the covering corresponding to the Galois closure Ω of $k(X)/k(t)$, there is a correspondence between equivalence classes of subcovers $h : Y \to \mathbb{P}^1_k$ of $\tilde{f}$ and subgroups $D \leq A := \mathrm{Gal}(\Omega/k(t))$. Namely, to every such subcover the correspondence associates a subgroup $D \leq A$ (unique up to conjugation) such that h is equivalent to a covering $f_D : \tilde{X}/D \to \mathbb{P}^1_k$ whose composition with the natural projection $\tilde{X} \to \tilde{X}/D$ is $\tilde{f}$.

By the *genus* of X, we mean the genus of a geometrically irreducible component of X. Note that since $\overline{k}/k$ is Galois, it is independent of the choice of the component.

2.2. **Monodromy.** Let $f : X \to \mathbb{P}^1_k$ be a geometrically irreducible covering over k. Letting Ω denote the Galois closure of $k(X)/k(t)$, the *arithmetic (resp. geometric) monodromy group* $A = \mathrm{Mon}_k(f)$[4] (resp. $G = \mathrm{Mon}_{\overline{k}}(f)$) of f is the Galois group $\mathrm{Gal}(\Omega/k(t))$ (resp. $\mathrm{Gal}(\overline{k}\Omega/\overline{k}(t))$) equipped with its permutation action on A/A_1, where $A_1 = \mathrm{Gal}(\Omega/k(X))$. Note that since $\overline{k}(t)/k(t)$ is Galois, so is $k'(t)/k(t)$ for $k' = \overline{k} \cap \Omega$. Hence $G \lhd A$. Also note that f_D is geometrically irreducible if and only

[4]In cases where the base field is understood from the context, we shall simply write $\mathrm{Mon}(f)$.

if $\Omega^D/k(t)$ is linearly disjoint from $\overline{k}(t)$, or equivalently if $\Omega^D \cap k'(t) = k(t)$, that is, if $D \cdot G = A$.

Given a subgroup $C \leq G$, we say that the covering f_C (of $\mathbb{P}^1_{\overline{k}}$) is *defined* (resp. *uniquely defined*) over k if there exists a covering (resp. a covering unique up to k-equivalence) $f' : X' \to \mathbb{P}^1_k$ over k which is equivalent to f_C after base change to $\overline{k}$.

Remark 2.1. For a subgroup $C \leq G$, the covering $f_C : \tilde{X}/C \to \mathbb{P}^1$ is always defined over $k' = k \cap \Omega$. We claim that f_C is defined over k if and only if there exists $C \leq D \leq A$ such that $D \cap G = C$ and $DG = A$. Indeed as above, f_D is geometrically irreducible if and only if $DG = A$. Also, f_C is defined over k if and only if the extension $\Omega^C/k'(t)$ is defined over $k(t)$, that is, if there exists an intermediate field $k(t) \leq \Omega^D \leq \Omega^C$ for some $C \leq D \leq A$ such that $\Omega^D \cdot k'(t) = \Omega^C$ or equivalently $D \cap G = C$. Finally, f_C is furthermore uniquely defined if and only if the subgroup $D \leq A$, satisfying $D \cap G = C$ and $DG = A$, is unique up to conjugation in A.

Note that the assumption that f is geometrically indecomposable is equivalent to the maximality of $G_1 := A_1 \cap G$ in G, and hence to G acting primitively. For polynomials $f \in k[x]$, the monodromy group of the induced map $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$ is the Galois group of $f(x) - t \in k(t)[x]$, and one further has:

Remark 2.2. An indecomposable polynomial in $k[x]$ is indecomposable even over $\overline{k}$ by a theorem of Fried and MacRae [15]. We shall therefore call such a polynomial simply "indecomposable" without specifying the base field.

2.3. **Specializations.** Let $F \in k(t)[x]$ be an irreducible polynomial. In this section, we shall replace it by a polynomial $F \in k[t, x]$, by multiplying it with an element of $k(t)$. Note that this operation changes the reducibility of $F(t_0, x)$ only for the finitely many values $t = t_0$ which are zeros or poles of coefficients of F in $k(t)$.

We next recover a well known criterion for the reducibility of $F(t_0, x)$. Let Ω be the splitting field of F over $k(t)$, so that $A = \mathrm{Gal}(\Omega/k(t))$ is the arithmetic monodromy group of f. A well known fact from algebraic number theory [33, Lemma 2], asserts that for every $t_0 \in k$ which is neither a root nor a pole of the discriminant $\delta_F \in k(t)$ of F, the splitting field Ω_{t_0} of $F(t_0, x)$ is Galois, and its Galois group is identified as a permutation group with a subgroup $D \leq A$, unique up to conjugation, known as the decomposition group at t_0. Moreover, Ω^D has a degree 1 place P over t_0. In particular, $\Omega^D \cap \overline{k}(t) = k(t)$. Thus, Remark 2.1 implies that the corresponding morphism $f_D : X_D \to \mathbb{P}^1$ is a geometrically irreducible covering over k. The place P corresponds to a k-rational point $P \in X_D(k)$ such that $f_D(P) = t_0$. Since D and $\mathrm{Gal}(\Omega_{t_0}/k)$ are isomorphic as permutation groups, $F(t_0, x)$ is reducible if and only if D is intransitive. In total we have:

Proposition 2.3. *Let $F \in k(t)[x]$ be irreducible with splitting field Ω, and Galois groups A and G over $k(t)$ and $\overline{k}(t)$, respectively. Suppose $t_0 \in k$ is neither a root nor* *a pole of $\delta_F(t)$ and of the coefficients of F. Let $D = D_{t_0}$ be its decomposition group, and $f_D : X_D \to \mathbb{P}^1_k$ the covering corresponding to $\Omega^D/k(t)$. Then:*

1. *$t_0 \in f_D(X_D(k))$, and $DG = A$;*
2. *$F(t_0, x) \in k[x]$ is reducible if and only if D is intransitive.*

Since $F(t, x)$ is irreducible, the natural projection $f : X \to \mathbb{P}^1$ to the t-coordinate is a covering over k. For such a covering f, let $R_f = R_f(k)$ be the set of $t_0 \in k$ whose fiber is reducible over k. Note that R_f and Red_F agree up to a finite set.

Proposition 2.3 implies that R_f is the union of $\bigcup_D f_D(X_D(k))$ with a finite set, where $D \leq A$ runs over maximal intransitive subgroups with $DG = A$. If $X_D(k)$ is infinite and k is a finitely generated field, Faltings' theorem implies that the genus g_{X_D} is at most 1. Similarly if k is a number field with ring of integers O_k, and $f_D(X_D(k)) \cap O_k$ is infinite, then Siegel's theorem implies that f_D is a Siegel function, that is, $g_{X_D} = 0$ and ∞ has at most two preimages under f_D. We therefore have:

Corollary 2.4. *Let $f : X \to \mathbb{P}^1$ be a covering over a finitely generated field k with arithmetic (resp. geometric) monodromy A (resp. G). Then R_f and $\bigcup_D f_D(X_D(k))$ differ by a finite set, where D runs over maximal intransitive subgroups of A with $g_{X_D} \leq 1$ and $DG = A$.*

Similarly, if k is a number field and O_k is its ring of integers, then $R_f \cap O_k$ and $\bigcup_D (f_D(X_D(k)) \cap O_k)$ differ by a finite set, where D runs over maximal intransitive subgroups of A such that $DG = A$ and f_D is a Siegel function.

Example 2.5. Let $k := \mathbb{Q}(e^{2\pi i/8})$, and $F(t, x) := T_4(x) - t \in k(t)[x]$. We will show that (1) Red_F is the union of $f_1(\mathbb{Q}) \cup h(\mathbb{Q})$ with a finite set, where $f_1 : \mathbb{P}^1_k \to \mathbb{P}^1_k$ and $h : \mathbb{P}^1_k \to \mathbb{P}^1_k$ are given (on an affine chart) by $x \mapsto T_2(x)$ and $x \mapsto -T_4(x)$, respectively. Furthermore, (2) f_1 is the the unique indecomposable subcover of the natural projection $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$, $x \mapsto T_4(x)$ corresponding to F. Since f_1 is of degree 2, it is Galois, and hence h does not factor through f_1. As pointed out in Section 1, this shows that the nonsolvability assumption in Theorem 1.1 is necessary.

To show (1) and (2), first note that the Galois closure of f is the covering $\tilde{f} : \tilde{X} \to \mathbb{P}^1$ by $\tilde{X} \cong \mathbb{P}^1_k$ given by $x \mapsto (x + 1/x)^4$, so that $\tilde{f} = f \circ (x + 1/x)$. The arithmetic and geometric monodromy groups A and G of f are the dihedral group D_4 of order 8 equipped with its standard degree 4 action. Let s be the automorphism of $\tilde{X}$ given by $x \mapsto 1/x$, so that f is equivalent to the subcover $f_s : \tilde{X}/\langle s\rangle \to \mathbb{P}^1_k$. We next deduce (1) and (2) from:

Claim 2.6. h is equivalent to the covering $f_{sr} : \tilde{X}/\langle sr\rangle \to \mathbb{P}^1_k$.

By Corollary 2.4, it suffices to find the maximal intransitive subgroups $D \leq A$ for which $g_{X_D} \leq 1$ and $DG = A$. However, since $\tilde{X}$ is of genus 0 and $G = A$, the last two conditions are immediate. Up to conjugacy the maximal intransitive subgroups of D_4 are $\langle sr\rangle$, and $\langle s, r^2\rangle$. Since $U := \langle s, r^2\rangle$ is the only intermediate subgroup $\langle s\rangle \leq U \leq D_4$, we deduce that f_U is equivalent to f_1, showing that (1) follows from Claim 2.6. Since the only proper subgroup of D_4 which contains $\langle sr\rangle$ is $\langle sr, r^2\rangle$ which is not conjugate to U, (2) follows.

It remains to prove Claim 2.6. Note that the composition $\hat{f} := T_2 \circ \tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ is a Galois covering with arithmetic monodromy group D_8 containing $A = D_4$ as a subgroup. Since $sr \in A$ and $s \in A$ are conjugate in D_8, the coverings $T_2 \circ f_{sr}$ and $T_2 \circ f_s$ are equivalent. Since the latter is given by $x \mapsto T_8(x) = T_2 \circ T_4(x)$, the covering f_{sr} is given either by $x \mapsto T_4(x)$, or by $x \mapsto -T_4(x)$. Since $\langle sr\rangle$ and $\langle s\rangle$ are not conjugate in A, f_{sr} is not equivalent to f_s, and hence is given by $x \mapsto -T_4(x)$.

For an example over $\mathbb{Q}$, see [22, §2],[23, Chp. 13, Ex. 1]. To check that a covering $f_D : \tilde{X}/D \to \mathbb{P}^1$ is defined over k, we shall use:

Remark 2.7. Let $f : X \to \mathbb{P}^1$ be a covering over k with arithmetic and geometric monodromy groups A and G, and point stabilizers A_1 and $G_1 = A_1 \cap G$, respectively. Assume that A decomposes as $A = G \rtimes B$ with a complement $B \leq A_1$. We claim that $f_C : \tilde{X}/C \to \mathbb{P}^1$ is defined over k for every maximal intransitive subgroup $C \leq G$ normalized by B.

The claim follows from Remark 2.1, noting that C is contained in an intransitive subgroup $D := CB \leq A$ satisfying $DG = A$ and $D \cap G = C$. Indeed, D is a subgroup since $CB = BC$, and it is intransitive since the inequality $CG_1 \neq G$ implies that

$$DA_1 = CBA_1 = CA_1 \not\supseteq G.$$

2.4. **Fiber products and pullbacks.** Let $\tilde{f} : \tilde{X} \to Y$ be a Galois covering over k with arithmetic monodromy group A. Let $A_1, H \leq A$ be subgroups and $f_{A_1} : \tilde{X}/A_1 \to Y$ and $f_H : \tilde{X}/H \to Y$ the corresponding coverings, respectively. Setting $X := \tilde{X}/A_1$ and $Z := \tilde{X}/H$, we denote by $X\#Z$ the (normalization of the) *fiber* product of f_{A_1} and f_H.

Remark 2.8. The irreducibility of $X\#Z$ is equivalent to the linear disjointness of the function fields $k(X)$ and $k(Z)$ over $k(Y)$, which in turn is equivalent to the transitivity of H on A/A_1, that is, $HA_1 = A$. When these conditions hold, the natural projection $X\#Z \to Y$ is equivalent to the covering $f_{H\cap A_1} : \tilde{X}/(H \cap A_1) \to Y$.

Lemma 2.9. *Let $f : X \to Y$ and $h : Z \to Y$ be coverings with reducible fiber product. Then $f = f_0 \circ f_1$ where f_0 is a subcover of the Galois closure $\tilde{h}$ whose fiber product with h is reducible.*

Proof. Let $g : Z \to Y$ be a common Galois closure for f and h, let A be its (arithmetic) monodromy group, and assume $f \sim g_U$, $h \sim g_V$, and $\tilde{h} \sim g_N$ for $U, V, N \leq A$ with $N = \mathrm{core}_A(V) \lhd A$. Since the fiber product of f and h is reducible,

$UV \neq A$. Since $N \lhd A$, the set UN is a group, and as $U \leq UN$, f factors through $f_0 := g_{UN} : Z/(UN) \to Y$. Since $UN \leq UV < A$, we have $\deg f_0 > 1$. Since $UN \cdot V = UV < A$, the fiber product of f_0 and h is reducible. □

The *pullback* of f along h is the natural projection $f_h : W \to Z$ from $W := X\#Z$.

Remark 2.10. Assume that $W = X\#Z$ is irreducible, and let $\tilde{f}_h : \tilde{W} \to Z$ be the Galois closure of f_h, and $\Gamma = \mathrm{Mon}_k(f_h)$. Then we shall identify Γ with a subgroup of A via the following embedding. Since $k(W)$ is the compositum of $k(X)$ and $k(Z)$ by Remark 2.8, the Galois closure Ω_W of $k(W)/k(Z)$ is the compositum of the Galois closure Ω_X of $k(X)/k(Y)$ with $k(Z)$. Thus $\Gamma = \mathrm{Gal}(\Omega_W/k(Z))$ is isomorphic, via restriction, to $\mathrm{Gal}(\Omega_X/\Omega_X \cap k(Z)) \leq A$.

2.5. **Primitive groups.** We describe the structure theory of finite primitive groups, following [2] and [26]. Assume U is a finite primitive group and denote by $\mathrm{soc}(U)$ the socle of U, that is, the product of minimal normal subgroups of U. In the case where $\mathrm{soc}(U)$ is abelian, also known as the affine case, one has

(A) $\mathrm{soc}(U)$ is the unique minimal normal subgroup of U, is isomorphic to an elementary abelian subgroup $\mathrm{soc}(U) \cong \mathbb{F}_p^d$ for some prime p, and the action of U on $\mathbb{F}_p^d$ by conjugation is irreducible.

Otherwise, $\mathrm{soc}(U) \cong L^t$, where L is a nonabelian simple group. Moreover, either:

(B) $\mathrm{soc}(U) \cong Q \times R$, where Q and R are isomorphic, and are the only minimal normal subgroups of U; or

(C) $\mathrm{soc}(U) \cong L^t$ is the unique minimal normal subgroup of U.

We shall describe subgroups of L^t according to their projections using [2, (1.4)]:

Lemma 2.11. *Let L be a finite nonabelian simple group, I a finite set, and K a subgroup of L^I which surjects onto L under each projection $\pi_i : K \to L$ to the i-th component for all $i \in I$. Then K decomposes as $(K \cap L^{O_1}) \times \cdots \times (K \cap L^{O_r})$ where $O_1, \ldots, O_r$ is a partition of I, and $K \cap L^{O_j} \cong L$ for all $j = 1, \ldots, r$.*

Finally, we also use the following version of Goursat's lemma [34, Corollary 1.4]:

Lemma 2.12. *Let $G = A \times B$ be a product of two finite groups, and assume the center of each quotient of A is trivial. Then every normal subgroup $N \lhd G$ is of the form $N = (N \cap A) \times (N \cap B)$.*

2.6. **Wreath products.** Let $f : X \to \mathbb{P}^1, h : Y \to X$ be two coverings over k, of degrees m, n and monodromy groups U, V with point stabilizers U_1, V_1, respectively. It is well known that the monodromy group A of $h \circ f$ is naturally a subgroup of the wreath product $U \wr_J V := U^J \rtimes V$, where the semidirect product action of $V \leq S_J$ is given by permuting the J-copies of U. The action of A is the the natural imprimitive degree $m \cdot n$ action of $U \wr_J V$.

We note two further properties of such monodromy groups $A \leq U \wr_J V$. Letting Ω_X denote the Galois closure of $k(X)/k(\mathbb{P}^1)$, the restriction map surjects onto $V = \mathrm{Gal}(k(X)/k(\mathbb{P}^1))$, that is, (1) the projection modulo U^J maps A onto V. Letting Ω denote the Galois closure of $k(Y)/k(\mathbb{P}^1)$ and $A_0 := A \cap (U^J \rtimes S_{J\setminus\{0\}})$ be the stabilizer of a block $0 \in J$, (2) A_0 maps onto U under the projection to the 0-th coordinate.

2.7. **Solvable actions.** For $H_0 \leq G$, we shall say that the action of G on G/H_0 is *solvable* if $G/\mathrm{core}_G(H_0)$ is a solvable group. For finite groups $H \leq G$, there exists a unique minimal subgroup $H \leq H_{sol} \leq G$ such that G/H_{sol} is solvable: For, the solvability of the action on G/H_1 and G/H_2 implies that of $G/(H_1 \cap H_2)$.

A covering is called solvable if its monodromy group is, otherwise nonsolvable.

2.8. **Ramification.** The *ramification type* of a covering $f : X \to \mathbb{P}^1$ at a point $P \in \mathbb{P}^1_{\overline{k}}$ is defined to be the multiset of ramification indices $\{e_f(Q/P) \mid Q \in f^{-1}(P)\}$, and the ramification type of f is the multiset of all ramification types over all branch points of f. The ramification type of a geometrically irreducible covering f over k is the ramification type of $f \times_k \overline{k}$.

2.9. **Polynomials.** A *polynomial* covering $f : \mathbb{P}^1 \to \mathbb{P}^1$ is a covering which satisfies $f^{-1}(\infty) = \{\infty\}$ over $\overline{k}$. In particular on the affine line it is given by a polynomial. The following theorem is the combination of [36] and [28, §1.2]:

Theorem 2.13. *Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be an indecomposable polynomial covering over $\overline{k}$, and $\tilde{f} : \tilde{X} \to \mathbb{P}^1$ its Galois closure. For every indecomposable subcover $h : Y \to \mathbb{P}^1$ of $\tilde{f}$ with genus $g_Y \leq 1$, one of the following holds:*

1. *h is equivalent to f.*
2. *f is one of the nine families of polynomials whose ramification is given in Table 1 with monodromy group $G = A_\ell$ or S_ℓ; and h is the degree $\ell(\ell-1)/2$ covering $\tilde{X}/G_2 \to \mathbb{P}^1$ where G_2 is the stabilizer of a set of cardinality* 2. *The ramification of the corresponding subcovers h is listed in* [43, Table 2]. *These do not correspond to Siegel functions.*
3. *The monodromy group of f is either* $\mathrm{P\Gamma L}_3(4)$ *or* $\mathrm{PSL}_5(2)$*, in their natural action of degree* 21 *and* 31*, resp. In each case, there is only one possible ramification type for f, and exactly one more subcover h of genus ≤ 1.* [5]
4. *f is of degree ≤ 20. The corresponding subcovers h with $10 \leq \deg h \leq 20$ are also listed in* [28, Theorem A.4.1].

[5] More precisely, h is of genus 0 and corresponds to the image of the point stabilizer under the graph automorphism. Explicit equations for f and h are given in [8].

Table 1. Ramification types of polynomial maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree $\ell > 20$ and monodromy group A_ℓ or S_ℓ for which the genus of the 2-set stabilizer is 0. Here $a \in \{1, \dots, \ell-1\}$ is odd, $(a, \ell) = 1$, and in each type ℓ satisfies the necessary congruence conditions to make all exponents integral.

$[\ell], [a, \ell-a], [1^{\ell-2}, 2]$
$[\ell], [1^3, 2^{(\ell-3)/2}], [1, 2^{(\ell-1)/2}], [1^{\ell-2}, 2]$
$[\ell], [1^2, 2^{(\ell-2)/2}]$ twice, $[1^{\ell-2}, 2]$
$[\ell], [1^3, 2^{(\ell-3)/2}], [2^{(\ell-3)/2}, 3]$
$[\ell], [1^2, 2^{(\ell-2)/2}], [1, 2^{(\ell-4)/2}, 3]$
$[\ell], [1, 2^{(\ell-1)/2}], [1^2, 2^{(\ell-5)/2}, 3]$
$[\ell], [1^3, 2^{(\ell-3)/2}], [1, 2^{(\ell-5)/2}, 4]$
$[\ell], [1^2, 2^{(\ell-2)/2}], [1^2, 2^{(\ell-6)/2}, 4]$
$[\ell], [1, 2^{(\ell-1)/2}], [1^3, 2^{(\ell-7)/2}, 4]$

Remark 2.14. 1) The mere conclusion that G is either solvable or a 2-transitive nonabelian almost simple group, and hence with primitive socle, is derived from more classical results. Indeed, due to results of Burnside, see [41], and Schur [51], any primitive group with a full cycle is known to be either solvable or 2-transitive; moreover, the minimal normal subgroup of a non-affine 2-transitive group is known to be simple and primitive due to Burnside [13, Theorem 7.2E].
2) The indecomposable polynomial coverings f with affine monodromy group G were essentially classified by Chisini and Ritt. It follows that the polynomials with solvable monodromy group G are equivalent either to x^n, or a Chebyshev polynomial, or an indecomposable degree 4 polynomial, see the proof of [31, Satz 5] or [36].
3) Let $A = \mathrm{Mon}_k(f)$. If $f \times_k \overline{k}$ is in case (3) of Theorem 2.13, then $A = G$. In case (2), either $A = G$ or $(A, G) = (S_n, A_n)$.

We next mention few further facts concerning decompositions of polynomials.

Remark 2.15. Writing $f = u \circ v$ for polynomial coverings u, v of degrees m, n, respectively, we note that the kernel of the natural projection from $\mathrm{Mon}(f) \leq S_n \wr S_m$ to $\mathrm{Mon}(u) \leq S_m$ is nontrivial. Indeed, letting $\tilde{u}$ be the Galois closure of u, Abhyankar's lemma implies that $e_{\tilde{u}}(Q/\infty) = m$ for every $Q \in \tilde{u}^{-1}(\infty)$. Since $e_f(\infty/\infty) = mn$, it follows that f is not a subcover of the Galois closure $\tilde{u}$ of u, and hence that the kernel of the above projection is nontrivial.

Remark 2.16. The decompositions of a polynomial $f \in k[x]$ into indecomposables $f_1 \circ \cdots \circ f_r$ are described by Ritt's theorems [48, 42]. In particular, these imply that if each f_i has nonsolvable geometric monodromy group, then this decomposition is unique up to composition with linear polynomials over $\overline{k}$. That is, for every decomposition $f = g_1 \circ \cdots \circ g_s$ into indecomposables, one has $s = r$ and $g_i = \mu_i \circ f_i \circ \mu_{i-1}$ for linear polynomials μ_i, $i = 1, \ldots, r$ with $\mu_0 = \mu_r = id$. Due to subsequent work of Fried and MacRae [15, Theorem 3.5], the linear polynomials may even be assumed to be over k.

2.10. **The classification of monodromy groups.** In the more general case of rational functions or large degree coverings $f : X \to \mathbb{P}^1$, we apply [28, 43, 44]:

Theorem 2.17. *For a fixed nonnegative integer g, there exists a constant N_g such that for every indecomposable covering $f : X \to \mathbb{P}^1$ over $\overline{k}$, of genus $g_X := g$, degree $n \geq N_g$, and nonsolvable monodromy group G, one of the following holds:*
(1) $G \in \{A_\ell, S_\ell\}$ with the natural action of degree $n = \ell$ or with the degree $n = \frac{\ell(\ell-1)}{2}$ action on 2-sets. For the latter, the ramification of f is given in [43, Table 4.2].
(2) $A_\ell^2 < G \leq S_\ell \wr C_2$ with the natural primitive action of degree $n = \ell^2$. The ramification of f is listed in [44, Table 3.1].

Remark 2.18. (a) Note that in case (1), the Galois closure $\tilde{f}$ admits at most two minimal nonsolvable subcovers of genus $\leq g$. In this case, the stabilizer of a 2-set acts intransitively in the natural action, which implies that the fiber product of the above two subcovers is reducible, cf. Remark 2.8.
In comparison, in case (2) there is only one *indecomposable* subcover of genus $\leq g$, but there may be three minimal nonsolvable subcovers of genus $\leq g$.

(b) Crossing the list in (1) with [37, Theorem 3.3], we see that in these cases the corresponding covering f is not a Siegel function if $G \in \{A_\ell, S_\ell\}$ and $n = \ell(\ell-1)/2$. Thus, given a large degree indecomposable Siegel function f with almost simple monodromy, every other nonsolvable Siegel function in its Galois closure factors through f.
(c) We note that this classification is expected to extend, in a subsequent work, to coverings over arbitrary fields of characteristic 0, with similar resulting monodromy.

The following follows from the monodromy classification in arbitrary degree:

Lemma 2.19. *Suppose $f : X \to \mathbb{P}^1_{\overline{k}}$ is an indecomposable covering with nonaffine monodromy group G. If $g_X \leq 1$, then G has a unique minimal normal subgroup* $\mathrm{soc}(G)$ *and $G/\mathrm{soc}(G)$ is solvable.*

Proof. Since G is assumed to be nonaffine, it is either of type (B) or (C). By [52], Type (B) does not occur with genus ≤ 1, so that we may assume G has a unique minimal normal subgroup. Thus by [29, Theorem C1] and [1], the only case in which $G/\mathrm{soc}(G)$ may be nonsolvable is the product type, that is, when G is isomorphic to a power L^t of a nonabelian simple group L and the point stabilizer of G intersects each copy of L nontrivially, also known as case (C3) following [29]. By [27, Theorem 7.1], when G is of product type case and $G/\operatorname{soc}(G)$, the genus ≤ 1 condition implies either that $G/\operatorname{soc}(G) \cong A_5$ acting as a genus 0 group in the natural action, or that $G/\operatorname{soc}(G) \cong S_5$ with ramification type $[2^{60}], [4^{30}], [5^{24}]$, and $G \leq S_\ell \wr S_5$ with $\ell \leq 10$. The first case is already ruled out by [27, Theorem 8.6], whereas a computer check shows that the second case does not occur with genus $g \leq 1$. □

Using Theorem 2.13 for polynomial coverings, and Theorem 2.17 for large degree coverings, Monderer–Neftin [35] obtain the following classification of (not necessarily indecomposable) low genus coverings with monodromy A_n or S_n. Let N_g be the constant from Theorem 2.17.

Lemma 2.20. *For every $g \geq 0$, and every degree $n > N_g$ covering (resp. degree $n > 20$ polynomial covering) $f : X \to \mathbb{P}^1_k$ with monodromy group $G \in \{A_n, S_n\}$ and $g_X \leq g$, the stabilizer H of a point is either A_{n-1}, or S_{n-1}, or $A_{n-2} < H \leq S_{n-2} \times S_2$.*

As a consequence, we enumerate arithmetically indecomposable low-genus subcovers of a geometrically indecomposable cover in these cases.

Lemma 2.21. *Suppose $\tilde{f}$ is the Galois closure of a nonsolvable, geometrically indecomposable covering $f : X \to \mathbb{P}^1_k$ such that one of the following holds:*

a) *f is a polynomial covering of degree $n > 20$,*
b) *f is a covering with almost simple monodromy and degree $\deg(f) > N_1$.*

Suppose h is a nonsolvable subcover of $\tilde{f}$ of genus ≤ 1. If h is indecomposable over k, then h is geometrically indecomposable, and $h \times_k \overline{k}$ is uniquely defined over k.

Proof. Let A (resp., G) denote the arithmetic (resp., geometric) monodromy group of f, and let $D \leq A$ be the preimage of a point stabilizer in $\operatorname{Mon}_k(h)$. Note that D is maximal in A since h is indecomposable over k. As G is almost simple in both cases (see Theorem 2.13 for case (a)), the first assertion follows once we show that $D \cap G$ is an intransitive maximal subgroup of G.

Since both assertions of the lemma are trivial in the case $G = A$, we assume $G < A$. As G is almost simple, the nonsolvability of $\operatorname{Mon}_k(h)$ implies the nonsolvability (and thus, faithfulness) of the action of G on $G/(D \cap G)$. Thus, we may pick a maximal $D \cap G \leq C < G$ for which the action of G on G/C is nonsolvable. In case a), Theorem 2.13 then readily implies that $A = S_n$, $G = A_n$, and C is either conjugate to a point stabilizer $G_1 = \operatorname{Sym}\{2, \dots, n\} \cap G$ or to the stabilizer of a 2-set $G_2 = (\operatorname{Sym}\{1, 2\} \times \operatorname{Sym}\{3, \dots, n\}) \cap G$. In case b), note that since A is almost simple, A/G is solvable. Since $\tilde{X}/C$ is of genus ≤ 1, it follows from Theorem 2.17 that $A = S_n$, $G = A_n$ for large n, and C is conjugate to G_1 or G_2 as in case a). In both cases, Lemma 2.20 implies that $D \cap G = C$, and C is conjugate to G_1 or G_2. In particular, $D \cap G$ is maximal in G and h is indecomposable over $\overline{k}$.

Furthermore, to show that $h \times_k \overline{k}$ is uniquely defined over k, we verify that the conditions of Remark 2.7: Without loss assume that $C = G_1$ or G_2 (stabilizing $\{1\}$ or $\{1,2\}$). Then A decomposes as $G \rtimes \langle (3,4) \rangle$, and C is normalized by $\langle (3,4) \rangle$. □

Remark 2.22. (1) Lemma 2.21 does not require the full force of Lemma 2.20. Indeed, [13, Theorem 5.2A and B] classify all subgroups of A_n and S_n of index $< \binom{n}{n/2}$. If M is a maximal subgroup of S_n with this property, then it turns out that (with a few low degree exceptions) $M \cap A_n < A_n$ is also maximal. But then our assumptions together with monodromy classification yield that $M \cap A_n$ must be the stabilizer of a point or a 2-set. To prove Lemma 2.21 in another way, it therefore suffices to show that there is no covering with genus $g \leq 1$, monodromy A_n, and degree $\geq \binom{n}{n/2}$.
(2) In the setup of Lemma 2.21, Theorems 2.13 and 2.17 imply that the fiber product of h and f is reducible. Indeed, in view of the theorems, it suffices to note that a point stabilizer A_1 in the natural action of $A = A_n$ or S_n acts intransitively on A/A_1 and on cosets A/A_2 of a 2-set stabilizer, so that the fiber product of $\tilde{X}/A_1 \to \tilde{X}/A$ and $\tilde{X}/A_2 \to \tilde{X}/A$ is reducible.

3. Quotients and transitive subgroups of imprimitve groups

Throughout this section, we consider subgroups G of the wreath product $U \wr_J V$, for finite permutation groups U and V, with V acting on a set J.

3.1. **Normal subgroups.** We start by describing the minimal normal subgroups of G. The following is a consequence of [2, (1.6),(2)-(3)]:

Lemma 3.1. *Let $G \leq U \wr_J V$ be a subgroup whose natural projection to V is onto, whose block stabilizer projects onto U, and assume V acts transitively on J. Assume U is primitive of type (C) with $\mathrm{soc}(U) \cong L^I$, and $K := G \cap U^J$ is nontrivial. Then*

$$\mathrm{soc}(K) = K \cap \mathrm{soc}(U)^J \cong (K \cap L^{O_1}) \times \cdots \times (K \cap L^{O_r}),$$

where $K \cap L^{O_j} \cong L$ for all $j \in J$, and $O_1, \ldots, O_r$ is a G-invariant partition of $I \times J$.

Remark 3.2. We use the following observation. Suppose $K \leq U^J$ and V is a group of outer automorphisms of K acting transitively by permuting J. Then (a) the images of projections $\pi_j : K \to U$ to the j-th coordinate, for $j \in J$, are all isomorphic; and (b) if furthermore $K \neq 1$, $\pi_j(K) \lhd U$, and U has a unique minimal normal subgroup, then $\pi_j(K) \supseteq \mathrm{soc}(U)$, for all $j \in J$.

To see (a), let $v_j \in V$ be an automorphism which sends j to 1, and observe that $\pi_1(K) = \pi_1(v_j(K)) = \pi_j(K)$ for all $j \in J$. To see (b), note that since $\mathrm{soc}(U)$ is the unique minimal normal subgroup of U and $\pi_j(K) \lhd U$, the images $\pi_j(K)$, $j \in J$ either contain $\mathrm{soc}(U)$ or are $\{1\}$. However, the latter case does not occur since $K \neq 1$.

Proof of Lemma 3.1. First recall that as G is a subgroup of $U \wr_J V$, it has a natural imprimitive action on $I \times J$ as in Section 2.6. The assertion is an immediate consequence of Lemma 2.11 and [2, (1.6)] (with $M = G$ and $D = \mathrm{soc}(K)$). To apply these it suffices to show 1) that the projection of $\mathrm{soc}(K)$ to the (i, j) component is onto L for every $(i, j) \in I \times J$, and 2) G acts transitively on $I \times J$.

We deduce 1) from Remark 3.2: First G acts transitively on J, so that the assumption of a) holds. Since the projection $\pi_j : G_0 \to U$ from the j-th block stabilizer G_0 to the j-th copy of U is onto, and since $K \lhd G_0$, we have $\pi_j(K) \lhd U$, $j \in J$. As in addition U is of type (C), and $K \neq 1$, the conditions of Remark 3.2.(b) also hold.

To show 2), note that since $\mathrm{soc}(U)$ is a normal subgroup of the primitive group U, it acts transitively on I [13, Theorem 1.6A]. As K projects onto $\mathrm{soc}(U)$, this implies that G acts transitively on each block $I \times \{j\}$, $j \in J$. Furthermore, G acts transitively on the blocks J, proving its transitivity on $I \times J$. $\square$

In particular, in the setting of Lemma 3.1 one has:

Corollary 3.3. *The socle* $\mathrm{soc}(K)$ *is a minimal normal subgroup of* G.

Proof. As in Lemma 2.11, decompose $\mathrm{soc}(K)$ as $\prod_{i=1}^{r} \mathrm{soc}(K) \cap L^{O_i}$ where $O_1, \ldots, O_r$ is a partition of $I \times J$, and $\mathrm{soc}(K) \cap L^{O_i} \cong L$. For N normal in K, Lemma 2.11 yields that $N \cap \mathrm{soc}(K)$ decomposes as $\prod_{i \in R} N \cap L^{O_i}$, where R is a subset of $\{1, \ldots, r\}$. Since G acts transitively on $I \times J$ (proof of Lemma 3.1), the normality of N in G implies that $R = \{1, \ldots, r\}$ or $\emptyset$, and hence $N \cap \mathrm{soc}(K) = \mathrm{soc}(K)$ or 1. $\square$

3.2. **Normal subgroups and decompositions.** The following lemma relates normal subgroups of an imprimitive group $G \leq U \wr V$ to other partitions of its action.

Lemma 3.4. *Let $G \leq U \wr_J V$ be transitive, where U is primitive of type (C), and G surjects onto V. Let $G_1 \leq G$ be a point stabilizer, and $G_1 \leq G_0 \leq G$ a block stabilizer. Let $K := \bigcap_{g \in G} G_0^g$ be the block kernel, and assume $K \neq 1$.*

Then every minimal normal subgroup N of G which is disjoint from K gives rise to a proper subgroup $G_1 N$ of $G_0 N$, with neither of $G_1 N$ and G_0 containing the other.

$$\begin{array}{ccc} G_0N \leq G & \text{———} & G_1N \\ | & & | \\ G_0 & \text{———} & G_1 \end{array}$$

Proof. To show $G_1 N \neq G_0 N$, it suffices to show that $N' := N \cap G_0$ acts trivially on G_0/G_1, since then $(N \cap G_0)G_1 = N'G_1 \neq G_0$, and hence $G_0 \not\leq G_1 N$.

Let $K_0 := \mathrm{soc}(K)$, and let M be the kernel of the action of $K_0 \times N'$ on G_0/G_1, so that $(K_0 \times N')/M$ embeds into U as a (transitive) normal subgroup. It remains to show that M contains N'. However, since U is nonaffine and K_0 is nontrivial, $\mathrm{soc}(U)$ and hence also $\mathrm{soc}(K_0)$, are nontrivial powers of a nonabelian simple group. Since K_0 is a power of a nonabelian simple group, Lemma 2.12 implies that every normal subgroup M of $K_0 \times N'$ decomposes as $M = (M \cap K_0) \times (M \cap N')$. In particular, the image $K_0/(K_0 \cap M) \times N'/(N' \cap M)$ is a normal subgroup of U. Since $K_0 \neq 1$, it acts nontrivially on G_0/G_1, and hence $K_0/(M \cap K_0)$ is nontrivial. As U is of type (C) and $K_0 \lhd G$, this shows that $K_0/(M \cap K_0)$ contains $\mathrm{soc}(U)$. Moreover, since U is of type (C), this forces $N'/(N' \cap M) = 1$, as desired.

It remains to note that $G_1 N$ is not contained in G_0, since by assumption

$$1 = N \cap K = N \cap \bigcap_{g \in G} G_0^g = \bigcap_{g \in G} (N \cap G_0)^g$$

while $K \neq 1$, giving $N \not\subseteq G_0$. □

Note that the conclusion of Lemma 3.4 yields a refinement $G > G_0 N > G_1 N > G_1$ of the inclusion $G > G_1$ which is essentially different from $G > G_0 > G_1$ (since neither of $G_1 N$ and any conjugate of G_0 contain the other).

If G is assumed to be the monodromy group of a polynomial map $f : \mathbb{P}^1 \to \mathbb{P}^1$, then the conclusion gives two essentially different decompositions of f, yielding:

Corollary 3.5. *Let k be a field of characteristic 0, and $f_i \in k[x]$, $i = 1, \dots, r$ be indecomposable polynomials with nonsolvable monodromy. Let A be the arithmetic monodromy group of $f = f_1 \circ \cdots \circ f_r$, and K the kernel of the natural projection $A \to \mathrm{Mon}(f_1 \circ \cdots \circ f_{r-1})$. Then $\mathrm{soc}(A) = \mathrm{soc}(K)$.*

Remark 3.6. Furthermore, we show that $\mathrm{soc}(K)$ is the unique minimal normal subgroup of every transitive subgroup $U \leq G$ containing $\mathrm{soc}(K)$.

Proof of Corollary 3.5 and Remark 3.6. First note that $\mathrm{soc}(K)$ is a minimal normal subgroup of A by Lemma 3.3. Ritt's theorem, cf. Remark 2.16, impies that the decomposition of f into indecomposables is unique up to composition with linear polynomials, so that $\mathrm{soc}(K)$ is the unique minimal normal subgroup of A by Lemma 3.4. In particular, $\mathrm{soc}(K)$ has a trivial centralizer in G, forcing $\mathrm{soc}(U) = \mathrm{soc}(K)$. Finally, since U is transitive, we also deduce that $\mathrm{soc}(K)$ is a minimal normal subgroup of U from Corollary 3.3. □

3.3. **Solvable proper quotients.** Finally, as a consequence of the above two sections, we deduce the following criterion under which an imprimitive group $G \leq U \wr V$ has solvable proper quotients.

Lemma 3.7. *Let V be a solvable permutation group on J, let U be a primitive nonsolvable permutation group with solvable proper quotients, and let $G \leq U \wr_J V$ be a transitive subgroup which surjects onto V and whose block stabilizer surjects onto*

U. Let G_1 be a point stabilizer, and assume that the action of G on G/H is solvable for every $H \supsetneq G_1$. Then every proper quotient of G is solvable.

Proof. Recall, as in Section 2.7, there exists a minimal subgroup $G_1 \leq \tilde{G}_0 \leq G$ for which $G/\tilde{G}_0$ is solvable. This group $\tilde{G}_0$ coincides with the block stabilizer G_0 of the block in J to which the point belongs to. Indeed, since G/G_0 is solvable, and $G_0 \supseteq G_1$, we have $G_1 < \tilde{G}_0 \leq G_0$. Since G_1 is maximal in G_0 by assumption and G/G_1 is nonsolvable, this gives $\tilde{G}_0 = G_0$, as claimed.

Assume $M \lhd G$ is a nontrivial normal subgroup with G/M nonsolvable, and consider the subgroup $G_1 M$. To apply Lemma 3.4, we claim that $M \cap K = 1$. Assuming this claim, we get that $G_1 M$ does not contain G_0. On the other hand, the action of G on $G/(G_1 M)$ is solvable by assumption, contradicting the fact that G_0 is minimal for which G/G_0 is solvable. Thus there is no such M, as desired.

To prove the claim, note that since $M \cap K$ is normal in G, Corollary 3.3 implies that either $M \cap K = 1$ or $M \supseteq \mathrm{soc}(K)$. Assuming on the contrary that the latter holds, we will show that $G/\mathrm{soc}(K)$ is solvable, contradicting the assumption that G/M is nonsolvable, and proving the claim.

let $I = G_0/G_1$ be a given block and $\psi : G_0 \to S_I$ denote the action of G_0 on this block, so that its image is the nonsolvable group U. Since G/K is solvable and U has a unique minimal normal subgroup, $\psi(K)$ contains $\mathrm{soc}(U)$. Since G is transitive on blocks, we may replace I by any other block, and deduce that the projection of K onto each of the blocks contains $\mathrm{soc}(U)$. We may therefore apply Lemma 3.1 to deduce that $\mathrm{soc}(K) = K \cap \mathrm{soc}(U)^d$, and hence that $K/\mathrm{soc}(K)$ injects into $U^d/\mathrm{soc}(U)^d$. Since U has solvable proper quotients, $U/\mathrm{soc}(U)$ is solvable and hence $U^d/\mathrm{soc}(U)^d$ and $K/\mathrm{soc}(K)$ are solvable. As G/K is solvable, this implies that so is $G/\mathrm{soc}(K)$. □

3.4. **Transitive subgroups.** In view of the connection between reducible specializations and intransitivity, see Section 2, we give the following transitivity criteria:

Lemma 3.8. *Let $G \leq S_n$ be transitive with point stabilizer H, and $H =: H_0 < H_1 < \cdots < H_r = G$ a chain of maximal subgroups of length $r \geq 1$ such that the action of H_i on H_i/H_{i-1} is nonsolvable for $i = 1, \ldots, r$. Let $U \leq G$ be a subgroup such that the action of G on G/U is solvable. Then U is transitive on G/H.*

Proof. Here, even $G/\bigcap_{g \in G} U^g$ is solvable, so by replacing U by $\bigcap_{g \in G} U^g$, we may assume without loss that U is normal in G. The case $r = 1$ is obvious, since any nontrivial normal subgroup of a primitive group is transitive. So assume $r \geq 2$.

Let $K = \bigcap_{g \in G} H_1^g$ be the normal core of H_1 in G. Since $G/(UK)$ is solvable, it follows inductively that UK, and therefore U, is transitive in the action on cosets of H_1. We claim that $U \cap H_1$ is transitive in its action on the block H_1/H. Since U is transitive on the set of blocks and on each block, the claim gives the transitivity of U on G/H.

Let $\psi : H_1 \to \mathrm{Sym}(H_1/H)$ be the action on the block H_1/H. By assumption, $\Gamma := \psi(H_1)$ is a primitive nonsolvable permutation group. Now $\psi(U \cap H_1)$ is a normal subgroup of Γ, and therefore either trivial or transitive. In the latter case it follows that U is transitive in the action on cosets of H. Assume therefore that $\psi(U \cap H_1) = 1$. But $\Gamma/\psi(U \cap H_1)$ is a quotient of the solvable group $H_1/(U \cap H_1)$, and thus solvable, implying that Γ is solvable, a contradiction. □

As a consequence concerning decompositions of coverings, we have:

Corollary 3.9. *Let $f : X \to \mathbb{P}^1$ be a covering over a field k of characteristic 0, written as $f = f_1 \circ \cdots \circ f_r$ where all f_i are indecomposable with nonsolvable (arithmetic) monodromy. Assume that there exists a decomposition $f = g \circ h$, with coverings $h : X \to Y$ and $g : Y \to \mathbb{P}^1$, such that g has solvable monodromy. Then* $\deg(g) = 1$.

Proof. Let A be the monodromy group of f, and let $A > H_1 > \ldots > H_r$ be the chain of maximal subgroups induced by the decomposition $f = f_1 \circ \cdots \circ f_r$. Assume that $f = g \circ h$, where g has solvable monodromy group and $\deg g > 1$. Then there is a proper subgroup U containing H_r, such that the action of A on A/U induces a solvable group. By Lemma 3.8, U is transitive on A/H_r, contradicting $H_r \subseteq U$. □

Note that the assumption that the action of G on G/U is solvable in Proposition 3.8 can be replaced with the following equivalent condition. There exists a chain $U =: U_0 < U_1 < \cdots < U_s = G$ of maximal subgroups such that the action on each U_i/U_{i-1} is solvable. We state the analogous transitivity property, as well as few other properties of use, when U_i/U_{i-1}, $i = 1, \ldots, s$ are more generally affine:

Lemma 3.10. *Let $G \leq S_n$ be transitive with point stabilizer H, and let $H =: H_0 < H_1 < \cdots < H_r = G$ and $U =: U_0 < U_1 < \cdots < U_s = G$ be two chains of maximal subgroups with $r \geq 1$. Assume that 1) the action of H_i on H_i/H_{i-1} is nonsolvable and its image in $\mathrm{Sym}(H_i/H_{i-1})$ has solvable proper quotients for $i = 1, \ldots, r$, whereas U_i/U_{i-1} is affine for $i = 1, \ldots, s$; and 2) the block kernels $\bigcap_{g\in G} H_i^g$, $i = 0, \ldots, r-1$, are pairwise distinct.*[6] *Then*

a) *U is transitive.*
b) *U acts faithfully on cosets of $U \cap H$ in U.*

[6]We suspect that the technical assumption 2) is in fact not necessary for the assertion to hold. It however occurs naturally in many cases of interest. E.g., if the chain $H_0 < H_1 < \ldots < H_r = G$ arises as the chain of point stabilizers in $\mathrm{Mon}(f_1 \circ \cdots \circ f_i)$, $i = 1, \ldots, r$ for polynomial maps f_i, then due to Remark 2.15, it is automatic that $\cap_{g\in G} H_i^g$ can never be contained in H_{i-1}.

c) *If additionally the image of H_i in* $\mathrm{Sym}(H_i/H_{i-1})$ *is even* 2*-transitive for all* $i = 1, \dots, r$*, then 1) and 2) above hold with G replaced by U and H_i replaced by $H_i \cap U$ for* $i = 1, \dots, r$.

The proof of Lemma 3.10 relies on the following observation.

Lemma 3.11. *In the setup of Lemma 3.10, for every $N \triangleleft G$, we claim that the group $U \cap N$ must contain all nonabelian composition factors of N.*

Proof. First note that U contains every nonabelian composition factor of G, including multiplicities. Indeed, this follows by applying the following argument iteratively to $U_i = U_{s-1}, \dots, U_0$: Since a point stabilizer U_i, in the primitive affine action of U_{i+1} on U_{i+1}/U_i, has an elementary abelian complement, it contains every nonabelian composition factor of U_{i+1}.

Applying this to the quotient G/N (resp. G) shows that its nonabelian composition factors are the same as those of $U/(N \cap U)$ (resp. U). Since the composition factors of U are those of $N \cap U$ combined with those of $U/(N \cap U) \cong UN/N \leq G/N$, this implies that the nonabelian composition factors of $N \cap U$ and those of N are the same, as desired. □

Proof of Lemma 3.10. We begin with a) and argue by induction on s. For the induction base $s = 0$, the assertion holds trivially. Set $K := \bigcap_{g \in G} H_1^g$ and note that $K \neq 1$. By induction the action of UK/K on the blocks G/H_1 is transitive. It therefore remains to show that $U \cap H_1$ is transitive in its action on a given block H_1/H_0. Since $\mathrm{soc}(K) \triangleleft G$, Lemma 3.11 shows that U must contain every non-abelian composition factor of $\mathrm{soc}(K)$. Let Γ denote the image of the action $\psi : H_1 \to \mathrm{Sym}(H_1/H_0)$. Since Γ is of type (C), and $K \neq 1$, Remark 3.2 implies that the projection $\psi(\mathrm{soc}(K))$ to any block is a nontrivial normal subgroup of Γ. Since Γ is primitive, $\psi(\mathrm{soc}(K))$ and hence $U \cap H_1$ is transitive on H_1/H_0, completing a).

Next, the transitivity of U implies $\bigcap_{u \in U} (U \cap H)^u \subseteq \bigcap_{u \in U} H^u = \bigcap_{g \in G} H^g = 1$, and hence b) follows.

Finally, since the minimal normal subgroup of a non-affine 2-transitive group is simple and primitive, cf. Remark 2.14, the image of $U \cap H_1$ in $\mathrm{Sym}((U \cap H_1)/(U \cap H_0))$ is again primitive with solvable proper quotients, showing that 1) continues to hold under the assumptions of c). Moreover, since $\mathrm{soc}(K)$ is a direct product of nonabelian simple groups by Lemma 3.1 and its composition factors are contained in U as above, $\mathrm{soc}(K) \subseteq \cap_{u \in U} (U \cap H_1)^u$, i.e., in the kernel of the action of U on cosets of $U \cap H_1$. In particular, this kernel is nontrivial. It follows by induction that 2) continues to hold as well. □

Remark 3.12. Due to Remarks 2.14 and 2.15, the assumptions of Lemma 3.10 (including that of (c)) are fulfilled when G is the monodromy group of a polynomial

$f \in k[X]$, over a field k of characteristic 0, decomposing as $f_1 \circ \cdots \circ f_r$ for indecomposable polynomials f_i, $i = 1, \dots, r$ with nonsolvable monodromy group. Namely, letting $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ denote the Galois closure of f, we pick $H = H_0 < H_1 < \cdots < H_r = G$ so that f_i is equivalent to the projection $\tilde{X}/H_{r-i} \to \tilde{X}/H_{r-i+1}$, $i = 1, \dots, r$. Finally, suppose the projection $h : \tilde{X}/U \to \tilde{X}/G$, for $U \le G$, is a composition of coverings with affine monodromy. Lemma 3.10 then yields:

a) The pullback $f' : \tilde{X}/(H \cap U) \to \tilde{X}/U$ of f along h is a covering of the same degree as f.
b) f and f' have the same Galois closure $\tilde{X}$.
c) f' is equivalent to the composition of the indecomposable coverings $f_i' : \tilde{X}/(U \cap H_{r-i}) \to \tilde{X}/(U \cap H_{r-i+1})$, $i = 1, \dots, r$ with almost simple monodromy group (of the same degree as f_i). Furthermore, the kernel of the projection $\mathrm{Mon}(f_1' \circ \cdots \circ f_i') \to \mathrm{Mon}(f_1' \circ \cdots \circ f_{i-1}')$ contains the socle of the kernel of $\mathrm{Mon}(f_1 \circ \cdots \circ f_i) \to \mathrm{Mon}(f_1 \circ \cdots \circ f_{i-1})$, for $i = 1, \dots, r$.

Note that c) follows immediately from the proof of Lemma 3.10.(c), rather than its assertion.

4. Main theorem

The following theorem, the main result of this paper, establishes a machinery to compare low genus subcovers of the Galois closure $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ of a covering $f : X \to \mathbb{P}^1_k$, with the composition factors of f itself. In this section, we fix a base field k of characteristic 0. All occurring coverings are to be understood as coverings over k. Consequently, the term "monodromy group" always refers to the arithmetic monodromy group.

Theorem 4.1. *Suppose $f : X \to \mathbb{P}^1_k$ is a covering with decomposition $f = f_1 \circ \cdots \circ f_r$ for indecomposable coverings $f_i : X_i \to X_{i-1}, i = 1, \dots, r$ whose monodromy groups Γ_i have solvable proper quotients. Suppose $h : Y \to \mathbb{P}^1_k$ is a minimal subcover of $\tilde{f}$ with nonsolvable monodromy group Γ whose proper quotients are solvable. Then:*

(1) *there exists a subcover f' of f that has the same Galois closure as h. Moreover, $f' = f_1' \circ f_2'$ with $\mathrm{Mon}(f_1')$ solvable and f_2' indecomposable;*
(2) *if moreover $\Gamma_1, \dots, \Gamma_r$ are nonsolvable, then $f' = f_2'$ is indecomposable.*

Addendum to Theorem 4.1. Under the above assumption that $\Gamma_1, \dots, \Gamma_r$ are nonsolvable, we moreover show:

(a) If $i \in \{1, \dots, r\}$ is minimal such that h is a subcover of the Galois closure of $f_1 \circ \cdots \circ f_i$, then $\mathrm{Mon}(f_1 \circ \cdots \circ f_i)$ embeds into the direct product $\mathrm{Mon}(f_1 \circ \cdots \circ f_{i-1}) \times \mathrm{Mon}(f_i)$.

(b) Conversely, given $i \in \{1, \dots, r\}$, let $\tilde{g}_i$ denote the Galois closure of $f_1 \circ \cdots \circ f_i$. Consider all minimal subcovers h of $\tilde{g}_i$, but not of $\tilde{g}_{i-1}$, whose monodromy group is nonsolvable with solvable proper quotients. All such subcovers h have the same Galois closure, and monodromy group isomorphic to $\mathrm{Mon}(f_i)$.

(c) Let i be as in (a). Then the covering f_i is equivalent to the pullback of a subcover of $\tilde{h}$ along $f_1 \circ \cdots \circ f_{i-1}$.

Remark 4.2. (1) Every minimal nonsolvable subcover h of $\tilde{f}$, can be written as $h = h_1 \circ h_2$ with $\mathrm{Mon}(h_1)$ solvable, and $\mathrm{Mon}(h_2)$ primitive nonsolvable. The assumption on $\mathrm{Mon}(h)$ to have no proper nonsolvable quotients is guaranteed once the proper quotients of $\mathrm{Mon}(h_2)$ are solvable, by Lemma 3.7.

If h_2 is additionally assumed to be polynomial (resp. geometrically indecomposable of sufficiently large degree), then Theorem 2.13 (resp. Theorem 2.17) yields that, indeed, $\mathrm{Mon}(h_2)$ has solvable proper quotients.

(2) Since Γ_i, $i \in \{1, \dots, r\}$ has solvable proper quotients, it is primitive of type (A) or (C). The further assumption that Γ_i is nonsolvable forces it to be of type (C).

Example 4.3. This example demonstrates that the assumption on the proper quotients of $\mathrm{Mon}(h)$ to be solvable is unavoidable. Let $G := S_n \wr S_m$ for $m, n \geq 5$. Let f_1 and f_2 be coverings with monodromy groups S_n and S_m resp., whose composition $f = f_1 \circ f_2$ has monodromy group G with the natural imprimitive action. Let $h : \tilde{X}/H \to \mathbb{P}^1$ be the subcover of $\tilde{f} : \tilde{X} \to \mathbb{P}^1$ corresponding to the point stabilizer H in the natural primitive action of G. Then h is a minimal nonsolvable subcover of $\tilde{f}$, and there is no subcover f' of f with the same Galois closure as h such that $f' = f_1' \circ f_2'$ where f_1' has solvable monodromy and f_2' is indecomposable.

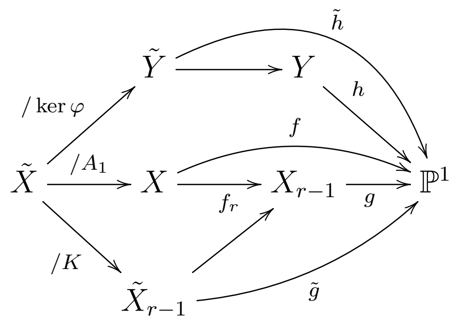
Indeed, the point stabilizer $H = S_{n-1} \wr S_{m-1}$ has trivial core in G, and hence the Galois closure of h is all of $\tilde{f}$. The point stabilizer in the imprimitive action is $G_1 = (S_{n-1} \times S_n^{m-1}) \rtimes S_{m-1}$, and the only intermediate subgroup between G_1 and G is the block kernel $S_n^m \rtimes S_{m-1}$ whose core is nontrivial. Thus every proper subcover of f does not have Galois closure $\tilde{f}$ while f itself has no decomposition $f_1' \circ f_2'$ with f_1' solvable and f_2' indecomposable.

Proof of Theorem 4.1. **Step I:** Setting up the proof. For $r = 1$, the assertion holds trivially with $\tilde{f}_1 = f$ and $\tilde{f}_2 = id$ since by assumption the proper quotients of $\mathrm{Mon}(f_1)$ are solvable. Assume inductively that the assertion holds for $r - 1$.

Set $g := f_1 \circ \cdots \circ f_{r-1}$, so that $f = g \circ f_r$, set $m := \deg g$, and let $\tilde{g} : \tilde{X}_{r-1} \to \mathbb{P}^1$ denote the Galois closure of g. Let A be the (arithmetic) monodromy group of f, and K the kernel of the natural projection $A \to \mathrm{Mon}(g)$. In particular, A is a subgroup of $\Gamma_r \wr \mathrm{Mon}(g)$, and K is a subgroup of Γ_r^m whose projection to each of the m components is the same and is either trivial or contains $Q := \mathrm{soc}(\Gamma_r)$ by Remark 3.2.

In the first case, $K=1$ and hence $\tilde g$ can be identified with $\tilde f$, in which case the claim follows by replacing f by g and applying induction. Henceforth assume that the projection of K to any of its components contains Q.

Finally, identify h with the subcover $\tilde X/D\to\mathbb{P}^1$ corresponding to a subgroup $D\le A$. Let $\Gamma:=\mathrm{Mon}(h)$, and let $\varphi: A\to\Gamma$ be the restriction map. Note that since Γ has solvable proper quotients, as long as K is not fully contained in $\ker\varphi$, the quotient $\Gamma/\varphi(K)$ is solvable. As a summary consider the following diagram, where $/K$ mean the quotient by K map.



Step II: Reduction to the case where $K\cap\ker\varphi=1$; $\Gamma/\varphi(K)$ is solvable; and Γ_r is nonsolvable. Since $K\cap\ker\varphi$ is normal in A, Corollary 3.3 shows that either $\ker\varphi\ge\mathrm{soc}(K)$ or $\ker\varphi\cap\mathrm{soc}(K)=1$ and hence $\ker\varphi\cap K=1$. Note that we can apply the corollary since Q is contained in the projection of K onto each of the m components.

Assume first that $\ker\varphi\ge\mathrm{soc}(K)$. In this case, we claim that $\tilde g$ factors through h, and hence we deduce the assertion from the induction hypothesis. The claim is equivalent to $K\le D$, and as $\mathrm{core}_A(D)=\ker\varphi$, also to $K\le\ker\varphi$. Assume otherwise that $\ker\varphi$ is a proper subgroup of $\ker\varphi\cdot K$. The natural projection $\tilde Y/\varphi(K)\to\mathbb{P}^1$ is then a nontrivial subcover of $\tilde h$. Since $\Gamma=\mathrm{Mon}(\tilde h)=\varphi(A)$ has solvable proper quotients, the monodromy group $\Gamma/\varphi(K)$ of the covering $\tilde Y/\varphi(K)\to\mathbb{P}^1$ is solvable.

On the other hand, since $\mathrm{soc}(K)=K\cap\mathrm{soc}(\Gamma_r)^m$ by Lemma 3.1, and $\Gamma_r/\mathrm{soc}(\Gamma_r)$ is solvable by assumption, we deduce that $K/\mathrm{soc}(K)$ is solvable. Since $K/\mathrm{soc}(K)$ is solvable and $\ker\varphi\ge\mathrm{soc}(K)$, we get that $\varphi(K)$ is solvable. The solvability of $\varphi(K)$ and of $\Gamma/\varphi(K)$ contradicts the nonsolvability of Γ.

Henceforth assume $\ker\varphi\cap K=1$, i.e., φ is injective on K. In particular, K and $\ker\varphi$ form their direct product in A. We note that since Γ has solvable proper quotients, $\Gamma/\varphi(K)$ is solvable. Thus $\varphi(K)$ must be nonsolvable, since Γ is. In particular, $\Gamma_r=\mathrm{Mon}(f_r)$ is nonsolvable.

Step III: We construct a subcover f' of both $\tilde h$ and f whose Galois closure is $\tilde h$, and find a decomposition $f'=f_1'\circ f_2'$ such that f_1' has solvable monodromy, and f_2' is indecomposable, giving (1).

Let $A_1 \leq A$ be the point stabilizer in $\mathrm{Mon}(f)$, and $A_0 \leq A$ the subgroup corresponding to X_{r-1}. Let f' (resp., f_1') be the natural projection $\tilde{X}/(A_1 \ker\varphi) \to \mathbb{P}^1$ (resp., $\tilde{X}/(A_0 \ker\varphi) \to \mathbb{P}^1$). Note that since $\Gamma \cong A/\ker\varphi$, f' is equivalent to the natural projection $\tilde{Y}/\varphi(A_1) \to \mathbb{P}^1$, so that f' is a subcover both of $\tilde{h}$ and of f.

Note first that the monodromy of f_1' is solvable: By step II, $A/(K\ker\varphi) \cong \Gamma/\varphi(K)$ is solvable. Since $\varphi(A_0) \geq \varphi(K)$ and $\varphi(K) \lhd \Gamma$, the Galois closure of f_1' is a subcover of $\tilde{Y}/\varphi(K) \to \mathbb{P}^1$ and hence also has solvable monodromy.

We next claim that f_2' is indecomposable. Recall that A_0 has a primitive nonsolvable (although not faithful) permutation action on A_0/A_1, namely the action through the quotient $\Gamma_r = Mon(f_r)$. Since A_0 is primitive in this action, the action of its image $\varphi(A_0)$ on $\varphi(A_0)/\varphi(A_1)$ is either primitive or trivial. In the latter case, $A_0 \ker\varphi = A_1 \ker\varphi$, contradicting Lemma 3.4 with $N = \ker\varphi$. This proves the claim, and hence part (1).

Step IV: To deduce part (2), assume moreover that Γ_i, $i = 1, \ldots, r$ are nonsolvable. Since f' is a subcover of f and f_1' has solvable monodromy, Corollary 3.9 implies that f_1' is an isomorphism, proving that f_2' can be chosen to be f'.

Step V: Deducing parts (a) and (c) of the addendum. Under the assumption that Γ_j, $j = 1, \ldots, r$ are nonsolvable, we show the direct product decomposition. We may assume without loss of generality that $i = r$, and hence $\tilde{g}$ does not factor through h. Thus, $\ker\varphi \cap K = 1$ by step II.

Set $K_0 := \bigcap_{g \in G_0} G_1^g$. From steps III and IV, we know that $\varphi(A_0) = \Gamma$ and $\varphi(K_0) \neq \Gamma$ is a normal subgroup with nonsolvable quotient. Since Γ is nonsolvable with solvable proper quotients, this forces $\varphi(K_0)$ to be trivial. Thus, $\Gamma \cong \mathrm{Mon}(f_r)$. So $\mathrm{Mon}(f)$ has two quotients $\mathrm{Mon}(g)$ and $\mathrm{Mon}(f_r)$, and the corresponding kernels K and $\ker(\varphi)$ are disjoint. This implies that $\mathrm{Mon}(f)$ embeds into the direct product $\mathrm{Mon}(g) \times \mathrm{Mon}(f_r)$, giving (a). Moreover, since φ induces an isomorphism of abstract groups from $\mathrm{Mon}(f_r) = A_0/K_0$ to Γ, Remark 2.10 implies that the pullback of the natural projection $\tilde{Y}/\varphi(A_1) \to \mathbb{P}^1$ along g is equivalent to $f_r : \tilde{X}/A_1 \to X_{r-1}$.

Step VI: Deducing part (b) of the addendum. For each minimal subcover h whose monodromy group is nonsolvable with solvable proper quotients, part (2) associates an indecomposable covering f', through which by assumption $f_1 \circ \cdots \circ f_i$, but not $f_1 \circ \cdots \circ f_{i-1}$ factors. For convenience replace f by $f_1 \circ \cdots \circ f_i$; g by $f_1 \circ \cdots \circ f_{i-1}$; and retain the above notation. By Step II, the associated normal subgroup $N = \ker\varphi$ fixing the Galois closure of f' satisfies $K \cap N = 1$. It now suffices to show that N is independent of f' (and hence of h).

Assume there were two such normal subgroups N_1 and N_2. Then by Lemma 2.12:

$$N_1 \cap N_2 = (N_1 \cap soc(K)) \cdot (N_1 \cap N_2) = N_1 \cap (soc(K) \times N_2).$$

Thus

$$N_1/(N_1 \cap N_2) = N_1/(N_1 \cap (N_2 \operatorname{soc}(K))) \cong N_1 N_2 \operatorname{soc}(K)/(N_2 \operatorname{soc}(K)) \le A/(N_2 \operatorname{soc}(K))$$

which is solvable. Therefore, $N_1N_2/N_2 \cong N_1/(N_1 \cap N_2)$ is a solvable normal subgroup of A/N_2. Since A/N_2 has no such nontrivial subgroups, $N_1 \cap N_2 = N_1$, that is, $N_2 \supseteq N_1$. By symmetry $N_1 = N_2$, concluding the proof. □

Remark 4.4. In the notation of Step I, if in addition $\operatorname{soc}(K)$ is assumed to be the unique minimal normal subgroup of G, then Step II shows that either h is a subcover of the Galois closure of $f_1 \circ \cdots \circ f_{r-1}$, or h has the same Galois closure as f. The former corresponds to the case $\ker \varphi \supseteq K$, while the latter corresponds to the case $\ker \varphi \cap \operatorname{soc}(K) = 1$ which implies $\ker \varphi = 1$ by the uniqueness assumption on $\operatorname{soc}(K)$.

5. Main conclusions

5.1. **The polynomial case.** Let k be a field of characteristic 0 with algebraic closure $\overline{k}$. The following is our most general result concerning the *geometric* monodromy group $G = \operatorname{Mon}_{\overline{k}}(f)$ when f is a polynomial. Let $\tilde{f} : \tilde{X} \to \mathbb{P}^1_{\overline{k}}$ be the Galois closure of f over $\overline{k}$, and $f_C : \tilde{X}/C \to \mathbb{P}^1_{\overline{k}}$ the covering corresponding to $C \le G$.

Theorem 5.1. *Suppose $f = f_1 \circ \cdots \circ f_r \in \overline{k}[x]$ for indecomposable polynomials f_i, $i = 1, \ldots, r$ with nonsolvable monodromy groups. Let $C \le \operatorname{Mon}_{\overline{k}}(f)$ be an intransitive subgroup whose corresponding covering $f_C : \tilde{X}/C \to \mathbb{P}^1_{\overline{k}}$ is of genus ≤ 1. Then there exists a subcover h of f_C with the same Galois closure as f_1.*

Proof. **Step I**: *Constructing a minimal nonsolvable subcover of f_C.* Let $G = \operatorname{Mon}_{\overline{k}}(f)$. Since C is intransitive, Remark 3.12 implies that f_C is not a composition of coverings with affine monodromy. Thus, f_C has a minimal subcover $f_V : \tilde{X}/V \to \mathbb{P}^1$, $C \le V \le G$ with decomposition $f_V = f_U \circ h'$, $V \le U \le G$, such that $f_U : \tilde{X}/U \to \mathbb{P}^1$ is a composition of coverings with affine monodromy and $h' : \tilde{X}/V \to \tilde{X}/U$ is an indecomposable covering with nonaffine (in particular, nonsolvable) monodromy. Note that $\tilde{X}/U$ is of genus 0, since otherwise h' is a covering between genus 1 curves, hence with abelian monodromy [54, Theorem 4.10(c)], contradicting the assumption that its monodromy is nonaffine. Lemma 2.19 then implies that the proper quotients of $\operatorname{Mon}_{\overline{k}}(h')$ are solvable[7].

We will show that f_V has a subcover h with the same Galois closure as f_1.

Step II: *Pulling back f along f_U.* Since $f_1, \ldots, f_r$ are polynomials, Remark 2.14 implies that $\operatorname{Mon}_{\overline{k}}(f_i)$, $i = 1, \ldots, r$ are nonabelian almost simple groups and 2-transitive. Moreover, as $g_i = f_1 \circ \cdots \circ f_i$ is a polynomial, the kernel K_i of the projection

[7] The subcover f_V is then a minimal subcover of f_C whose monodromy group is nonsolvable with solvable proper quotients, by Lemma 3.7. However, we do not make use of this fact.

$\mathrm{Mon}(g_i) \to \mathrm{Mon}(g_{i-1})$, $i = 1, \dots, r$, is a nontrivial minimal normal subgroup of $\mathrm{Mon}(g_i)$ by Corollary 3.3.

We may therefore apply Lemma 3.10, as in Remark 3.12, to deduce that the pullback[8] $f' : \tilde{X}/(U \cap G_1) \to \tilde{X}/U$ of f along f_U is a covering with Galois closure $\tilde{X}$, and that f' decomposes as $f'_1 \circ \cdots \circ f'_r$ for indecomposable f'_i with almost simple monodromy group. Since $g'_i := f'_1 \circ \cdots \circ f'_i$ is the pullback of g_i along f_U, we shall henceforth identify $\mathrm{Mon}(g'_i)$ as a subgroup of $\mathrm{Mon}(g_i)$ for all i, as in Remark 2.10. The lemma then moreover shows that the kernel K'_i of the projection $\mathrm{Mon}(g'_i) \to \mathrm{Mon}(g'_{i-1})$ contains $\mathrm{soc}(K_i)$.

Step III: *Showing that h' has the same Galois closure as f'_1.* As f' has Galois closure $\tilde{f}' : \tilde{X} \to \tilde{X}/U$ by Step II, we may regard h' as a subcover of $\tilde{f}'$. Suppose $1 \le s \le r$ is minimal for which h' is a subcover of the Galois closure of g'_s. We claim that $s = 1$.

Since $\mathrm{soc}(K_i) \le \mathrm{Mon}(g'_i)$ by Step II, Corollary 3.5 and Remark 3.6 imply that $\mathrm{soc}(K_i)$ is the unique minimal normal subgroup of $\mathrm{Mon}(g'_i)$. By minimality of s, Remark 4.4 implies that the Galois closure of h' is the same as that of g'_s. Since the proper quotients of $\mathrm{Mon}(h')$ are solvable by Step I, and $\mathrm{Mon}(g'_{s-1})$ is a nonsolvable proper quotient of $\mathrm{Mon}(g'_s)$ for $s > 1$, the claim follows. Finally, as $\mathrm{Mon}(f'_1)$ is almost simple, the Galois closure of h' coincides with that of f'_1.

Step IV: *Conclusion.* Let $\tilde{f}_1 : \tilde{X}_1 \to \mathbb{P}^1$ be the Galois closure of f_1 and $\phi_1 : G \to \mathrm{Mon}(f_1)$ the natural projection. The subcover $h : \tilde{X}_1/\phi_1(V) \to \tilde{X}_1/\mathrm{Mon}(f_1)$ of the Galois closure of f_1 is then equivalent to $\tilde{X}/(\ker(\phi_1) \cdot V) \to \tilde{X}/G$, and hence is also a subcover of $f_V : \tilde{X}/V \to \tilde{X}/G$. Moreover, $\phi_1(V)$ has trivial core in $\mathrm{Mon}(f'_1)$, and hence also in $\mathrm{Mon}(f_1)$, via the identification $\mathrm{Mon}(f'_1) \le \mathrm{Mon}(f_1)$ in Step II. Thus, the Galois closure of h is the same as that of f_1. □

We can now deduce the following strong form of Theorem 1.1. Note that, unlike Theorem 5.1, this result gives a conclusion about coverings over k.

Corollary 5.2. *Suppose k is finitely generated. Let $f = f_1 \circ \cdots \circ f_r$ be a decomposition of the polynomial $f \in k[x]$ into indecomposable polynomials. Assume that all of the f_i are of degree ≥ 5, and none of them is linearly related to x^n or a Chebyshev polynomial. Additionally, assume $\deg(f_1) > 20$. Then R_f and R_{f_1} differ only by a finite set. More precisely, one of the following holds:*

1. *R_f and $f_1(k)$ differ by a finite set;*
2. *There exists a (single) covering $f'_1 : X' \to \mathbb{P}^1$ over k with genus $g_{X'} = 0$, such that R_f and $f_1(k) \cup f'_1(X'(k))$ differ by a finite set. Moreover, either the ramification of f_1 is as in Table 1, or f_1 is one of the two cases in Theorem 2.13.(3) with monodromy group $\mathrm{P\Gamma L}_3(4)$ or $\mathrm{PSL}_5(2)$; and f'_1 is a subcover of the Galois closure of f_1.*

[8]The pullback is equivalent to the projection $\tilde{X}/(U \cap G_1) \to \tilde{X}/U$ by Remark 2.8.

If furthermore k is a number field with ring of integers O_k and $\mathrm{Mon}(f_1) \notin \{\mathrm{P\Gamma L}_3(4), \mathrm{PSL}_5(2)\}$,[9] *then $R_f \cap O_k$ and $f_1(k) \cap O_k$ differ by a finite set.*

Proof. Note first that, due to Remark 2.14, our assumptions imply that all f_i have nonsolvable monodromy. Let A and G denote the arithmetic and geometric monodromy group of f. By Corollary 2.4, it suffices to determine the subcovers $f_D : \tilde{X}/D \to \mathbb{P}^1_k$ for $D \leq A$ such that $\tilde{X}/D$ is of genus ≤ 1, and D is maximal intransitive with $D \cdot G = A$.

Step I: Showing that f_D is a geometrically indecomposable covering whose Galois closure is the same as that of f_1, and that a covering h equivalent to $f_D \times_k \overline{k}$ is uniquely defined over k. We first claim that f_D has a subcover h' over k with the same Galois closure as f_1. To show the claim, first apply Theorem 5.1 to obtain a subcover h over $\overline{k}$ of $f_{D\cap G}$ with the same Galois closure as f_1. Next, consider the image of D under the natural projection π from A onto $\Gamma_1 := \mathrm{Mon}_k(f_1)$, and note that $(f_1)_{\pi(G\cap D)} : \tilde{X}_1/\pi(G \cap D) \to \mathbb{P}^1_{\overline{k}}$ has the same Galois closure as f_1, since its subcover h does. If the action of Γ_1 on $\Gamma_1/\pi(D)$ is nonsolvable, the claim follows since the nonsolvable common k-subcover $(f_1)_{\pi(D)} : \tilde{X}_1/\pi(D) \to \mathbb{P}^1_k$ of $\tilde{f}_1$ and f_D has the same Galois closure as f_1. Assume on the contrary that the action on $\Gamma_1/\pi(D)$ is solvable. Since $\deg f_1 > 20$, Remark 2.14 implies that either $\mathrm{Mon}_{\overline{k}}(f_1) = \Gamma_1$ or $\mathrm{Mon}_{\overline{k}}(f_1) = A_n < S_n = \Gamma_1$. In both cases, $\pi(D) \supseteq \mathrm{soc}(\Gamma_1)$, due to the solvability of $\Gamma_1/\pi(D)$. Since $\pi(D \cap G) \lhd \pi(D)$, either $\pi(D \cap G)$ contains the socle as well, contradicting the nonsolvability of $\mathrm{Mon}_{\overline{k}}(f_{D\cap G})$; or $\pi(D \cap G) = 1$ contradicting that $f_{D\cap G}$ is a covering of genus ≤ 1, proving the claim.

Since $\deg f_1 > 20$, Lemma 2.21 and Remark 2.22.(2) show that the above covering h is uniquely defined over k by a (geometrically indecomposable) subcover h', and has reducible fiber product with f_1 (and a fortiori with f). By maximality of D, we deduce that f_D and h' are k-equivlalent, and $f_{D\cap G}$ and h are $\overline{k}$-equivalent.

Step II: Finding the genus ≤ 1 coverings h over $\overline{k}$ with the same Galois closure as f_1. We claim that there are at most two equivalence classes for h over $\overline{k}$. The only possible nonsolvable monodromy groups G for indecomposable f_1 of degree > 20, which are not alternating or symmetric, are $\mathrm{P\Gamma L}_3(4)$, M_{23} and $\mathrm{PSL}_5(2)$. A computer check shows that the Galois closure of the only polynomial covering with monodromy group M_{23} has no other genus ≤ 1 equivalence class of subcovers, so in this case (1) is fulfilled. In the same way, for $\mathrm{P\Gamma L}_3(4)$ and $\mathrm{PSL}_5(2)$, one verifies that the Galois closures of the corresponding polynomials have only one other equivalence class of subcovers of genus ≤ 1, and its stabilizer U acts intransitively, whence (2) is fulfilled. The ramification types of those f_1 with alternating or symmetric monodromy, whose Galois closure admits more than one equivalence of genus ≤ 1 subcovers, are listed

[9]Note that this extra assumption on $\mathrm{Mon}(f_1)$ is unnecessary for, e.g., $k = \mathbb{Q}$, since those two groups do not occur as monodromy groups of polynomials with rational coefficients, see [36].

in Table **??** of genus ≤ 1, whose stabilizer U (the stabilizer of a 2-element set) acts intransitively, hence these fall into case (2).

For the final assertion, it suffices to note that the coverings f_1' in case (2) are not Siegel functions by Theorem 2.13. □

Remark 5.3. 1) Note that as remarked in Section 2, the exceptional indecomposable polynomials f_1 with alternating or symmetric monodromy of degree $10 \leq n \leq 20$ and their corresponding genus ≤ 1 subcovers of $\tilde{f}_1$ are listed in [28, Theorem A.4.1]. Adding this exceptional list to Theorem 1.1, as well as the list arising from [36], would lower the degree assumption on f_1 to merely $\deg f_1 \geq 10$. In particular over the rationals $k = \mathbb{Q}$, Corollary 5.2 holds for polynomials f_1 of degree $\deg f_1 > 10$.
2) In the same way, the bound $\deg(f_1) > 20$ can be dropped in the statement about integral specializations in Corollary 5.2, at the cost of a list of exceptional indecomposable polynomials f_1. This list is, however, fully explicit. In particular for the analogous statement about integral specializations over $k = \mathbb{Q}$, one may replace $\deg(f_1) > 20$ by $\deg(f_1) > 5$. In fact, for the indecomposable case $f = f_1$, this conclusion was already reached by Fried [20]. To see the claim, first note that an exception arises when $\mathrm{Mon}(f_1)$ acts as the monodromy group of another Siegel function f_1' not equivalent to f_1. Since this action may be assumed minimally nonsolvable and $\mathrm{Mon}(f_1)$ is almost simple, this means that either $\mathrm{Mon}(f_1)$ must induce a Siegel function in a second action *permutation-equivalent* to that of $\mathrm{Mon}(f_1)$; or some subgroup between $\mathrm{Mon}(f_1)$ and its socle must induce a Siegel function in a *different* primitive action. From the classification of primitive monodromy groups of Siegel functions in [37] (in particular Theorems 4.8 and 4.9), one extracts easily (aided by a computer check) that the first scenario happens only for $\mathrm{Mon}(f_1) \in \{\mathrm{PSL}_2(11), \mathrm{PSL}_3(2), \mathrm{PSL}_3(3), \mathrm{PSL}_4(2), \mathrm{P\Gamma L}_3(4), \mathrm{PSL}_5(2)\}$, whereas the second one only happens for $\mathrm{Mon}(f_1) \in \{A_5, S_5, \mathrm{PSL}_3(2), \mathrm{P\Gamma L}_2(9), M_{11}, \mathrm{PSL}_4(2)\}$. Out of those possibilities, only the polynomials with monodromy group S_5 and $\mathrm{P\Gamma L}_2(9)$ can be defined over $\mathbb{Q}$, and for the latter group the Siegel function f_1' does not have two poles of the same order, and so is not a Siegel function over $\mathbb{Q}$ (cf., e.g., [37, Section 4.4]).

Finally we apply Theorem 5.1 to prove Theorem 1.2:

Proof of Theorem 1.2. The reducibility of $f(x) - g(y) \in \mathbb{C}[x, y]$ implies that of the corresponding normal curve. It is well know that this curve is (the normalization of) the fiber product of $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, and $g : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. By Lemma 2.9, we may replace g by a common polynomial subcover g_0 of g and of the Galois closure $\tilde{f}$, whose fiber product with f is still reducible. Since x^n, T_n, and an indecomposable degree 4 polynomial do not appear as composition factors of f, the monodromy group of each f_i is nonsolvable with proper solvable quotients, as in Remark 2.14.

Theorem 5.1 then shows that there is a polynomial subcover h of g_0, with the same Galois closure as f_1. Since $\deg f_1 > 31$, the possibilities for h are described in cases (1)-(2) of Theorem 2.13. In fact, as both h and f_1 are polynomials with alternating or symmetric monodromy Γ_1, the point stabilizer of both of them is conjugate to the stabilizer in the natural action of Γ_1. Hence h and f_1 are equivalent, as desired. ☐

We note that Remark 5.3.(1) applies similarly to Theorem 1.2.

5.2. **Composition of coverings with almost simple monodromy.** Finally the following theorem strengthens Theorem 1.3:

Theorem 5.4. *There exists an absolute constant $N \in \mathbb{N}$ satisfying the following. Let $f : X \to \mathbb{P}^1_k$ be a covering over a finitely generated field k of characteristic 0, with decomposition $f = f_1 \circ \cdots \circ f_r$ such that each f_i is of degree $\geq N$, and is geometrically indecomposable with nonabelian almost simple monodromy group Γ_i. Then there exist a finite extension k'/k, nonsolvable indecomposable genus ≤ 1 coverings $h_i : Y_i \to \mathbb{P}^1_{k'}$, $i = 1, \ldots, u_f$ and $h'_j : \mathbb{P}^1_{k'} \to \mathbb{P}^1_{k'}$, $j = 1, \ldots, v_f$, such that $v_f \leq u_f \leq r$, and $R_f(k')$ is contained in the union of $\bigcup_{i=1}^{u_f} h_i(Y_i(k')) \cup \bigcup_{j=1}^{v_f} h'_j(k')$ and a finite set.*

If moreover all alternating or symmetric Γ_i occur in the natural action, then $R_f(k')$ and $\bigcup_{i=1}^{u_f} R_{h_i}(k')$ differ by a finite set. Furthermore for all i with alternating or symmetric Γ_i in the natural action, h_i is a subcover of f, and $R_{h_i}(k')$ differs by a finite set either from $h_i(k')$ or from $h_i(k') \cup h'_{j_i}(k')$ for some $j_i \leq v_f$.

More precisely, we show $u = u_f$ is at most the number of $i \in \{1, \ldots, r\}$ such that $\mathrm{Mon}(f_i)$ is isomorphic to an alternating or symmetric group and $\mathrm{Mon}(f_1 \circ \cdots \circ f_i)$ embeds into $\mathrm{Mon}(f_1 \circ \cdots \circ f_{i-1}) \times \mathrm{Mon}(f_i)$; out of which $v = v_f$ is the number of i's for which the ramification of h_i is as in Theorem 2.17.(1).

Proof. Let $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ denote the Galois closure of f over k. Set $k' := \overline{k} \cap \Omega$ where $\Omega = k(\tilde{X})$, so that the arithmetic and geometric monodromy groups $A := \mathrm{Mon}_{k'}(f)$ and $G := \mathrm{Mon}_{\overline{k}}(f)$ identify. We shall henceforth replace k by k' and assume $A = G$, cf. Remark 5.5.

To deduce the assertion from Corollary 2.4, we will find (up to equivalence) all minimal k-subcovers $h : Z \to \mathbb{P}^1$ of $\tilde{f}$ whose fiber product with f is reducible and for which Z is of genus ≤ 1. By Lemma 3.8, without loss of generality we restrict to minimal nonsolvable subcovers h.

Step I: Choice of N. By Theorem 2.17 (the classification of monodromy groups), there exists a constant N such that for every indecomposable covering $h_{\overline{k}} : Z' \to \mathbb{P}^1_{\overline{k}}$ with genus $g_{Z'} \leq 1$ and nonsolvable monodromy Γ of order $\geq N$, the group Γ is nonsolvable with solvable proper quotients. Furthermore by Remark 2.18, for large N, there are at most two minimal nonsolvable (and, in fact, necessarily indecomposable) subcovers of $\tilde{h}_{\overline{k}}$ with genus ≤ 1, and at most one such subcover if the ramification of $h_{\overline{k}}$ does not appear in [43, Tables 4.1, 4.2] and [44, Table 3.1]. Note that in case there are two such subcovers and Γ is almost simple, Remark 2.18 implies that Γ is alternating or symmetric in fact, from [43, §4], both subcovers are then of genus 0).

Step II: Applying Theorem 4.1. Note that since all nonabelian composition factors of A are of large degree, $h = h_1 \circ h_2$ where h_1 is a rational function with solvable monodromy and $h_2 : Z \to \mathbb{P}^1_k$ is nonsolvable of large degree. Since $A = G$, Theorem 2.17 implies that $\mathrm{Mon}_k(h_2)$ has solvable proper quotients, and hence so does Γ by Lemma 3.7. The assumptions of Theorem 4.1 are therefore fulfilled, and we deduce that there exists an indecomposable k-subcover h with Galois closure $\tilde{h}$, and almost simple monodromy isomorphic to $\mathrm{Mon}_k(f_i)$ for some i. Also note that since Γ is alternating or symmetric by Theorem 2.17, and since h is of genus ≤ 1 and minimal nonsolvable, we in fact get that h itself is indecomposable.

Step III: We claim by induction on r that the number m_f of (inequivalent) minimal nonsolvable subcovers $h : Z \to \mathbb{P}^1_k$ of $\tilde{f}$ with genus $g_Z \leq 1$ is at most $u_f + v_f$, with $u = u_f$ and $v = v_f$ as defined in the theorem. Write $g := f_1 \circ \cdots \circ f_{r-1}$, and assume inductively that $m_g \leq u_g + v_g$. By the addendum to Theorem 4.1, every minimal nonsolvable subcover h of $\tilde{f}$ is either a subcover of the Galois closure of g, or a subcover of the Galois closure of a uniquely determined indecomposable subcover h' of f with $\mathrm{Mon}(h') \cong \mathrm{Mon}(f_r)$.

Therefore, our choice of N implies:
(1) If h' as above exists, then $\mathrm{Mon}_k(f_r) \cong \mathrm{Mon}_k(h')$ is isomorphic to an alternating or symmetric group. In particular, if $\mathrm{Mon}_k(f_r)$ is nonalternating and nonsymmetric, then $u_f = u_g$, $v_f = v_g$, and $m_f = m_g$, as desired;
(2) If $\mathrm{Mon}_k(f_r)$ is alternating or symmetric, the Galois closure $\tilde{h}'$ contains at most two minimal subcovers $h : Z \to \mathbb{P}^1_k$ with genus $g_Z \leq 1$ and nonsolvable monodromy, and at most one such subcover if its ramification does not appear in Theorem 2.17.(1). If the latter holds, we have $u_f = u_g + 1$, $v_f = v_g$ and $m_f = m_g + 1$, otherwise, $u_f = u_g + 1$, $v_f = v_g + 1$, and $m_f = m_g + 2$, as desired.

To get equality up to a finite set in the assertion of Theorem 5.4, rather than just inclusion, it suffices to show that the above coverings h and h' (with monodromy $\mathrm{Mon}(f_i)$) in fact have reducible fiber product with f, by Corollary 2.4 and Remark 2.8. Denote by f_i' the subcover of f whose Galois closure equals the one of h, given by Theorem 4.1. It of course suffices a fortiori to show that the fiber product of h and (if exists) of h' with f_i' is reducible. The latter is not always the case for alternating or symmetric $\mathrm{Mon}(f_i')$ in a "nonnatural" primitive action. However, from Theorem 2.17, it is true as soon as that action is the natural one, concluding the proof. □

Remark 5.5. (1) In Theorem 5.4, one shall in fact be able to take k' to be k. Indeed, the only place where the proof uses crucially the assumption $A = G$ is in order to verify that the monodromy group $\tilde{A} := \mathrm{Mon}_k(h_2)$ in Step II has proper solvable quotients. A work in progress of the authors, P. Müller and M. Zieve shows that for an indecomposable covering $h_2 : X \to \mathbb{P}^1_k$ of genus $g_X \leq 1$ and sufficiently large degree, the proper quotients of $\tilde{A}$ are either all solvable, as needed; or the geometric monodromy group $\tilde{G} \triangleleft \tilde{A}$ is solvable. The latter does not happen, since in our scenario $\tilde{A}$ is alternating or symmetric, and $\tilde{G} \neq 1$.

(2) Assume further that k be a number field with ring of integers O_k. Using Corollary 2.4 to describe $R_f \cap O_k$, we furthermore get that all coverings h_i, h_j in Theorem 5.4 are Siegel functions. Recall that Remark 2.18 asserts that the Galois closure of a geometrically indecomposable covering h of large degree factors through at most one Siegel subcover with nonsolvable monodromy. Hence, the same argument, as in the proof of Theorem 5.4, shows that $R_f \cap O_k$ and $\bigcup_{i=1}^{s}(h_i(k) \cap O_k)$ differ by a finite set, for s indecomposable Siegel subcovers of $\tilde{f}$ over k, where $s \leq u_f$. Here, the conclusion $k' = k$ is obtained more easily than in (1), since arithmetically indecomposable Siegel functions are necessarily geometrically indecomposable [39, Theorem 3.4].

(3) The assumption that the groups $\mathrm{Mon}(f_i)$, $i = 1, \ldots, r$ are almost simple in Theorem 5.4 can be relaxed to the mere assumption that these are (large degree) primitive groups with solvable proper quotients. The maximal number of coverings needed to describe R_f should then be $3r$ (rather than $2r$), due to the following fact: Given a large degree indecomposable covering $h : Z \to \mathbb{P}^1_k$ of genus $g_Z \leq 1$ and nonsolvable monodromy, $\tilde{h}$ factors through at most three minimal subcovers of genus ≤ 1 and nonsolvable monodromy, as pointed out in Remark 2.18.

(4) It is well known that for compositions $f = f_1 \circ \cdots \circ f_r$ of general coverings with monodromy $\mathrm{Mon}_{\overline{k}}(f_i) \cong S_{n_i}$, $i = 1, \ldots, r$, the monodromy of the composition $\mathrm{Mon}_{\overline{k}}(f)$ is the full wreath product $(S_{n_1} \wr \cdots \wr S_{n_{r-1}}) \wr S_{n_r}$. In such cases, none of the groups $\mathrm{Mon}(f_1 \circ \cdots \circ f_i)$ embeds into $\mathrm{Mon}(f_1 \circ \cdots \circ f_{i-1}) \times \mathrm{Mon}(f_i)$ for $i \geq 2$. Hence, R_f differs by a finite set from at most one value set $h_1(Y_1(k))$!

References

[1] M. Aschbacher, On conjectures of Guralnick and Thompson. J. Algebra 135 (1990), 277–343. 13

[2] M. Aschbacher, L. Scott, Maximal subgroups of finite groups. J. Algebra 92 (1985), 44–80. 10, 15, 16

[3] R. Avanzi, U. Zannier, Genus one curves defined by separated variable polynomials and a polynomial Pell equation. Acta Arith. 99 (2001), 227–256. 1

[4] R. Avanzi, U. Zannier, The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. Comp. Math. 139 (2003), 263–295. 2

[5] E. Bank, L. Bary-Soroker, and L. Rosenzweig, Prime polynomials in short intervals over large finite fields, Duke Math. J. 164 (2015), 277–295. 2

[6] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman, T. J. Tucker, Current trends and open problems in arithmetic dynamics. Bull. Amer. Math. Soc. 56 (2019), 611–685. 2

[7] Y. Bilu, R. Tichy, The Diophantine equation $f(x) = g(y)$. Acta Arith. 95 (2000), 261–288. 1

[8] P. Cassou-Noguès, J. Couveignes, Factorizations explicites de $g(y) - h(z)$, Acta Arith. 87 (1999), 291–317. 2, 11

[9] H. Davenport, D. J. Lewis, A. Schinzel, Equations of the form $f(x) = g(y)$. Quarterly J. of Math. 12 (1961), 304–312. 2

[10] H. Davenport, A. Schinzel, Two problems concerning polynomials. J. Reine Angew. Math. 214 (1964), 386–391. 2

[11] P. Dèbes, M. D. Fried, Integral specialization of families of rational functions. Pacific J. Math. 190 (1999), 45–85. 2

[12] P. Dèbes, F. Legrand, Twisted covers and specializations, in: Galois-Teichmueller theory and Arithmetic Geometry, Proceedings for Conferences in Kyoto (October 2010). H. Nakamura, F. Pop, L. Schneps, A. Tamagawa eds., Advanced Studies in Pure Mathematics 63 (2012), 141–162. 6

[13] J. D. Dixon, B. Mortimer, Permutation Groups. Springer GTM 163 (1996). 12, 15, 16

[14] T. Do, J. Hallett, Q. Sun, B. Weiss, E. Wells, S. Xia, and M. E. Zieve, On the Diophantine equation $f(x) = g(y)$. Preprint. 1

[15] M. D. Fried, R. E. MacRae, On the invariance of chains of fields. Illinois J. Math. 13 (1969), 165–171. 7, 13

[16] M. D. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables. Illinois J. of Math. 17 (1973), 128–146. 2

[17] M. D. Fried, On the diophantine equation $f(y) - x = 0$. Acta Arith. 19 (1971), 79–87. 2

[18] M. D. Fried, On a theorem of Ritt and related Diophantine problems J. Reine Angew. Math. 264 (1973), 40–55. 1

[19] M. D. Fried, On Hilbert's irreducibility theorem. J. Number Theory 6 (1974), 211–231. 2

[20] M. D. Fried, Applications of the classification of simple groups to monodromy, part ii: Davenport and Hilbert–Siegel problems, preprint (1986), 1–55. 2, 28

[21] M. D. Fried, Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the finite simple group classification. Sci. China Math. 55 (2012), 1–72. 2

[22] M. D. Fried, On the Sprindzuk-Weissauer approach to universal Hilbert subsets. Israel J. Math. 51 (1985), 347–363. 9

[23] M. D. Fried, M. Jarden, Field arithmetic. vol. **11**, 2nd edn. Revised and enlarged by Moshe Jarden. Ergebnisse der Mathematik (3). Springer, Berlin, 2005. 9

[24] M. D. Fried, I. Gusić, Schinzel's problem: imprimitive covers and the monodromy method. Acta Arith. 155 (2012), 27–40. 2

[25] D. Ghioca, T. J. Tucker, M. E. Zieve, Linear relations between polynomial orbits. Duke Math. J. 161 (2012), 1379–1410. 1

[26] R. Guralnick, Monodromy Groups of Coverings of Curves. Galois Groups and Fundamental Groups, MSRI Publications 41 (2003). 10

[27] R. Guralnick, M. Neubauer, Monodromy groups of branched coverings: the generic case. Contemp. Math. 186 (1995), 325–352. 14

[28] R. Guralnick, J. Shareshian, Symmetric and Alternating Groups as Monodromy Groups of Riemann Surfaces I: Generic Covers and Covers with Many Branch Points. Appendix by R. Guralnick and R. Stafford. Mem. Amer. Math. Soc. 189 (2007). 3, 5, 11, 13, 28

[29] R. Guralnick, J. Thompson, Finite groups of genus zero. J. Algebra 131 (1990), 303–341. 3, 13, 14

[30] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten.* J. reine angew. Math. 110 (1892), 104–129. 1

[31] B. Huppert, Primitive, auflösbare Gruppen, Arch. Math. 6 (1955), 303–310. 12

[32] R. Jones, A. Levy, Eventually stable rational functions. Int. J. Number Theory 13 (2017), 2299–2318. 2

[33] J. König, D. Neftin, The admissibility of M_{11} over number fields. J. Pure Appl. Alg. 222 (2018), 2456–2464. 7

[34] M. Larsen, A. Lubotzky, Normal subgroup growth of linear groups: the (G_2, F_4, E_8)-Theorem. Algebraic groups and arithmetic, 441–468, Tata Inst. Fund. Res., Mumbai, (2004). 10

[35] T. Monderer, D. Neftin, Symmetric Galois groups under specialization. To appear in Israel J. Math. ArXiv:2003.11324. 14

[36] P. Müller, Primitive monodromy groups of polynomials. Recent developments in the inverse Galois problem, Contemp. Maths. 186, 385–401, Amer. Math. Soc., 1995. 5, 11, 12, 27, 28

[37] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) XII (2013), 369–438. 13, 28

[38] P. Müller, Hilbert's irreducibility theorem for prime degree and general polynomials. Israel J. Math. 109 (1999), 319–337. 3

[39] P. Müller, Finiteness results for Hilbert's irreducibility theorem. Ann. Inst. Fourier 52 (2002), 983–1015. 3, 31

[40] P. Müller, Reducibility behavior of polynomials with varying coefficients. Israel J. Math. 94 (1996), 59–91. 2

[41] P. Müller, Permutation groups of prime degree, a quick proof of Burnside's theorem. Arch. Math. 85 (2005), 15–17. 12

[42] P. Müller, M. Zieve, On Ritt's polynomial decomposition theorems. Preprint, arXiv:0807.3578. 1, 12

[43] D. Neftin, M. Zieve, Monodromy groups of indecomposable coverings of bounded genus. Preprint (2020). At https://neftin.net.technion.ac.il/files/2020/11/monodromy-3.pdf. 3, 5, 11, 13, 30

[44] D. Neftin, M. Zieve, Monodromy groups of product type. Preprint (2020). At: https://neftin.net.technion.ac.il/files/2020/11/wreath-2.pdf. 5, 13, 30

[45] A. Néron. Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. Bull. Soc. Math. France 80 (1952) 101–166. 1

[46] F. Pakovich, Polynomial semiconjugacies, decompositions of iterations, and invariant curves. Ann. Sc. Norm. Super. Pisa Cl. Sci. XVII (2017), 1417–1446. 1

[47] F. Pakovich, On polynomials sharing preimages of compact sets, and related questions. Geom. Funct. Anal. 18 (2008), 163–183. 1

[48] J. F. Ritt, Prime and composite polynomials. Trans. Amer. Math. Soc. 23 (1922), 51–66. 1, 12

[49] A. Makowski, A. Schinzel, Sur l'équation indéterminée de M. Goormaghtigh, Mathesis 68 (1959), 128–142. 2

[50] A. Schinzel, Some unsolved problems on polynomials. Mate. Biblioteka 25 (1963), 63–70. 2

[51] I. Schur, Zur Theorie der einfach transitiven Permutationsgruppen. S. B. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 598–623. 12

[52] T. Shih, A note on groups of genus zero. Comm. Algebra 19 (1991), 2813–2826. 13

[53] J.-P. Serre, Topics in Galois theory. Second edition. Springer, 2008. 1

[54] J. H. Silverman, The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Second Edition. 25

[55] H. Völklein, Groups as Galois Groups: An Introduction. Cambridge Studies in Advanced Mathematics, 1996. 1

[56] U. Zannier, A proof of Pisot's d-th root conjecture. Ann. Math. 151 (2000), 375–383.

1

Department of Mathematics Education, Korea National University of Education, Cheongju, South Korea

Department of Mathematics, Technion - Israel Institute of Technology, Israel