REDUCIBLE FIBERS OF POLYNOMIAL MAPS

JOACHIM KÖNIG AND DANNY NEFTIN

ABSTRACT. For a degree n polynomial $f \in \mathbb{Q}[x]$, the elements in the fiber $f^{-1}(a) \subseteq \mathbb{C}$ are of degree n over $\mathbb{Q}$ for most values $a \in \mathbb{Q}$ by Hilbert's irreducibility theorem. Determining the set of exceptional a's without this property is a long standing open problem that is closely related to the Davenport–Lewis–Schinzel problem (1959) on reducibility of separated polynomials. As opposed to previous work which mostly concerns indecomposable f, we answer both problems for decomposable $f = f_1 \circ \cdots \circ f_r$, as long as the indecomposable factors $f_i \in \mathbb{Q}[x]$ are of degree ≥ 5 and are not x^n or a Chebyshev polynomial composed with linear polynomials.

1. INTRODUCTION

Given a degree n (rational) map $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ (between smooth projective curves), Hilbert's irreducibility theorem [31] asserts the existence of infinitely many $a \in \mathbb{Q}$ for which the fiber $f^{-1}(a) \subseteq \mathbb{C}$ is irreducible[1] over $\mathbb{Q}$, that is, it's elements are of degree n over $\mathbb{Q}$. Moreover, letting $\mathrm{Red}_f = \mathrm{Red}_f(\mathbb{Q})$ denote the set of values $a \in \mathbb{Q}$ over which the fiber $f^{-1}(a)$ is reducible, Hilbert's theorem asserts that Red_f is the union of finitely many value sets $h_i(Y_i(\mathbb{Q}))$ of nontrivial maps $h_i : Y_i \to \mathbb{P}^1_{\mathbb{Q}}$, $i = 1, \ldots, r$. However, determining which of the value sets $h_i(Y_i(\mathbb{Q}))$ are infinite is far from known.

For polynomial maps $f \in \mathbb{Q}[x]$, determining the infinite value sets contributing to Red_f is a long standing open problem of special interest, firstly due to its relation with reducibility of separated polynomials: for $h_i \in \mathbb{Q}[x]$, the value set $h_i(\mathbb{Q})$ is contained in Red_f if and only if $f(x) - h_i(y) \in \mathbb{Q}[x, y]$ is reducible. The reducibility of such polynomials plays a key role in studying the rational points on components of the associated curves $f(x) = h(y)$ [4, 8, 50, 17] for $h \in \mathbb{Q}[y]$, a problem with a wide range of applications e.g. to functional equations [52, 20, 48], dynamics [39, 26], and complex analysis [51].

Secondly, the problem arises in arithmetic dynamics in the context of stability and newly reducible values, cf. [7, §19],[10, 33]. Namely, 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

[1]Equivalently it asserts the existence of infinitely many $a \in \mathbb{Q}$ such that $F(a, x) \in \mathbb{Q}[x]$ is irreducible for a polynomial $F(t, x) \in \mathbb{Q}(t)[x]$ defining a curve birational to X over $\mathbb{Q}$. This is also equivalent to $\mathbb{P}^1_{\mathbb{Q}}$ having the Hilbert property, a property of high interest in recent years [6, 11].

over $\mathbb{Q}$, but the fiber of $f^{\circ m}$ over a 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, cf. [46].

Most known results concern indecomposable maps f, that is, maps that cannot be written as the composition of two maps of degree > 1. For integral values and indecomposable $f \in \mathbb{Q}[x]$ with[2] $\deg f > 5$, $\mathrm{Red}_f(\mathbb{Z})$ is the union of a finite set with the integers $f(\mathbb{Q}) \cap \mathbb{Z}$ in a single value set, by Fried, cf. [46]. In the more general case of rational values, for indecomposable $f \in \mathbb{Q}[x]$ with $\deg f > 20$, $\mathrm{Red}_f(\mathbb{Q})$ is the union of the single value set $f(\mathbb{Q})$ with a finite set, by Müller [42] and Guralnick–Shareshian [29], cf. Corollary 5.2 and Theorem 5.4.

This paper deals with decomposable polynomial maps $f = f_1 \circ \cdots \circ f_r$ when the monodromy groups of f_i, $i = 1, \dots, r$ are nonsolvable. This gives the following solution when $f \in \mathbb{Q}[x]$ has no composition factor of the form x^n, or the (normalized) Chebyshev polynomial T_n. 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. *Suppose $f = f_1 \circ \ldots \circ f_r$ for indecomposable $f_i \in \mathbb{Q}[x]$, $i = 1, \dots, r$ 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 $\mu_1, \mu_2 \in \mathbb{C}[x]$. If $\deg f_1 > 5$, then $\mathrm{Red}_f(\mathbb{Z})$ is the union of $f_1(\mathbb{Q}) \cap \mathbb{Z}$ and a finite set.*

If further $\deg f_1 > 20$, then Red_f is the union of Red_{f_1} and a finite set. In particular, either Red_f is the union of $f_1(\mathbb{Q})$ with a finite set, or f_1 is as in Table 1.

A surprising part of Theorem 1.1 is that if the fiber of the first polynomial f_1 is irreducible over a, then the fibers of the rest of the compositions $f_1 \circ \cdots \circ f_i$ remain irreducible for all but finitely many $a \in \mathbb{Q}$. In particular for $m > 1$, it follows that the iterate $f^{\circ m}$ is newly reducible only over finitely many values $a \in \mathbb{Q}$. See Theorem 5.6 for the analogous result over other fields.

We further apply our methods to the *Davenport–Lewis–Schinzel (DLS)* problem on reducibility of separated polynomials. This problem originates in the late 50's [38, 53, 12, 13] in view of the above relation to the curves $f(x) = h(y)$. It seeks to determine the polynomials $f, h \in \mathbb{C}[x] \setminus \mathbb{C}$ for which $f(x) - h(y) \in \mathbb{C}[x, y]$ is reducible. A trivial case in which $f(x) - h(y)$ is reducible is when f and h have a nontrivial common left composition factor, that is, $f = g \circ f_1, h = g \circ h_1$ for $g, f_1, h_1 \in \mathbb{C}[x] \setminus \mathbb{C}$ with $\deg g > 1$. The problem is to find the nontrivial reducible cases.

In case at least one of f and h is indecomposable, the problem is solved by Fried [19], who gives the possible ramification of f and h. The polynomials themselves are then determined by Cassou-Noguès–Couveignes [9]. More recent progress is described in [4, Theorem 3 and §3], [21, 24], and here as well the main difficulty is the remaining case of decomposable polynomials.

[2]Moreover, by Dèbes and Fried [14], examples with $\deg f_1 = 5$ actually occur!

Our methods give the following answer to the DLS problem when one avoids composition factors of the form x^n and T_n:

Theorem 1.2. *Let $f, h \in \mathbb{C}[x]$ 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 $f(x) - h(y) \in \mathbb{C}[x, y]$ is reducible if and only if $h = f_1 \circ h'$ for some $h' \in \mathbb{C}[x]$.*

Note that common composition factors of f and h necessarily factor 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, see Theorem 2.9. We note the degree assumptions on f_1 can be removed in both of the above theorems at the account of a longer list of exceptions, cf. §5.3. However, different methods are required for both of the above theorems 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 even when the decomposition of f is unique, see Example 2.6.

The above two problems share a common ground, namely, they require determining the maps $h : Y \to \mathbb{P}^1_k$, from Y of genus ≤ 1, whose fiber product with f is reducible. The key step in doing so is reducing the problem to determining the genus ≤ 1 maps whose fiber product with f_1 is reducible, see §5.1. This relies on a combination of Ritt's theorem, group theoretic tools, and a new relation between normal subgroups of the *monodromy group* of f with decompositions $f = f_1 \circ \cdots \circ f_r$, see Lemma 3.5.

The main property of indecomposable polynomials used in the proof is that either their monodromy groups are solvable or they are nonabelian almost simple by Burnside's theorem on doubly transitive groups. However, our strategy applies more generally to compositions of indecomposable maps whose monodromy groups are nonsolvable, but have the property that all their proper quotients are solvable. As opposed to Müller's finiteness results [44, 45] for indecomposable maps, for such decomposable maps Red_f may contain many infinite value sets. For the sake of simplicity of this paper, this is carried out separately in [35] for integral values.

The classification of finite simple groups (CFSG) is used in the above reduction process only for basic assertions regarding the outer automorphism group of a simple group such as Schreir's conjecture, and for the "further" part of Theorem 1.1 (in applying Theorem 2.3). The final step of classifying subcovers of the Galois closure of f_1 is then carried out by applying the primitive monodromy classification theorems (and hence the CFSG) for polynomials by Feit and Müller [42], and Guralnick–Shareshian [29], see §5.2 and §5.3. In light of the further development of the classification of primitive monodromy groups [49, 25, 1], the above results would hopefully extend to rational functions, and to general maps under group theoretic restrictions on their monodromy groups, cf. [36, §5.2].

We thank Robert Guralnick for helpful discussions. The second author was supported by the Israel Science Foundation (grants 577/15 and 353/21), the U.S.-Israel Binational Science Foundation (grant No. 2014173), and is grateful for the hospitality of the Institute for Advanced Studies. All computer calculations were carried out using Magma.

2. Preliminaries

2.1. **Coverings.** Let k be a field of characteristic 0, and $\overline{k}$ its algebraic closure. An (irreducible branched) *covering* $f : X \to Y$ (of curves) 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 $\overline{k}$), 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. [15, 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.

The *ramification type* of a covering $f : X \to \mathbb{P}^1_{\overline{k}}$ 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 $f \times_k \overline{k}$.

2.2. **Polynomials and Siegel functions.** 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. For polynomial coverings, Fried and MacRae [18] show that an indecomposable polynomial over k is indecomposable over $\overline{k}$. We shall therefore call such a polynomial simply "indecomposable" without specifying the base field.

Two polynomials $f, g \in k[x]$ are called *linearly related* (resp. linearly related *over* k), if there exist linear polynomials $\mu, \nu \in \overline{k}[x]$ (resp., $\in k[x]$) such that $g = \mu \circ f \circ \nu$.

A *Siegel function* is a covering $f : X \to \mathbb{P}^1_k$ over a number field k, for which $f^{-1}(O_k)$ has infinitely many k-rational points. Due to Siegel's theorem, for such a function one has $X \cong \mathbb{P}^1_k$ and ∞ has at most two preimages over $\overline{k}$. With a slight abuse of notation, coverings with the latter property are also called Siegel functions.

2.3. **Monodromy.** Let $f : X \to \mathbb{P}^1_k$ be a covering over k. Letting Ω denote the Galois closure of $k(X)/k(t)$, the *arithmetic (resp. geometric) monodromy group* $A = \mathrm{Mon}_k(f)$ (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 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 $D \cdot G = A$.

The following theorem describes the structure of monodromy groups of polynomials. This classical version is essentially due to Burnside and Schur, cf. Section 5.2 for the full classification result of Feit and Müller. Note that the CFSG is used in the following theorem only to assert that proper quotients of an almost simple group are solvable, an assertion also known as Schreier's conjecture. Denote by $\mathrm{soc}(A)$ the socle of A, that is, the product of minimal normal subgroups of A. When $\mathrm{soc}(A)$ is abelian, we say A is an affine permutation group.

Theorem 2.1. *Let $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$ be a polynomial covering with monodromy group $A = \mathrm{Mon}_k(f)$. Then A is either solvable or a 2-transitive nonabelian almost simple group. In the former case, f is linearly related (over $\overline{k}$) either to x^n, or to a Chebyshev polynomial, or an indecomposable degree 4 polynomial. In the latter case, $\mathrm{soc}(A)$ is primitive and $A/\mathrm{soc}(A)$ is solvable.*

Proof. Due to results of Burnside, see [47], and Schur [54], any primitive group containing a full cycle is known to be either solvable or 2-transitive; moreover, the minimal normal subgroup of a nonaffine 2-transitive group is known to be simple and primitive due to a theorem of Burnside [16, Theorem 7.2E]. The indecomposable polynomial coverings f with affine monodromy group G, and in particular those with solvable monodromy group, were essentially classified by Chisini and Ritt, see the proof of [32, Satz 5] or [42]. Finally if A is almost simple, then $A/\mathrm{soc}(A)$ is solvable by Schreier's conjecture, which follows from the classsifcation of finite simple groups. □

In case f is a Siegel function, Müller [43, Theorem 3.3] gives the following description of $\mathrm{Mon}(f)$. This version requires the CFSG only for Schreier's conjecture and the following bound on orders of elements in the outer automorphism group $\mathrm{Out}(S)$

of a nonabelian simple group S other than A_5 and $\mathrm{PSL}_2(7)$:

$$o(\mathrm{Out}(S)) < \frac{\#S}{2o(S)^2}, \tag{2.1}$$

where $o(G)$ denotes the maximal order of an element in a group G.

Theorem 2.2. *Let $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$ be a indecomposable Siegel function with nonaffine monodromy group $A = \mathrm{Mon}_k(f)$. Then A is either nonabelian almost simple, or $A \leq (\mathrm{Aut}(S) \times \mathrm{Aut}(S)) \rtimes C_2$ contains S^2 as a unique minimal normal subgroup for a nonabelian simple group S. In particular, the proper quotients of A are solvable.*

Proof. We note how the proof of [43, Theorem 3.3] adjusts to give this version without relying on the CFSG. Assume A is not almost simple. As in addition A is not affine, the remaining possibilities for A have product action, or regular normal subgroup action, or diagonal action in the terminology of [43, §2]. Without invoking the CFSG, [43, §3.4.1] shows that, for A of product action, one has $S^2 \lhd A \leq (U \times U) \rtimes C_2$ where U is a primitive group of degree r which contains an r-cycle and has socle S. Since A is nonaffine, S is nonabelian and Burnside's theorem shows that U is a 2-transitive almost simple group, so that S is simple and $U \leq \mathrm{Aut}(S)$, yielding the desired conclusion in the product type case.

Without invoking the CFSG, [43, §3.5] shows that A cannot have a regular normal subgroup: More precisely, it shows that in such case A must be a subgroup of $H^m \rtimes S_m$ equipped with a product action for H which is not 2-transitive, contradicting the above conclusion in the product type case. Finally, [43, §3.6] shows that A cannot have a diagonal action using the CFSG only when applying (2.1).

In total it follows that A has a unique minimal normal subgroup $\mathrm{soc}(A) = S^t$ for a simple group S and $t \in \{1, 2\}$, and hence the quotient $A/\mathrm{soc}(A)$ is a subgroup of $\mathrm{Out}(S)^t \rtimes S_t$, $t \leq 2$, which is solvable by Schreier's conjecture. □

For coverings of genus at most 1 the following analogous assertion is shown in Appendix A using the classification of monodromy groups and hence the CFSG.

Theorem 2.3. *Suppose $f : X \to \mathbb{P}^1_{\overline{k}}$ is an indecomposable covering of genus $g_X \leq 1$ and nonaffine monodromy group G. Then $G/\mathrm{soc}(G)$ is solvable.*

2.4. **Specializations.** To a covering $f : X \to \mathbb{P}^1_k$, one associates an irreducible polynomial $F \in k(t)[x]$ such that the curve $F(t, x) = 0$ is birational to X. Further, we replace F by a polynomial $F \in k[t, x]$ by multiplying it with an element of $k(t)$. Note that after these operations, the resulting set of values $t_0 \in k$ for which $F(t_0, x)$ is reducible differs from $\mathrm{Red}_f(k)$ only in finitely many values.

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 [34, 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 $t \mapsto t_0 \in k$. Moreover, Ω^D has a degree 1 place P over t_0. In particular, $\Omega^D \cap \overline{k}(t) = k(t)$, so that the corresponding morphism $f_D : X_D \to \mathbb{P}^1_k$ is geometrically irreducible, and $DG = A$. 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:

Proposition 2.4. *Let $f : X \to \mathbb{P}^1_k$ be a covering with arithmetic and geomertric monodromy groups A and G, respectively. Let $D = D_{t_0}$ be the decomposition group at $t \mapsto t_0$, and $f_D : X_D \to \mathbb{P}^1_k$ its corresponding covering. Then:*

1. *$t_0 \in f_D(X_D(k))$ and $DG = A$ for all but finitely many $t_0 \in k$;*
2. *For all but finitely many $t_0 \in k$, $t_0 \in \mathrm{Red}_f(k)$ if and only if D is intransitive.*

Proposition 2.4 implies that Red_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 $g_{X_D} \leq 1$. 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. This is the step in which the finite set of exceptions is no longer explicit; Computing it is in general hopeless since the curves X_D are arbitrary. We therefore have:

Corollary 2.5. *Let $f : X \to \mathbb{P}^1_k$ be a covering over a finitely generated field k with arithmetic (resp. geometric) monodromy A (resp. G). Then Red_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 $\mathrm{Red}_f(O_k)$ 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 2.6. Let $k := \mathbb{Q}(e^{2\pi i/8})$, and $f(x) := T_4(x) \in k[x]$. We will show that (1) Red_f is the union of $f_1(\mathbb{Q}) \cup h(\mathbb{Q})$ with a finite set, where $f_1(x) = T_2(x)$ and $h(x) = -T_4(x)$. Furthermore, (2) f_1 is the the unique indecomposable subcover of the natural projection $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$, $x \mapsto T_4(x)$. 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 $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ 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 2.7. h is equivalent to the covering $f_{\langle sr\rangle} : \tilde{X}/\langle sr\rangle \to \mathbb{P}^1_k$.

By Corollary 2.5, 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 2.7. Since the only proper subgroup of D_4 which contains $\langle sr\rangle$ is $\langle sr, r^2\rangle$ and it is not conjugate to U, (2) follows.

It remains to prove Claim 2.7. 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 $T_2 \circ f_{\langle sr\rangle}$ and $T_2 \circ f_{\langle s\rangle}$ are equivalent in D_8. However, since $\langle sr\rangle$ and $\langle s\rangle$ are not conjugate in A, $f_{\langle sr\rangle}$ is not equivalent to $f_{\langle s\rangle}$. As two covering which are inequivalent but whose compositions with T_2 are equivalent, $f_{\langle sr\rangle}$ is equivalent to $-f_{\langle s\rangle}$: $x \mapsto -T_4(x)$.

For an example over $\mathbb{Q}$, see [22, §2],[23, Chp. 13, Ex. 1].

2.5. **Decomposable coverings.** Let $f : Y \to X$ and $h : X \to \mathbb{P}^1$ be two coverings over k of degrees m, n and monodromy groups $U \leq \mathrm{Sym}(I), V \leq \mathrm{Sym}(J)$ with point stabilizers U_1, V_1, respectively. Then 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 $V \leq \mathrm{Sym}(J)$ permutes the J-copies of U. The action of A is the natural imprimitive degree mn action of $U \wr_J V$ on $I \times J$ with blocks indexed by J.

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 $V = \mathrm{Gal}(\Omega_X/k(\mathbb{P}^1))$, 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 $A_0 := A \cap (U^J \rtimes \mathrm{Sym}(J \setminus \{0\})$ be the stabilizer of a block $0 \in J$, (2) A_0 maps onto U under the projection to the 0-th coordinate. We shall use the following assertions on decompositions of polynomials:

Lemma 2.8. *Suppose $f = u \circ v$ for polynomial coverings u, v of degrees m, n, respectively, then the kernel of the natural projection π from $\mathrm{Mon}_k(f) \leq S_n \wr S_m$ to $\mathrm{Mon}_k(u) \leq S_m$ is nontrivial.*

Proof. 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 the kernel of π is nontrivial. □

The uniquness of decompositions of a polynomial with nonsolvable composition factors is given by Ritt's theorems [52, 48]. Due to subsequent work of Fried and

MacRae [18, Theorem 3.5], the linear polynomials in the following theorem may even be assumed to be over k.

Theorem 2.9. *Suppose $f = f_1 \circ \cdots \circ f_r$ for indecomposable $f_i \in k[x]$ with nonsolvable monodromy group. Then 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 $\mu_i \in k[x]$, $i = 1, \ldots, r$ with $\mu_0 = \mu_r = id$.*

2.6. **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 2.10. 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 2.11. *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 $W := X\#Z$.

Lemma 2.12. *Let $f : X \to Y$ be a covering with Galois closure $\tilde{f} : \tilde{X} \to Y$, and $h : Z \to Y$ a subcover of $\tilde{f}$ whose fiber product with f is irreducible. Then the Galois closure of the pullback f_h is equivalent to the projection $\tilde{X} \to Z$.*

Proof. First replace h by an equivalent subcover $f_H : \tilde{X}/H \to Y$ for some $H \leq \mathrm{Mon}_k(f)$. Since $X\#_Y Z$ is irreducible, H is transitive and f_h is equivalent to the projection $\tilde{X}/(H \cap G_1) \to \tilde{X}/H$ by Remark 2.10, where $G_1 \leq \mathrm{Mon}_k(f)$ is a point stabilizer. Moreover, the transitivity of H implies that

$$\bigcap_{x\in H} (H \cap G_1)^x \subseteq \bigcap_{x\in H} H^x = \bigcap_{g\in G} H^g = 1.$$

Thus the action of H on $H/H \cap G_1$ is faithful, so that there are no nontrivial Galois covers between $\tilde{X} \to \tilde{X}/H$ and $f_h : \tilde{X}/(H \cap G_1) \to \tilde{X}/H$. □

Remark 2.13. 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 may identify Γ with a (transitive) subgroup of A via the following embedding. Since $k(W)$ is the compositum of $k(X)$ and $k(Z)$ by Remark 2.10, 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 $\mathrm{Gal}(\Omega_X/\Omega_X \cap k(Z)) \leq A$.

3. Normal and transitive subgroups of imprimitive 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 essentially in [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 with a unique minimal normal subgroup $\mathrm{soc}(U) \cong L^I$ for a nonabelian simple group L, and $K := G \cap U^J$ is nontrivial. Then G acts transitively on a partition $O_1, \dots, O_r$ of $I \times J$ such that $K \cap L^{O_j} \cong L$, $j = 1, \dots, r$ and*

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

The proof relies on the following observations and lemma:

Remark 3.2. 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 $\pi_1(K) = \pi_1(v_j(K)) \cong \pi_j(K)$ 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 all $\{1\}$. However, the latter does not occur since $K \neq 1$.

The following lemma is a version of the well known Goursat lemma:

Lemma 3.3. [3, (1.4)] *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 $O_1, \dots, O_r$ is a partition of I, and $K \cap L^{O_j} \cong L$ for all $j = 1, \dots, r$.*

Proof of Lemma 3.1. We first show that the projection of $K \leq U^J$ to the j-th component contains $\mathrm{soc}(U) = L^I$, $j \in J$. First G acts transitively on J, so that the assumption of Remark 3.2.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 has a unique (nonabelian) minimal normal subgroup, and $K \neq 1$, the conditions of Remark 3.2.(b) also hold. Thus, the remark implies that $\mathrm{soc}(U) = L^I$ is a minimal normal subgroup of $\pi_j(K) \supseteq L^I$, $j \in J$. In particular, $K_0 := K \cap \mathrm{soc}(U)^J = K \cap L^{I\times J}$ surjects onto each copy of L, and hence $K_0 = (K \cap L^{O_1}) \times \cdots \times (K \cap L^{O_r})$ with $K \cap L^{O_k} \cong L$, $k = 1, \ldots, r$ for some partition $O_1, \ldots, O_r$ of $I \times J$, by Lemma 3.3.

Secondly, we show $G \leq U \wr_J V$ acts transitively on $I \times J$ via conjugation of the $I \times J$-indexed copies of L in $\mathrm{soc}(U)^J$. Since $\mathrm{soc}(U)$ is a normal subgroup of the primitive group U, it acts transitively on I [16, Theorem 1.6A]. As K_0 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, yielding its transitivity on $I \times J$. It follows that G acts transitively on the copies of L in K_0, and hence that G acts transitively on the partition $O_1, \ldots, O_r$ of $I \times J$.

It remains to note that $\mathrm{soc}(K)$ in fact equals K_0: Since $K_0 = K \cap \mathrm{soc}(U)^J$ is normal in K and is a direct product of isomorphic nonabelian simple groups which are permuted transitively by G, K_0 is contained in $\mathrm{soc}(K)$. To show equality, it suffices to show that a normal subgroup $C \lhd K$ which is disjoint from K_0 is trivial. Indeed, such C centralizes K_0, and hence $\pi_j(C)$ centralizers $\mathrm{soc}(U) = L^I \leq \pi_j(K_0)$, $j \in J$. Since the centralizer of $\mathrm{soc}(U)$ in U is trivial, $\pi_j(C) = 1$, $j \in J$ and hence $C = 1$, as needed. □

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

Corollary 3.4. *The socle* $\mathrm{soc}(K)$ *is a minimal normal subgroup of* G.

Proof. Let $N \lhd G$ be a normal subgroup. As in Lemma 3.3, 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 $\mathrm{soc}(K) \cap L^{O_i} \cong L$. Since $N \cap \mathrm{soc}(K)$ is normal in $\mathrm{soc}(K)$, it 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 $I \times J$ by 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. □

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 3.5. *Let* $G \leq U \wr_J V$ *be transitive, where* U *is primitive with a unique nonabelian minimal normal subgroup*[3]*, 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_1N *of* G_0N, *with neither of* G_1N *and* G_0 *containing the other.*

[3]In fact U has a unique minimal normal subgroup by Aschbacher–O'Nan–Scott [27, §9].

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

Proof. To show that $G_1N \neq G_0N$, 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 $G_0 \not\leq G_1N$.

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 and hence K_0 are nontrivial, $\mathrm{soc}(U)$ and hence also K_0 are nontrivial powers of a nonabelian simple group. Thus, Goursat's lemma [37, Corollary 1.4] implies that a normal subgroup M of $K_0 \times N'$ decomposes as $M = (M \cap K_0) \times (M \cap N')$. In particular, the image $K_0/(M \cap K_0) \times N'/(M \cap N')$ of the action is a normal subgroup of U. Since $K_0 \neq 1$, it acts nontrivially on each block, and hence $K_0/(M \cap K_0)$ is nontrivial. As U has a unique minimal normal subgroup and $K_0 \lhd G$, this shows that $K_0/(M \cap K_0)$ contains $\mathrm{soc}(U)$ as in Remark 3.2. Moreover, since U has a unique minimal normal subgroup, this forces $N'/(M \cap N') = 1$, as desired.

It remains to note that G_1N 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 3.5 yields a refinement $G > G_0N > G_1N > G_1$ of the inclusion $G > G_1$ which is essentially different from $G > G_0 > G_1$ (since neither of G_1N and any conjugate of G_0 contain the other).

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

Corollary 3.6. *Let k be a field of characteristic 0, and $f_i \in k[x]$, $i = 1, \ldots, r$ 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 $A \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{r-1})$. Then $\mathrm{soc}(A) = \mathrm{soc}(K)$.*

Remark 3.7. Furthermore, we show that $\mathrm{soc}(K)$ is the unique minimal normal subgroup of every transitive subgroup $B \leq A$ containing $\mathrm{soc}(K)$.

Proof of Corollary 3.6 and Remark 3.7. First note that $\mathrm{soc}(K)$ is a minimal normal subgroup of A by Lemma 3.4. Ritt's theorem 2.9 implies 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 3.5. In particular,

$\mathrm{soc}(K)$ has a trivial centralizer in A, forcing $\mathrm{soc}(B) = \mathrm{soc}(K)$. Finally, since B is transitive, we also deduce that $\mathrm{soc}(K)$ is a minimal normal subgroup of B from Corollary 3.4 (applied with U replaced by a subgroup of it, namely, the image of the action of a block stabilizer of B on a block). □

3.3. **Pulling back along covers with affine monodromy.** The following lemma is the base of our induction process in Proposition 4.1 below.

Lemma 3.8. *Let $U \leq G$ be a subgroup such that the action on G/U is affine. Suppose $G = H_0 > H_1 > \cdots > H_r =: H$ is a chain of maximal subgroups such that 1) the action $\Gamma_i \leq \mathrm{Sym}(H_{i-1}/H_i)$ of H_{i-1} on H_{i-1}/H_i is almost simple with primitive socle for $i = 1, \ldots, r$, and 2) the block kernels $\bigcap_{g\in G} H_i^g$, $i = 1, \ldots, r$ are pairwise distinct. Then $H_{i-1} \cap U$ is transitive on H_{i-1}/H_i, $i = 1, \ldots, r$ and 1) and 2) hold with H_i replaced by $H_i \cap U$ for $i = 0, \ldots, r$.*

In terms of coverings this gives the following corollary. As we shall see in Section 5.3, its conditions hold when the coverings are polynomial.

Corollary 3.9. *Let $f_i : X_i \to X_{i-1}$, $i = 1, \ldots, r$ be coverings such that 1) $\mathrm{Mon}(f_i)$ are nonabelian almost simple with primitive socle, and 2) $g_i = f_1 \circ \cdots f_i$ does not factor through the Galois closure $\tilde{g}_{i-1}$ of g_{i-1} for $i = 1, \ldots, r$. Let h be a subcover of $\tilde{g}_r : \tilde{X} \to \mathbb{P}^1_k$ that has an affine monodromy group. Let g'_i be the pullback of g_i along h, and define f'_i iteratively via $g'_i = g'_{i-1} \circ f'_i$, $i = 1, \ldots, r$. Then g'_i is irreducible, and 1) and 2) above hold with g_i replaced by g'_i and f_i by f'_i.*

Proof. Pick $G =: H_0 > H_1 > \cdots > H_r = H$ (resp. U) so that f_i (resp. h) is equivalent to the projection $\tilde{X}/H_{i-1} \to \tilde{X}/H_i$, $i = 1, \ldots, r$ (resp. $\tilde{X}/U \to X_0$). As the conditions of Lemma 3.8 hold, the lemma implies that $H_i \cap U$ is transitive on H_{i-1}/H_i so that the pullback $g'_i : \tilde{X}/(H_i \cap U) \to \tilde{X}/U$ of g_i along h is irreducible of the same degree as g_i, $i = 1, \ldots, r$. The second assertion of the corollary now follows directly from the second assertion of Lemma 3.8. □

The proof of Lemma 3.8 relies on the following observation.

Lemma 3.10. *In the setup of Lemma 3.8, for every $N \triangleleft G$, 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, since U has an elementary abelian complement, it contains every nonabelian composition factor of G. 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 3.8. We first show transitivity by induction on r. For the induction base $r = 0$, the assertion holds trivially. Set $K_i := \bigcap_{g\in G} H_i^g$, and note that $K_i \neq 1$, $i = 1, \dots, r$. By induction the action of UK_{r-1}/K_{r-1} on a block G/H_{r-1} is transitive. It therefore remains to show that $U \cap H_{r-1}$ is transitive in its action on a given block H_{r-1}/H_r. Since $\mathrm{soc}(K_{r-1}) \triangleleft G$, Lemma 3.10 shows that U must contain every nonabelian composition factor of $\mathrm{soc}(K_{r-1})$. Let Γ denote the image of the action $\psi : H_{r-1} \to \mathrm{Sym}(H_{r-1}/H_r)$. Since Γ is nonabelian almost simple and $K \neq 1$, Remark 3.2 implies that the projection $\psi(\mathrm{soc}(K_{r-1}))$ to any block is a nontrivial normal subgroup of Γ. Since Γ is primitive, $\psi(\mathrm{soc}(K_{r-1}))$ and hence $U \cap H_{r-1}$ is transitive on H_{r-1}/H_r, completing the induction.

To show that 1) and 2) hold, identify the image $\Gamma_i' \leq \mathrm{Sym}((H_{i-1} \cap U)/(H_i \cap U))$ of the action of $H_{i-1} \cap U$ with a subgroup of Γ_i. Then Γ_i' is almost simple with the same socle $\mathrm{soc}(\Gamma_i)$, so that 1) holds. Since $\mathrm{soc}(K_i)$ is a direct product of nonabelian simple groups by Lemma 3.1 and its composition factors are contained in U as above, $\mathrm{soc}(K_i)$ is contained in the kernel $\bigcap_{u\in U}(H_i \cap U)^u$ of the action of U on cosets of $H_i \cap U$, $i = 1, \dots, r$, so that these kernels are pairwise disjoint. □

Remark 3.11. In the setup of Corollary 3.9, we may identify $\mathrm{Mon}_k(g_i')$ as a subgroup of $\mathrm{Mon}_k(g_i)$ as in Remark 2.13. Then the kernel of $\mathrm{Mon}_k(g_i') \to \mathrm{Mon}_k(g_{i-1}')$ contains the socle of the kernel of $\mathrm{Mon}_k(g_i) \to \mathrm{Mon}_k(g_{i-1})$. Indeed, as the groups U and H_i, $i = 1, \dots, r$ in the proof of the corollary satisfy all of the hypotheses of Lemma 3.8, the final step of the proof of the lemma yields the desired conclusion.

4. The main tool

The following proposition establishes a machinery to compare low genus subcovers of the Galois closure $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ of polynomial coverings $f : \mathbb{P}^1_k \to \mathbb{P}^1_k$, 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.

Proposition 4.1. *Let $f = f_1 \circ \cdots \circ f_r$ for indecomposable polynomials $f_i \in k[x]$ with nonsolvable monodromy group. Let $f_V = f_U \circ h'$ be a subcover of the Galois closure of f such that f_U is a composition of coverings with affine monodromy groups while h' is indecomposable whose monodromy group Γ is nonsolvable with a solvable quotient $\Gamma/\mathrm{soc}(\Gamma)$. Then there exists a subcover h of f_V with the same Galois closure as f_1.*

Proof. As usual denote by $f_C : \tilde{X}/C \to \mathbb{P}^1_k$ the subcover corresponding to $C \leq \mathrm{Mon}_k(f)$. First note that the (nonsolvable) monodromy groups of $f_1, \dots, f_r$ have primitive nonabelian simple socles by Theorem 2.1. Moreover, $g_{i+1} := f_1 \circ \cdots \circ f_{i+1}$ is not a subcover of the Galois closure of g_i by Lemma 2.8, or equivalently the kernel K_i of the projection $\mathrm{Mon}_k(g_i) \to \mathrm{Mon}_k(g_{i-1})$ is nontrivial, for $i = 1, \dots, r-1$.

We first show that the pullback f' of f along f_U has similar properties to the above properties of f. First note that in view of our assumptions on f_U and f_i, $i = 1, \dots, r$, U is transitive by Lemma 3.8. Thus, letting $G_1 \leq \mathrm{Mon}_k(f)$ be a point stabilizer, f' is equivalent to the projection $\tilde{X}/(U \cap G_1) \to \tilde{X}/U$ by Remark 2.10, and f' has the same Galois closure $\tilde{X}$ as f by Lemma 2.12. As the socles of $\Gamma_i := \mathrm{Mon}_k(f_i)$ are primitive and nonabelian simple, Corollary 3.9 implies that f' decomposes as $f'_1 \circ \cdots \circ f'_r$ for indecomposable f'_i, $i = 1, \dots, r$ with almost simple monodromy groups. Since $g'_i := f'_1 \circ \cdots \circ f'_i$ is the pullback of g_i along f_U, we shall henceforth identify $\mathrm{Mon}_k(g'_i)$ as a subgroup of $\mathrm{Mon}_k(g_i)$ for all i, as in Remark 2.13. Moreover, Remark 3.11 then shows that the kernel K'_i of the projection $\mathrm{Mon}_k(g'_i) \to \mathrm{Mon}_k(g'_{i-1})$ contains $\mathrm{soc}(K_i)$ and in particular is nontrivial.

Since f' has Galois closure $\tilde{f}' : \tilde{X} \to \tilde{X}/U$ as shown above, we may regard h' as a subcover of the Galois closure of f'. Suppose $1 \leq s \leq r$ is minimal for which h' is a subcover of the Galois closure of g'_s. We claim that $s = 1$.

Since $\mathrm{Mon}_k(g'_i)$ is a transitive subgroup of $\mathrm{Mon}_k(g_i)$ and since $\mathrm{soc}(K_i) \leq \mathrm{Mon}_k(g'_i)$ as above, Corollary 3.6 and Remark 3.7 imply that $\mathrm{soc}(K_i)$ is the unique minimal normal subgroup of $\mathrm{Mon}_k(g'_i)$. Letting $\phi : A \to \Gamma$ be the natural projection, it follows that either $\mathrm{soc}(K_s) \subseteq \ker\phi$ or $\ker\phi = 1$. In the former case, since $K_s/\mathrm{soc}(K_s) \leq (\Gamma_s/\mathrm{soc}(\Gamma_s))^{\deg g_{s-1}}$ by Lemma 3.1, $K_s/\mathrm{soc}(K_s)$ is solvable by Schreier's conjecture, and hence so is $K'_s/\mathrm{soc}(K_s)$ and $\phi(K'_s)$. Since Γ is primitive (as h' is indecomposable) and $\mathrm{soc}(\Gamma)$ is nonabelian, Γ has no nontrivial solvable normal subgroups by Aschbacher–O'Nan–Scott [27, §11]. Thus $\phi(K'_s) = 1$ and h' is a subcover of the Galois closure of g'_{s-1}, contradicting the minimality of s.

Henceforth, we may assume $\ker\phi = 1$, that is, the Galois closure of h' is the same as that of g'_s. Since $\Gamma/\mathrm{soc}(\Gamma)$ is solvable, and $\mathrm{Mon}_k(g'_{s-1})$ is a nonsolvable quotient of $\mathrm{Mon}_k(g'_s)/\mathrm{soc}(K_s)$ for $s > 1$, the claim follows. Note that as $\mathrm{Mon}(f'_1)$ is almost simple, the Galois closure of h' in fact coincides with that of f'_1.

Let $\tilde{f}_1 : \tilde{X}_1 \to \mathbb{P}^1$ be the Galois closure of f_1 and $\phi_1 : \mathrm{Mon}(f) \to \mathrm{Mon}(f_1)$ 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 $\tilde{X}/(\ker(\phi_1)\cdot V) \to \tilde{X}/\mathrm{Mon}(f)$, and hence is also a subcover of $f_V : \tilde{X}/V \to \tilde{X}/\mathrm{Mon}(f)$. Moreover, since $\phi_1(V)$ has trivial core in $\mathrm{Mon}(f'_1)$ and hence in $\mathrm{Mon}(f_1)$, the Galois closure of h is the same as that of f_1. □

Note that the only facts about the polynomials $f_1, \dots, f_r$ used in the proof are: 1) $\mathrm{Mon}_k(f_i)$ is almost simple with primitive socle; 2) $f_1 \circ \cdots \circ f_r$ has a unique decomposition up to composition with linear polynomials (Theorem 2.9); and 3) $g_{i+1} = f_1 \circ \cdots \circ f_{i+1}$ does not factor through the Galois closure of g_i. Thus, one may replace $f_1, \dots, f_r$ in the proposition by arbitrary coverings satisfying 1)-3).

5. Proof of Theorems 1.1 and 1.2

5.1. **Reductions.** In this section we apply Proposition 4.1 to reduce Theorems 1.1 and 1.2 to assertions regarding merely the first composition factor f_1. Throughout this section k is finitely generated. For a number field k, let O_k be its ring of integers.

Corollary 5.1. *Suppose $f = f_1 \circ \cdots \circ f_r \in k[x]$ for indecomposable polynomials f_i, $i = 1, \dots, r$ with nonsolvable monodromy groups over a number field k. Then $\mathrm{Red}_f(O_k)$ is contained in the union of a finite set with $\bigcup_h (h(k) \cap O_k)$, where h runs over Siegel functions with the same Galois closure as f_1.*

Proof. Let $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$ be the Galois closure of f over k, and A its arithmetic monodromy group. By Corollary 2.5, Red_f is the union of a finite set with $\bigcup_D f_D(k)$, where $D \le A$ runs over maximal intransitive subgroups satisfying $D \cdot \mathrm{Mon}_{\overline{k}}(f) = A$, and f_D is a Siegel function equivalent to the projection $f_D : \tilde{X}/D \to \mathbb{P}^1_k$.

Since such D is intransitive, Corollary 3.9 implies that f_D is not a composition of coverings with affine monodromy. Thus, f_D has a minimal subcover $f_V : \tilde{X}/V \to \mathbb{P}^1_k$, $D \le V \le A$ with decomposition $f_V = f_U \circ h'$, $V \le U \le A$, such that $f_U : \tilde{X}/U \to \mathbb{P}^1_k$ is a composition of Siegel functions with affine monodromy and an indecomposable Siegel function $h' : \tilde{X}/V \to \tilde{X}/U$ with nonaffine (hence nonsolvable) monodromy.

Proposition 4.1 then implies that there exists a subcover h of f_V with the same Galois closure as f_1. Since f_D is a Siegel function, so is h. The claim now follows since clearly $f_D(k) \subseteq h(k)$. □

Corollary 5.2. *Let $f = f_1 \circ \cdots \circ f_r$ for indecomposable $f_i \in k[x]$, $i = 1, \dots, r$ with nonsolvable monodromy groups, such that the Galois closure of f_1 is of genus > 1. Then Red_f is contained in the union of a finite set and $\bigcup_h h(X(k))$, where $h : X \to \mathbb{P}^1_k$ runs over coverings of genus $g_X \le 1$ with the same Galois closure as f_1.*

Proof. The proof is similar to that of Corollary 5.1 but applies Proposition 4.1 over $\overline{k}$. Letting $\tilde{f} : \tilde{X} \to \mathbb{P}^1_k$, $\tilde{f}_{\overline{k}} : \tilde{X}_{\overline{k}} \to \mathbb{P}^1_{\overline{k}}$, A and G, be the Galois closures of f over k and $\overline{k}$, and arithmetic and geometric mondromy groups of f, respectively. Let $f_D : \tilde{X}/D \to \mathbb{P}^1_k$ be a genus ≤ 1 subcover of $\tilde{f}$ for maximal intransitive $D \le A$ satisfying $D \cdot G = A$.

The subgroup $C := D \cap G$ is also intransitive, so that the subcover f_C of $\tilde{f}_{\overline{k}}$ is not a composition of coverings with affine monodromy. Thus, f_C has a minimal subcover $f_V : \tilde{X}_{\overline{k}}/V \to \mathbb{P}^1_{\overline{k}}$, $C \le V \le G$ with decomposition $f_V = f_U \circ h'$, $V \le U \le G$, such that $f_U : \tilde{X}_{\overline{k}}/U \to \mathbb{P}^1_{\overline{k}}$ is a composition of coverings with affine monodromy, and $h' : \tilde{X}_{\overline{k}}/V \to \tilde{X}_{\overline{k}}/U$ is an indecomposable covering with nonaffine (hence nonsolvable) monodromy group. Note that $\tilde{X}_{\overline{k}}/U$ is of genus 0, since otherwise h' is a covering between genus 1 curves, hence with abelian monodromy [56, Theorem

4.10(c)], contradicting the assumption that its monodromy is nonaffine. Theorem 2.3 then implies that the proper quotients of $\mathrm{Mon}_{\overline{k}}(h')$ are solvable. Thus, the conditions of Proposition 4.1 hold over $\overline{k}$.

Proposition 4.1 then implies that there exists a subcover of f_V with the same Galois closure as f_1. Letting $\pi : A \to \Gamma_1$ be the projection to $\Gamma_1 := \mathrm{Mon}_k(f_1)$ and noting that Γ_1 is nonabelian almost simple by Theorem 2.1, it follows that $\pi(V)$ and hence $\pi(C)$ does not contain $\mathrm{soc}(\Gamma_1)$. We claim that $\pi(D)$ does not contain $\mathrm{soc}(\Gamma_1)$ and hence the natural projection $h : \tilde{X}/(\ker\pi \cdot D) \to \mathbb{P}^1_k$ has the same Galois closure as f_1. To see this, assume on the contrary $\pi(D)$ contains $\mathrm{soc}(\Gamma_1)$ and hence $\pi(D) \leq \Gamma_1$ is almost simple with the same socle. Note that $C \lhd D$ since $G \lhd A$, and hence $\pi(C) \lhd \pi(D)$. Since $\pi(D)$ is almost simple and $\pi(C)$ does not contain $\mathrm{soc}(\Gamma_1)$, this implies $\pi(C) = 1$. However, the latter contradicts the assumption that f_1 has Galois closure of genus > 1, proving the claim.

Since h is a subcover of f_D, it follows that $f_D(\tilde{X}/D(k)) \subseteq h(X(k))$, where $X := \tilde{X}/(\ker\pi \cdot D)$. Thus Corollary 2.5 implies that Red_f is contained in the union of a finite set with $\bigcup_h h(X(k))$, where $h : X \to \mathbb{P}^1_k$ runs over coverings of genus $g_X \leq 1$ with the same Galois closure as f_1. □

Corollary 5.3. *Let $f = f_1 \circ \cdots \circ f_r$ be the composition of indecomposable polynomials $f_i \in \mathbb{C}[x]$ with nonsolvable monodromy group. Assume $f(x) - h(y) \in \mathbb{C}[x, y]$ is reducible for nonlinear $h \in \mathbb{C}[y]$. Then $h = h_1 \circ g$ for $g, h_1 \in \mathbb{C}[x]$ such that h_1 has the same Galois closure as f_1.*

Proof. The reducibility of $f(x) - h(y) \in \mathbb{C}[x, y]$ implies the reducibility of the normalization of the curve defined by $f(x) - h(y) = 0$. This curve is (the normalization of) the fiber product of the maps $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ and $h : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. By Lemma 2.11, we may replace h by a common polynomial subcover h_4 of h and of the Galois closure $\tilde{f}$, whose fiber product with f is still reducible. It follows that h_4 is not a composition of polynomials with affine monodromy groups by Corollary 3.9.

We may therefore pick a minimal polynomial subcover $h_2 \circ h_3$ of h_4 which is not a composition of polynomials with affine monodromy groups, so that h_2 is a composition of polynomials with affine monodromy groups, and h_3 is indecomposable and $\Gamma := \mathrm{Mon}_{\mathbb{C}}(h_2)$ is nonaffine. As Γ is nonaffine, Theorem 2.1 implies that it is nonabelian almost simple, and in particular $\Gamma/\mathrm{soc}(\Gamma)$ is solvable. We may therefore apply Proposition 4.1 to deduce that $h_2 \circ h_3$ has a polynomial subcover h_1 with the same Galois closure as f_1. □

5.2. **A classification theorem.** The combination of [42] and [29, §1.2] gives:

Theorem 5.4. *Let $f : \mathbb{P}^1_{\overline{k}} \to \mathbb{P}^1_{\overline{k}}$ be an indecomposable polynomial covering over $\overline{k}$ of degree > 20, and $\tilde{f} : \tilde{X} \to \mathbb{P}^1$ its Galois closure. For every indecomposable subcover $h : Y \to \mathbb{P}^1$ with Galois closure $\tilde{f}$ and genus $g_Y \leq 1$, one of the following holds:*

TABLE 1. Ramification types of polynomial maps $\mathbb{P}^1_k \to \mathbb{P}^1_k$ of degree $\ell > 20$ and monodromy group A_ℓ or S_ℓ for which the genus of the quotient by a 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.

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

(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 genus 0 covering $\tilde{X}/G_2 \to \mathbb{P}^1$ where G_2 is the stabilizer of a set of cardinality 2.*
(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.* [4]

Remark 5.5. 1) Note that for polynomials of degree $10 \leq \deg f \leq 20$ the corresponding subcovers h are also listed in [42] and [29, Theorem A.4.1].
2) In Case (1), either $G = A_n$, S_n or M_{23}. Letting $A = \mathrm{Mon}_k(f)$, one has $A = G$ in case (3) or if $G = M_{23}$ since in these cases the symmetric normalizer of G is G.
3) The only groups in Theorem 5.4 which appear as the monodromy group of a polynomial over $\mathbb{Q}$ are alternating and symmetric.

5.3. **Deducing the theorems.** We first deduce the first assertion of Theorem 1.1 from Corollary 5.1 by applying the classification of Siegel functions:

Proof of Theorem 1.1 for integral values. Note that since $f_1, \dots, f_r$ are of degree ≥ 5 and are not linearly related to x^n or Chebyshev, $\mathrm{Mon}_{\mathbb{Q}}(f_i)$, $i = 1, \dots, r$ are nonabelian

[4] 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 [9].

almost simple by Theorem 2.1. Thus, Corollary 5.1 implies that $\mathrm{Red}_f(\mathbb{Z})$ is contained in the union of a finite set with $\bigcup_h (h(\mathbb{Q}) \cap \mathbb{Z})$, where h runs over Siegel functions with the same Galois closure as f_1. To show that equality holds, it suffices to show that $h(\mathbb{Q}) \cap \mathbb{Z}$ is contained in $\mathrm{Red}_{f_1}(\mathbb{Z})$ for such h.

As $f_1(\mathbb{Q}) \cap \mathbb{Z} \subseteq \mathrm{Red}_{f_1}(\mathbb{Z})$, it suffices to consider Siegel functions h arising in a different monodromy action of $\Gamma := \mathrm{Mon}_{\mathbb{Q}}(f_1)$, not equivalent to that of f_1. Since this action may be assumed minimally nonsolvable and Γ is almost simple, this means that either Γ must induce a Siegel function in a second action *permutation-equivalent* to that of $\mathrm{Mon}_{\mathbb{Q}}(f_1)$; or some subgroup between Γ and its socle must induce a Siegel function in a *different* primitive action. From the classification of primitive monodromy groups of Siegel functions in [43] (in particular Theorems 4.8 and 4.9), one extracts using a computer check that the first scenario happens only for $\mathrm{Mon}_{\overline{k}}(f_1) \in \{\mathrm{PSL}_2(11), \mathrm{PSL}_3(2), \mathrm{PSL}_3(3), \mathrm{PSL}_4(2), \mathrm{P\Gamma L}_3(4), \mathrm{PSL}_5(2)\}$, whereas the second one only happens for $\mathrm{Mon}_{\overline{k}}(f_1) \in \{A_5, S_5, \mathrm{PSL}_3(2), \mathrm{P\Gamma L}_2(9), M_{11}, \mathrm{PSL}_4(2)\}$. Out of those possibilities, only the polynomials with monodromy group S_5 and $\mathrm{P\Gamma L}_2(9)$ can be defined over $\mathbb{Q}$ (Remark 5.5), and for the latter group the Siegel function h does not have two poles of the same order, and so is not a Siegel function over $\mathbb{Q}$, cf. e.g. [43, §4.4]. □

Note that by invoking [43] over a general number field k instead, the same proof shows that $\mathrm{Red}_f(O_k)$ is the union of $\mathrm{Red}_{f_1}(O_k)$ and a finite set if one assumes k is a number field and merely[5] that $\deg f_1 > 15$.

The rest of the assertions of Theorem 1.1 follow from the following theorem which itself follows from Corollary 5.2 and Theorem 5.4.

Theorem 5.6. *Let k be finitely generated, and $f = f_1 \circ \cdots \circ f_r$ for indecomposable $f_i \in k[x]$ of degree ≥ 5, none of which is $\mu \circ x^n \circ \nu$ or $\mu \circ T_n \circ \nu$ for linear $\mu, \nu \in \overline{k}[x]$. If $\deg(f_1) > 20$, then Red_f is the union of Red_{f_1} and a finite set.*

In particular, either (1) Red_f is the union of $f_1(k)$ and a finite set, or (2) there exists (a single) $f_1' \in k(x)$ such that Red_f is the union of $f_1(k) \cup f_1'(k)$ and a finite set. In the latter case, either the ramification of f_1 is as in Table 1, or $k \neq \mathbb{Q}$ and f_1 is one of the two cases in Theorem 5.4.(3).

Proof. First note that $\mathrm{Mon}_k(f_i)$, $i = 1, \ldots, r$ are nonsolvable by Theorem 2.1. Since $\deg f_1 > 20$ and $\mathrm{Mon}_k(f_1)$ is nonsolvable, the Galois closure of f_1 is of genus > 1, e.g. by [30, Proposition 2.4]. Thus Corollary 5.2 implies that Red_f is contained in the union of a finite set and $\bigcup_h h(X(k))$, where $h : X \to \mathbb{P}^1_k$ runs over genus ≤ 1 subcovers of the Galois closure of f_1. To show that equality holds, it suffices to show that $h(X(k))$ is contained in Red_{f_1} for all such h. Note that $A := \mathrm{Mon}_k(f_1)$ is

[5]Here 15 is the degree of the action of $\mathrm{PSL}_4(2)$ from the second list of groups in the above proof.

nonabelian almost simple by Theorem 2.1 since f_1 is of degree ≥ 5 and is not linearly related to x^n or Chebyshev.

By Theorem 5.4 and Remark 5.5, the only possible nonsolvable geometric monodromy groups $G = \mathrm{Mon}_{\overline{k}}(f_1)$ for indecomposable f_1 of degree > 20, which are nonalternating and nonsymmetric, are $\mathrm{P\Gamma L}_3(4), M_{23}$ and $\mathrm{PSL}_5(2)$. In these cases $A = G$ and $k \neq \mathbb{Q}$ by Remark 5.5.(2)-(3). Moreover, 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) holds. For $\mathrm{P\Gamma L}_3(4)$ and $\mathrm{PSL}_5(2)$, the Galois closures of the corresponding polynomials have only one other equivalence class of subcovers of genus ≤ 1, and its stabilizer is intransitive, whence $h(X(k)) \subseteq \mathrm{Red}_{f_1}$ and (2) holds. Note that these cases do not occur over $\mathbb{Q}$ as well by Remark 5.5.

Henceforth, we may assume $A = A_n$ or S_n in their natural action. We may assume h is minimal with the same Galois closure as f_1, and that it is not equivalent to f_1. Let $D \leq A$ be its stabilizer, and set $C := D \cap G$. By [41, Theorem 5.3][6], either $C \geq A_{n-1}$ or $C \gneq A_{n-2}$ and the ramification of f_1 is in Table 1. As $D \supseteq C$ is maximal for which A acts faithfully on A/D, it follows that D is either a stabilizer $A_1 := A \cap S_{n-1}$ in the natural action or a stabilizer $A_2 = A \cap (S_{n-2} \times S_2)$ of a set of cardinality 2, and in the latter case the ramification of f_1 is in Table 1. The former case $D = A_1$ does not occur since h is not equivalent to f_1. In the latter case $D = A_2$, it is intransitive, and hence $h(X(k)) \subseteq \mathrm{Red}_{f_1}$ and (2) holds. □

When adding the lists from Remark 5.5.(1) as exceptions to Theorem 5.6, the same proof would lower the degree assumption on f_1 to merely $\deg f_1 \geq 10$. In particular over $k = \mathbb{Q}$, Theorem 5.6 holds for polynomials f_1 of degree $\deg f_1 > 10$ without adding further exceptions.

Finally we conclude Theorem 1.2 from Corollary 5.3 and Theorem 5.4:

Proof of Theorem 1.2. 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 by Theorem 2.1. Thus we may apply Corollary 5.3 to obtain a polynomial subcover h_1 of h with the same Galois closure as of f_1.

Since $\deg f_1 > 31$, the possibilities for h_1 are described in cases (1)-(2) of Theorem 5.4. In fact, as both h_1 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_1 and f_1 are equivalent, as desired. □

[6]Theorem 5.3 of [41] is based on the work of Guralnick–Shareshain [29] but no other results in the classification of monodromy groups are used.

Appendix A. Proof of Theorem 2.3

The proof requires the following addition to Shih's paper [55]. More generally, a classification of indecomposable genus 1 coverings with more than one minimal normal subgroup is addressed in [40].

Proposition A.1. *Let $f : X \to \mathbb{P}^1$ be an indecomposable covering of genus $g_X \leq 1$ whose monodromy group G has more than one minimal normal subgroup. Then $G/\operatorname{soc}(G)$ is solvable.*

Proof. Since G has more than one minimal normal subgroup, it has two isomorphic nonabelian minimal normal subgroup by the Aschbacher-Scott theorem [27, Theorem 11.2], so that $\operatorname{soc}(G) \cong L^{2t}$ for a nonabelian simple group L and $t \geq 1$.

We claim that the proof in Shih's paper yields that $t = 1$ even under the mere assumption $g_X \leq 1$, showing that $\operatorname{soc}(G) \cong L^2$. Since $G/\operatorname{soc}(G)$ embeds into $\operatorname{Aut}(L^2)/\operatorname{Inn}(L)^2 \cong (\operatorname{Aut}(L)/\operatorname{Inn}(L))^2 \rtimes S_2$ and $\operatorname{Aut}(L)/\operatorname{Inn}(L)$ is solvable by Schreier's conjecture, this shows that $G/\operatorname{soc}(G)$ is solvable, proving the proposition.

To prove the claim, we follow closely the proof of [55] and use the notation of [55, §1-2]: Let $S = [g_1, \dots, g_r]$ be a tuple with product 1 which is associated to f and generates G. Let $\operatorname{orb}(g_1)$ denote the multiset of orbits of g_1 and set $n := \deg f$. As $g_X \leq 1$, the Riemann–Hurwitz formula implies that

$$0 \geq 2(g_X - 1) = -2n + \sum_{i=1}^{r} (n - \#\operatorname{orb}(x_i)),$$

or equivalently $u(S) \geq r - 2$, where $u(g_i) := \#\operatorname{orb}(x_i)/n$ and $u(S) := \sum_{i=1}^{r} u(g_i)$, following the notation of [55, §2]. Shih's proof uses the assumption $g_X = 0$ only in order to make sure the strict inequality $u(S) > r - 2$ holds. However, we show below that already the inequality $u(S) \geq r - 2$ (or $g_X \leq 1$) suffices for his proof.

As in [55, (4.8)], one first shows that $r \leq 4$ using [55, (4.7)]. Indeed, by [55, (4.7).(1)], one has $u(g_i) \leq 3/5$, so that $r - 2 \leq u(S) \leq 3r/5$. The latter shows that $r \leq 5$ with equality only if $u(g_i) = 3/5$ for all i. However, [55, (4.7).(2-3)] show that $u(g_i) \leq \max\{7/20, 11/30, 8/15, 11/20\} = 11/20 < 3/5$, so that indeed $r \leq 4$.

For $L \neq A_5$, Part (i) of [55, (4.9)] shows that in fact $r = 3$. For $L = A_5$ and $r = 4$, Part (ii) of [55, (4.9)] shows that three of the g_i's are involutions, and the remaining, say g_4, is of order $m \geq 3$. This case is ruled out using merely $u(S) \geq r - 2 = 2$: Indeed, $u(g_i) \leq 11/20$ for $i = 1, 2, 3$ by [55, (4.9).(3)] and

$$u(g_4) \leq 1/m + \frac{m-1}{m} \cdot \frac{1}{n} \max_{1<i<m} \{f(g_4^i)\}$$

by [55, (2.1).(2)]. Since this maximum is at most $1/10$ by [55, (4.7)], the right hand side is strictly smaller than $1/4+1/10 = 7/20$ if $m \geq 4$. For $m \geq 4$, in total we have

$$u(S) = \sum_{i=1}^{3} u(g_i) + u(g_4) < 3 \cdot 11/20 + 7/20 = 2,$$

contradicting $u(S) \geq 2$. The case $m = 3$ is ruled out in [55, (4.9)] already using merely the inequality $u(S) \geq 2$, as needed.

Henceforth assume $r = 3$ and let k, ℓ, m be the orders of g_1, g_2, g_3, respectively. Without loss of generality, we assume $k \leq \ell \leq m$. Then [55, (4.11)] asserts that (k, ℓ, m) is one of the tuples $(2, 3, m)$, $7 \leq m \leq 18$, or $(2, 4, m)$, $5 \leq m \leq 35$, or $(2, 5, m)$, $5 \leq m \leq 10$, or $(2, 6, m)$, $m = 6, 7, 8$, or $(3, 3, m)$, $m = 4, 5$, or $(3, 4, 4)$. The only estimate of $u(S)$ used are those in [55, (4.10)] whose proof applies in the same way when replacing the inequality $u(S) > 1$ with the inequality $u(S) \geq 1$.

Finally, [55, (4.17)-(4.21)] show that $t = 1$: This relies on [55, (4.16)] which applies the inequality $u(S) \geq 1$ in order to deduce that (k, ℓ, m) is $(2, 3, 8)$, or $(2, 4, 5)$ or $(2, 4, 6)$. However, we note that for $(k, \ell, m) = (2, 3, 7)$ or $(2, 3, 10)$ the estimates on $u(S)$ in the proof of [55, (4.16)] do not contradict even the inequality $u(S) > 1$, leaving these cases open. In these cases we refine the estimates as follows. Let $f(g)$ denote the number of fixed points of $g \in G$. If $(k, \ell, m) = (2, 3, 10)$, then [55, (2.1).(1)] gives:

$$u(g_3) \leq \frac{1}{10}(1 + \frac{f(g_3^5)}{n} + 4\frac{f(g_3^2)}{n} + 4\frac{f(g_3)}{n}). \tag{A.1}$$

One has $f(g_3^5)/n \leq 1/15$ as in [55, (4.7).(3)] for $L \neq A_5$, and $f(g_3^2)/n \leq 1/12$ by [55, (4.6).(2)], and $f(g_3^2)/n \leq 1/60$ by the assumption of [55, (4.16)]. Thus, (A.1) gives $u(g_3) \leq 11/75$. As $u(g_1) + u(g_2) \leq 307/360$ as in [55, (4.16)], one gets $u(S) \leq 1799/1800$, contradicting $u(S) \geq 1$. For $(k, \ell, m) = (2, 3, 7)$, [55, (2.1).(1)] gives $u(g_3) \leq (1/7)(1 + 6f(g_3)/n)$. As $f(g_3)/n \leq 1/60$ by assumption of [55, (4.16)], one has $u(g_3) \leq 61/420$. As $u(g_1) + u(g_2) \leq 307/360$, this gives $u(S) \leq 503/504$, contradicting $u(S) \geq 1$. Now, [55, (4.16)] and the above addition in case $(k, \ell, m) = (2, 3, 7)$ or $(2, 3, 10)$ implies that the inequality $u(S) \geq 1$ suffices for [55, (4.17)-(4.21)]. □

Proof of Theorem 2.3. We use the Aschbacher–O'Nan–Scott structure theory of primitive groups [27, Theorem 11.2]. Since G is assumed to be nonaffine, $\mathrm{soc}(G)$ is isomorphic to a power L^t of a nonabelian simple group L. Proposition A.1 shows that either $\mathrm{soc}(G)$ is the (unique) minimal normal subgroup, or $G/\mathrm{soc}(G)$ is solvable. Henceforth assume $\mathrm{soc}(G)$ is the unique minimal normal subgroup of G.

Consider the action of G on the set $\Delta = \{L_1, \ldots, L_t\}$ of simple direct factors in $\mathrm{soc}(G)$, and let K be its kernel. Since $2(g_X - 1) < \deg f/1000$ and G is nonaffine,

[30, Theorem 9.3] implies that either G/K is solvable or $G/K \cong A_5$ or S_5 with $t = 5$. Since $L^t \le K \le \mathrm{Aut}(L)^t$ and $\mathrm{Aut}(L)/L$ is solvable by Schreier's conjecture, it follows that $G/\mathrm{soc}(G) \cong (G/K)/(K/\mathrm{soc}(G))$ is solvable when G/K is. In particular, since S_t is solvable for $t \le 4$, we may henceforth assume $t \ge 5$.

In case $\mathrm{soc}(G)$ acts regularly, we follow the argument of [30, Corollary 9.4]: Since a nontrivial normal subgroup of a primitive group acts transitively, we have $H\,\mathrm{soc}(G) = G$, where H is a point stabilizer. Moreover, as $\mathrm{soc}(G)$ is regular, we have $H \cap \mathrm{soc}(G) = 1$ and $G = H \ltimes \mathrm{soc}(G)$. Thus H acts transitively on Δ, and hence the stabilizer H_1 of $L_1 \in \Delta$ in this action is of index at least $t \ge 5$, while the kernel $H \cap K$ of this action is solvable since $H \cap \mathrm{soc}(G) = 1$ and $K/\mathrm{soc}(G)$ is solvable. However, the image of the action $H_1 \to \mathrm{Aut}(L_1)$ contains the group of inner automorphisms on L_1 by [3, Theorem 1][7]. As $H \cap K$ is solvable and is contained in H_1, it follows that $H/H \cap K$ contains a nonsolvable subgroup $H_1/H_1 \cap K$ of index ≥ 5. Thus $H/H \cap K \ncong A_5, S_5$ and is nonsolvable. As $G/K \cong H/H \cap K$ (since $HK = G$) the same conclusion holds for G/K, contradicting the above conclusion from [30, Theorem 9.3].

Henceforth assume $\mathrm{soc}(G)$ is not regular, that is, $H \cap \mathrm{soc}(G) \ne 1$. The coverings for which $H \cap L_1 = 1$ and $2(g_X - 1) < \deg f/168$, were classified in [2, Theorem]. As explained in [2, (11.1) and (19.1)], the resulting coverings have monodromy group $G \le S_5 \wr S_2$ with $\mathrm{soc}(G) = A_5^2$, so that $G/\mathrm{soc}(G)$ is solvable.

Henceforth assume $H \cap L_1 \ne 1$, in which case the group is called of product type. In this case, as $g_X \le 1$, [28, Theorem 7.1] implies that[8] either $G/\mathrm{soc}(G) \cong A_5$ such that its regular action is of genus 0, or that $G \le S_\ell \wr S_5$ with $\ell \le 10$ and $G/\mathrm{soc}(G) \cong S_5$ with regular action of ramification type $[2^{60}], [4^{30}], [5^{24}]$. The first case is ruled out by [28, Theorem 8.6], whereas a straightforward computer check shows that the second case does not occur with genus $g_X \le 1$. □

References

[1] N. Adrianov, Primitive monodromy groups of rational functions with one multiple pole. Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI), Kombinatorika i Teoriya Grafov. 446 (2016), 12–30. 3

[2] M. Aschbacher, On conjectures of Guralnick and Thompson. J. Algebra 135 (1990), 277–343. 23

[3] M. Aschbacher, L. Scott, Maximal subgroups of finite groups. J. Algebra 92 (1985), 44–80. 10, 23

[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. 1, 2

[7] More specifically, see the definition of n_1^* in [3, Theorem 1].

[8] [30, Theorem 9.3] allows a case where $A_5^5 < G \le S_5 \wr S_5$, and $G/K \cong S_5$, and the covering $\tilde{X}/K \to \mathbb{P}^1$, obtained as the quotient of the Galois closure $\tilde{X}$ of f by K, has three branch points with branch cycles x_1, x_2, x_3 of orders $2, 4, 6$, respectively. A straightforward computer check shows that there is no genus ≤ 1 product 1 tuple x_1, x_2, x_3 generating such G, ruling out this case.

[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] L. Bary-Soroker, and A. Fehm, S. Petersen, On varieties of Hilbert type. Ann. Ins. Fourier 64 (2014), 1893–1901. 1
[7] 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. 1
[8] Y. Bilu, R. Tichy, The Diophantine equation $f(x) = g(y)$. Acta Arith. 95 (2000), 261–288. 1
[9] P. Cassou-Noguès, J. Couveignes, Factorizations explicites de $g(y)-h(z)$. Acta Arith. 87 (1999), 291–317. 2, 18
Illig, Peter; Jones, Rafe; Orvis, Eli; Segawa, Yukihiko; Spinale, Nick Newly reducible polynomial iterates. Int. J. Number Theory 17 (2021), no. 6, 1405–1427
[10] K. Chamberlin, E. Colbert, S. Frechette, P. Hefferman, R. Jones, S. Orchard, Newly reducible iterates in families of quadratic polynomials. Involve 5 (2012), 481–495. 1
[11] P. Corvaja, U. Zannier, On the Hilbert property and the fundamental group of algebraic varieties. Math. Z. 286 (2017), 579–602. 1
[12] H. Davenport, D. J. Lewis, A. Schinzel, Equations of the form $f(x) = g(y)$. Quarterly J. of Math. 12 (1961), 304–312. 2
[13] H. Davenport, A. Schinzel, Two problems concerning polynomials. J. Reine Angew. Math. 214 (1964), 386–391. 2
[14] P. Dèbes, M. D. Fried, Integral specialization of families of rational functions. Pacific J. Math. 190 (1999), 45–85. 2
[15] P. Dèbes, F. Legrand, Twisted covers and specializations. 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. 4
[16] J. D. Dixon, B. Mortimer, Permutation Groups. Springer GTM 163 (1996). 5, 11
[17] 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
[18] M. D. Fried, R. E. MacRae, On the invariance of chains of fields. Illinois J. Math. 13 (1969), 165–171. 4, 9
[19] M. D. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables. Illinois J. Math. 17 (1973), 128–146. 2
[20] M. D. Fried, On a theorem of Ritt and related Diophantine problems. J. Reine Angew. Math. 264 (1973), 40–55. 1
[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. 8
[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. 8
[24] M. D. Fried, I. Gusić, Schinzel's problem: imprimitive covers and the monodromy method. Acta Arith. 155 (2012), 27–40. 2
[25] D. Frohardt, R. Guralnick, C. Hoffman, K. Magaard, Monodromy groups of coverings of curves. In preparation. 3
[26] D. Ghioca, T. J. Tucker, M. E. Zieve, Linear relations between polynomial orbits. Duke Math. J. 161 (2012), 1379–1410. 1

[27] R. Guralnick, Monodromy Groups of Coverings of Curves. Galois Groups and Fundamental Groups, MSRI Publications 41 (2003). 11, 15, 21, 22
[28] R. Guralnick, M. Neubauer, Monodromy groups of branched coverings: the generic case. Contemp. Math. 186 (1995), 325–352. 23
[29] 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). 2, 3, 17, 18, 20
[30] R. Guralnick, J. Thompson, Finite groups of genus zero. J. Algebra 131 (1990), 303–341. 19, 23
[31] D. Hilbert, Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. J. Reine Angew. Math. 110 (1892), 104–129. 1
[32] B. Huppert, Primitive, auflösbare Gruppen, Arch. Math. 6 (1955), 303–310. 5
[33] P. Illig, R. Jones, E. Orvis, Y. Segawa, N. Spinale, Newly reducible polynomial iterates. Int. J. Number Theory 17 (2021), 1405–1427. 1
[34] J. König, D. Neftin, The admissibility of M_{11} over number fields. J. Pure Appl. Alg. 222 (2018), 2456–2464. 6
[35] J. König, D. Neftin, Reducible fibers of generic compositions. In preparation. 3
[36] J. König, D. Neftin, Reducible specializations of polynomials: the nonsolvable case. Preprint, arXiv:2001.03630, V.2. 3
[37] 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). 12
[38] A. Makowski, A. Schinzel, Sur l'équation indéterminée de M. Goormaghtigh, Mathesis 68 (1959), 128–142. 2
[39] A. Medvedev, T. Scanlon, Invariant varieties for polynomial dynamical systems. Ann. of Math. 179 (2014), 81–177. 1
[40] H. M. Mohammed Salih, Genus one and two groups of diagonal type, in preparation. 21
[41] T. Monderer, D. Neftin, Symmetric Galois groups under specialization. Israel J. Math. 248 (2022), 201–227. 20
[42] P. Müller, Primitive monodromy groups of polynomials. Recent developments in the inverse Galois problem, Contemp. Maths. 186, 385–401, Amer. Math. Soc., 1995. 2, 3, 5, 17, 18
[43] 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. 5, 6, 19
[44] P. Müller, Hilbert's irreducibility theorem for prime degree and general polynomials. Israel J. Math. 109 (1999), 319–337. 3
[45] P. Müller, Finiteness results for Hilbert's irreducibility theorem. Ann. Inst. Fourier 52 (2002), 983–1015. 3
[46] P. Müller, Reducibility behavior of polynomials with varying coefficients. Israel J. Math. 94 (1996), 59–91. 2
[47] P. Müller, Permutation groups of prime degree, a quick proof of Burnside's theorem. Arch. Math. 85 (2005), 15–17. 5
[48] P. Müller, M. Zieve, On Ritt's polynomial decomposition theorems. Preprint, arXiv:0807.3578. 1, 8
[49] 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

[50] F. Pakovich, Polynomial semiconjugacies, decompositions of iterations, and invariant curves. Ann. Sc. Norm. Super. Pisa Cl. Sci. XVII (2017), 1417–1446. 1
[51] F. Pakovich, On polynomials sharing preimages of compact sets, and related questions. Geom. Funct. Anal. 18 (2008), 163–183. 1
[52] J. F. Ritt, Prime and composite polynomials. Trans. Amer. Math. Soc. 23 (1922), 51–66. 1, 8
[53] A. Schinzel, Some unsolved problems on polynomials. Mate. Biblioteka 25 (1963), 63–70. 2
[54] I. Schur, Zur Theorie der einfach transitiven Permutationsgruppen. S. B. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 598–623. 5
[55] T. Shih, A note on groups of genus zero. Comm. Algebra 19 (1991), 2813–2826. 21, 22
[56] J. H. Silverman, The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Second Edition. 17

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

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