REDDUCIBLE SPECIALIZATIONS OF POLYNOMIALS: THE NONSOLVABLE CASE

JOACHIM KÖNIG AND DANNY NEFTIN

Abstract. Given an irreducible polynomial $F(t, x) \in \mathbb{Q}(t)[x]$, Hilbert’s irreducibility theorem asserts that the set $\text{Red}_F$, of values $t_0 \in \mathbb{Q}$ for which $F(t_0, x) \in \mathbb{Q}[x]$ is reducible, is “thin”. However, an explicit description of $\text{Red}_F$ is unknown, and describing it up to a finite set in the key case $F(t, x) = f(x) - t \in \mathbb{Q}(t)[x]$, is a long standing open problem.

In this key case, we show that $\text{Red}_F$ is the union of the value set $f_1(\mathbb{Q})$ and a finite set, given that $f$ decomposes as $f_1 \circ \cdots \circ f_r$ for indecomposable $f_i \in \mathbb{Q}[x]$ of degree $\geq 5$ which are not the composition of $x^n$ or a Chebyshev polynomial with linear polynomials, and are not in an explicit list of exceptions. Similar results apply to general polynomials $F(t, x)$ under either genus assumptions on the curve $F(t, x) = 0$ or nonsolvability assumptions on the Galois group of $F$. We relate these results to the genus 0 problem (Guralnick–Thompson 1990) and apply them to the Davenport–Lewis–Schinzel problem (1961).

1. Introduction

Background. A central goal in arithmetic geometry is specifying the extent to which geometry determines arithmetic. Hilbert’s irreducibility theorem provides a fundamental bridge between the two. Its basic version concerns irreducible polynomials $F(t, x) \in \mathbb{Q}(t)[x]$ that depend on a parameter $t$, and asserts that for “most” values $t_0 \in \mathbb{Q}$ the specialized polynomial $F(t_0, x) \in \mathbb{Q}[x]$ is irreducible. In this context, the above goal aims at specifying the meaning of “most”.

Letting $\text{Red}_F = \text{Red}_F(\mathbb{Q})$ denote the set of values $t_0 \in \mathbb{Q}$ where $F(t_0, x)$ is defined and reducible, a more precise version of Hilbert’s theorem asserts that $\text{Red}_F$ is “thin” [41, Section 3], that is, up to a finite set, 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 $\mathbb{Q}$, $i \in I$. For example when $F(t, x) = x^2 - t$, up to including $\infty$, the set $\text{Red}_F = \mathbb{Q}^2$ 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 general, determining the set $\text{Red}_F$ is a notoriously difficult problem, cf. [9], [43], and [24]. Indeed, finding an efficient algorithm for computing the sets $Y_i(\mathbb{Q})$ is a well known open problem, and it is often the case that there are many coverings $h_i$, $i \in I$ in Hilbert’s proof, as many as the number of maximal intransitive subgroups of the Galois group of $F$. However, the sublist of coverings $h_j$, $j \in J \subseteq I$ for which
Then Red \( \mu \) is infinite, is usually short, allowing the explicit description of \( \text{Red}_F \) up to a finite set.

To describe \( \text{Red}_F \) up to a finite set, as often done in arithmetic geometry, one separates into cases according to the genus \( g_F \) of (a geometrically irreducible component\(^1\)) of the smooth projective model \( X_F \) of the curve \( F(t, x) = 0 \). We start with describing the set of integral reducible specializations \( \text{Red}_F \cap \mathbb{Z} \) which often admits a similar description. Müller [32] shows that \( \text{Red}_F \cap \mathbb{Z} \) is finite when \( g_F > 0 \), and the Galois group of \( F \) is symmetric with the standard action (a.k.a. a general polynomial). In fact the finiteness of \( \text{Red}_F \cap \mathbb{Z} \) is known in many other cases, e.g. see Müller [33], Langmann [25], and König [23].

A representing example for the case \( g_F = 0 \) is when \( F(t, x) \) is of the form \( f(x) - t \) for \( f \in \mathbb{Q}[x] \). In this key case, the question can be interpreted as determining the reducibility of \( f \) after varying its free coefficient. This was first studied in the 70’s by Fried [12, 13], cf. [34], showing that \( \text{Red}_F \cap \mathbb{Z} \) is the union of the single value set \( f(\mathbb{Q}) \cap \mathbb{Z} \) with a finite set, given that\(^2\) \( \deg f > 5 \) and \( f \) is indecomposable. 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 \( \deg h = 1 \), cf. Remark 2.2.

In view of its tight connection with the structure theory of primitive groups, the more accessible case on which most results focus on is the indecomposable case, i.e. where the natural projection \( f : X_F \to \mathbb{P}^1 \) to the \( t \) coordinate is indecomposable. A recent result by Neftin–Zieve [36] shows that in this case, avoiding an explicit list of ramification types\(^3\) and assuming \( \deg_x F \) is sufficiently large in comparison to \( g_F \), the set \( \text{Red}_F \) and the value set \( f(X_F(\mathbb{Q})) \) differ by a finite set. If \( g_F > 1 \), then \( X_F(\mathbb{Q}) \) and hence \( \text{Red}_F \) are finite by Faltings’ theorem.

Low genus case. This paper considers the so far inaccessible decomposable case, and relates the infinite value sets \( h_j(Y_j(\mathbb{Q})) \), \( j \in J \) with the composition factors \( f_i \) in a decomposition \( f = f_1 \circ \cdots \circ f_r \). In the key low genus case \( F(t, x) = f(x) - t \in \mathbb{Q}(t)[x] \), we get the following theorem.

Let \( T_n \in \mathbb{Z}[x] \) denote the degree \( n \) (normalized) Chebyshev polynomial, i.e., the 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 \( f = f_1 \circ \cdots \circ f_r \) for indecomposable \( f_i \in \mathbb{Q}[x] \), \( i = 1, \ldots, r \) of degree \( \geq 5 \), 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 \( \deg f_1 > 20 \). Then \( \text{Red}_F \) is either the union of \( f_1(\mathbb{Q}) \) with a finite set, or \( f_1 \) is as in Table 1.

In either case, \( \text{Red}_F \) is the union of \( \text{Red}_{f_1(x)} \) with a finite set.

---

\(^1\)Note that the genus is independent of the choice of the irreducible component, see Remark 2.3

\(^2\)There are counterexamples to the analogous assertion when \( \deg f = 5 \), see [6].

\(^3\)The list is given in Theorem 2.18. For such ramification \( \text{Red}_F \) is the union of two value sets.
The surprising part of the result is that in the tower of polynomials induced by the composition of polynomial maps \( f_i, \ i = 1, \ldots, r \), if the first polynomial \( f_1(x) - t_0 \in \mathbb{Q}[x] \) is irreducible then for the rest of the tower \( f_1 \circ \cdots \circ f_i(x) - t_0 \in \mathbb{Q}[x] \) will remain irreducible, for \( i = 1, \ldots, r \) and all but finitely many \( t_0 \in \mathbb{Q} \).

We note that the assumption \( \deg(f_1) > 20 \) can be removed at the account of a longer list of exceptions. For \( f_1 \) as in Table 1, the set \( \text{Red}_f \) is shown to be the union of two value sets, up to a finite set. The complete result is given in Section 5.1. On the other hand, different methods are required for removing the assumption that \( f_i, \ i = 1, \ldots, r \) are of degree \( \geq 5 \) and are not the composition of \( x^n \) or \( T_n \) with linear polynomials. This assumption is equivalent to the nonsolvability of the monodromy group \( \text{Mon}(f_i) \), that is, the Galois group of \( f_i(x) - t \) over \( \mathbb{Q}(t) \), see Section 2.

Note that the different possible decompositions \( f_1 \circ \cdots \circ f_r \) of \( f \in \mathbb{C}[x] \) into indecomposable polynomials are described by Ritt’s theorems, see Remark 2.16. When including \( x^n \) or \( T_n \) as composition factors more than one choice of \( f_1 \) may occur, in which case all of these choices should appear in the list \( h_j, j \in J \). However, even adding these choices is not always enough, see Example 2.6.

Our methods apply more generally to coverings of large degree (in comparison to their genera), that is, when the natural projection \( f : X_F \to \mathbb{P}^1 \) is a composition \( f_1 \circ \cdots \circ f_r \) of geometrically indecomposable coverings \( f_i : X_i \to X_{i-1} \) whose degrees are sufficiently large in comparison to \( g_F \). We expect that in combination with other methods, the above will lead to a determination of \( \text{Red}_F \) up to a finite set in case \( X_F \) is of genus 0 or 1, cf. Remark 5.4.

**Arbitrary genus.** Our methods apply in the absence of restrictions on \( g_F \). As opposed to the low genus case, here quite general “Ritt” decompositions occur, and hence 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, under group theoretic constraints on the monodromy groups of \( f_1, \ldots, f_r \), we can effectively bound the number of in infinite value sets in \( \text{Red}_F \). The following theorem is a special case of the more complete Theorem 5.5:

**Theorem 1.2.** There exists \( N > 0 \) with the following property. Let \( f : X_F \to \mathbb{P}^1 \) be the projection to \( t \)-coordinates from the curve \( F(t, x) = 0 \). Suppose that \( f = f_1 \circ \cdots \circ f_r \) for geometrically indecomposable \( f_i \) of degree \( n_i \geq N \) having monodromy group \( A_{n_i} \) or \( S_{n_i} \). Then there exists a number field \( k \) such that, up to a finite set, \( \text{Red}_F(k) \) is the union of at most \( 2r \) value sets \( h_i(Y_i(k)), i = 1, \ldots, 2r \) of coverings \( h_i : Y_i \to \mathbb{P}^1_k \).

We note that the coverings \( h_i, i = 1, \ldots, r \) admit a rather explicit description. Those are coverings of genus at most one whose pullback along \( f_1 \circ \cdots \circ f_{i-1} \) is a covering with the same Galois closure as \( f_i \). For each \( i \), there is at most one such

\[^4\text{Work in progress implies that one may choose } k = \mathbb{Q}, \text{ see Remark 5.6.(1).}\]
covering \( h \), if its ramification is not listed in Theorem 2.18, and at most two otherwise. Also note that restrictions on \( \text{Mon}(f_i) \) come from group theoretic limitations of our methods. These restrictions can be relaxed, see Remark 5.6.(3), and are adjustable to other scenarios. The constant \( N \) in the degree assumption is expected to be dropped once the classification of monodromy groups is complete. Finally, note that \( 2r \) can be replaced by \( r \) value sets in the analogous description of \( \text{Red}_F \cap \mathbb{Z} \), see Remark 5.6.(2).

Relation to the genus 0 and Davenport–Lewis–Schinzel problems. The problem underlying determining the list of infinite value sets is of finding which coverings \( h : Y \to \mathbb{P}^1 \) of genus \( \leq 1 \) are subcovers of the Galois closure \( \tilde{f} \) of \( f \), that is, for which \( h \) one has \( \tilde{f} = h \circ h' \) for some cover \( h' : \tilde{X} \to Y \). This problem was extensively studied in the case where \( f \) is indecomposable, starting with Guralnick–Thompson [21], and Feit and Müller [30], continued by many authors, conjectured in the large degree case by Guralnick–Shareshian [20] and completed in [36, 37]. Without the indecomposability assumption, such a classification is currently beyond reach.

The crux in proving the above results is relating the minimal subcovers \( h : Y \to \mathbb{P}^1 \) of \( \tilde{f} \) with genus \( \leq 1 \), and nonsolvable monodromy, to the composition factors \( f_i \) of \( f \). Here \( f \) is not assumed to be indecomposable. This relation is given in Theorem 4.1. The following is a simplified version:

**Theorem 1.3.** 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 \( f \) that has the same Galois closure as \( h \).

\[
\begin{array}{ccc}
\tilde{X} & \xrightarrow{\tilde{f}'} & \tilde{Y} \\
\downarrow & & \downarrow \\
\tilde{X} & \xrightarrow{f} & Y \\
\downarrow & & \downarrow \\
X & \xrightarrow{f'} & Y \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \xrightarrow{h} & \mathbb{P}^1 \\
\end{array}
\]

Note that the the proof of Theorems 1.3 and 4.1 is of group theoretic nature and no genus assumptions on \( Y \) are imposed. We note that all nonsolvable monodromy groups \( H \) of large degree indecomposable coverings \( h : Y \to \mathbb{P}^1 \) of genus \( \leq 1 \),
satisfy the condition that \( H \) has no proper nonsolvable quotients. The list of low degree exceptions \( H \) to this statement is expected to come out of a solution of the indecomposable genus 0 problem in low degrees.

The genus 0 problem is known to have a wide range of consequences, in number theory, complex analysis, dynamics, and other subjects, cf., [36]. Similar consequences are expected from its combination with Theorem 4.1. We note here one application which is closely related to Hilbert irreducibility: the Davenport–Lewis–Schinzel (DLS) problem [4, 5, 39] asks for the classification of all polynomials \( u, v \) such that \( u(x) - v(y) \in \mathbb{C}[x, y] \) is reducible. An obvious case in which \( u(x) - v(y) \) is reducible is when \( u \) and \( v \) have a common composition factor \( u = w \circ u_0, v = w \circ v_0 \) for \( w, u_0, v_0 \in \mathbb{C}[x] \setminus \mathbb{C} \) with \( \deg w > 1 \). The DLS problem asks to determine the list of exceptions to this assertion. It was solved by Fried for indecomposable \( u, v \) in [11] and further recent progress is described in [17, 14]. Using Theorem 1.1 we get:

Corollary 1.4. Let \( u, v \in \mathbb{C}[x] \) be nonconstant polynomials. Assume that \( u = u_1 \circ \ldots \circ u_r \) for indecomposable \( u_i \in \mathbb{C}[x] \) of degree \( \geq 5 \), 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 \( \deg u_1 > 31 \). Then \( u(x) - v(y) \in \mathbb{C}[x, y] \) is reducible if and only if \( u = w \circ u_0 \) and \( v = w \circ v_0 \) for \( w \in \mathbb{C}[x] \) of degree \( > 1 \), and \( u_0, v_0 \in \mathbb{C}[x] \).

This is an immediate consequence of Theorem 1.1. The degree assumption can be easily lowered and in combination with other methods this suggests a general strategy towards the DLS conjecture. We plan to carry this out in subsequent work.

The second author thanks 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 (V2.24-5).

2. Preliminaries

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 \( \overline{k} \)), 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 \( f_i : X_1 \to Y_i, i = 1, 2 \) 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 an equivalence of categories between equivalence classes of coverings of \( \mathbb{P}^1_k \) and finite field extensions of \( k(t) \), up to \( k(t) \)-isomorphisms, cf., e.g.,
[7]. In particular, letting \( \tilde{f} : \tilde{X} \to \mathbb{P}^1_k \) denote the covering corresponding to the Galois closure \( \Omega \) 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 \( C \leq A := \text{Gal}(\Omega/k(t)) \). Namely, to every such subcover the correspondence associates a subgroup \( C \leq A \) (unique up to conjugation) such that \( h \) is equivalent to a covering \( f_C : \tilde{X}/C \to \mathbb{P}^1 \) whose composition with the natural projection \( \tilde{X} \to \tilde{X}/C \) is \( \tilde{f} \).

**Monodromy.** Let \( f : X \to \mathbb{P}^1_k \) be a geometrically irreducible covering over \( k \). Letting \( \Omega \) denote the Galois closure of \( k(X)/k(t) \), the arithmetic (resp. geometric) monodromy group \( A = \text{Mon}_k(f) \) (resp. \( G = \text{Mon}_\mathbb{Q}(f) \)) of \( f \) is the Galois group \( \text{Gal}(\Omega/k(t)) \) (resp. \( \text{Gal}(\overline{k}\Omega/\overline{k}(t)) \)) equipped with its permutation action on \( A/A_1 \), where \( A_1 = \text{Gal}(\Omega/k(X)) \). Note that since \( \overline{k}(t)/k(t) \) is a Galois extension, so is \( f'(t)/k(t) \) where \( f' = \overline{k} \cap \Omega \), and hence \( G \leq A \).

Given a subgroup \( C \leq G \), we say that the covering \( f_C \) (of \( \mathbb{P}^1_L \)) 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 becomes 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 defined over \( k' \).

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, the extension \( \Omega^C/k(t) \) is defined over \( k(t) \) if and only 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 \( D \cap G = C \). Furthermore, \( \Omega^D/k(t) \) is linearly disjoint from \( \overline{k}(t) \) if and only if \( \Omega^D \cap k(t) = k(t) \) or equivalently \( D \cdot G = A \). Finally, we note that \( f_C \) is further 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 \( A \).

For a polynomial \( f \in k[x] \), the monodromy group of the induced map \( f : \mathbb{P}^1 \to \mathbb{P}^1 \) is the Galois group of \( f(x) - t \in k(t)[x] \). 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.

**Remark 2.2.** A well known result of Fried and MacRae [10] asserts that an indecomposable polynomial in \( k[x] \) is indecomposable even over \( \overline{k} \). We shall therefore call such a polynomial simply “indecomposable” without specifying the base field.

**Specializations.** Let \( F(t, x) \in k[t, x] \) be an irreducible polynomial of positive \( x \)-degree\(^6\).

\(^5\)In cases where the base field is understood from the context, we shall simply write \( \text{Mon}(f) \).

\(^6\)Every \( F \in k(t)[x] \) as in the introduction may be replaced by such a polynomial by multiplying by an element of \( k(t) \). Note that this operation changes \( \text{Red}_F \) only by a finite set.
Remark 2.3. It may happen that $F$ factors as the product of $r > 1$ irreducible $F_i \in \overline{k}[t, x]$, $i = 1, \ldots, r$. However since $\overline{k}(t)/k(t)$ is Galois, the curves $F_i(t, x) = 0$, $i = 1, \ldots, r$ are all isomorphic over $\overline{k}$, and in particular are of the same genus.

We shall henceforth assume $F$ is irreducible over $\overline{k}$, and hence corresponds to a geometrically irreducible covering $f : X \to \mathbb{P}^1$ over $k$. We next recover a well known criterion for the reducibility of the specialized polynomial $F(t_0, x) \in k[x]$. Let $\Omega$ be the splitting field of $F$ over $k(t)$, so that $A = \text{Gal}(\Omega/k(t))$ is the arithmetic monodromy group of $f$. A well known fact from algebraic number theory, see e.g. [22, 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 $\Omega_{t_0}$ of $F(t_0, x)$ is Galois, and its Galois group is identified with a unique (up to conjugation) subgroup $D \leq A$, known as the decomposition group at $t_0$. Moreover, $\Omega^D$ has a degree 1 place $P$ over $t_0$. In particular, $\Omega^D \cap \overline{k}(t) = k(t)$. Thus letting $C := D \cap A$, Remark 2.1 implies the existence of a covering $f_D : X_D \to \mathbb{P}^1$ over $k$ which is equivalent to $f_C : X/C \to \mathbb{P}^1$. Moreover, the place $P$ corresponds to a $k$-rational point $P \in X_{t_0}(k)$ such that $f_D(P) = t_0$. For $t_0$ as above, $D$ and $\text{Gal}(\Omega_{t_0}/k)$ are in fact isomorphic as permutation groups, and hence $F(t_0, x)$ is reducible if and only if $D$ is intransitive. In total one has:

Proposition 2.4. Let $F \in k(t)[x]$ be irreducible with 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 $\delta_F(t)$, let $D = D_{t_0}$ be its decomposition group, and $f_D : X_D \to \mathbb{P}^1$ the covering corresponding to $\Omega^D/k(t)$. Then:

1. $t_0$ has a $k$-rational preimage under $f_D$, 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 over $\overline{k}(t)$, the natural projection $f : X \to \mathbb{P}^1$ to the $t$-coordinate is a (geometrically irreducible) 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 $\text{Red}_f$ agree, up to the finite set of roots and poles of $\delta_F$.

Proposition 2.4 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 $\infty$ has at most two preimages under $f_D$. We therefore have:

Corollary 2.5. 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 \( \bigcup_D \left( f_D(\mathbb{X}_D(k)) \cap O_k \right) \) differ by a finite set, where \( D \) runs over maximal intransitive subgroups of \( A \) such that \( f_D \) is a Siegel function.

**Example 2.6.** 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) \( \text{Red}_F \) is the union of \( f_1(\mathbb{Q}) \cup h(\mathbb{Q}) \) with a finite set, where \( f_1, h : \mathbb{P}^1 \to \mathbb{P}^1 \) are given 
(on affine charts) by \( x \mapsto T_2(x) \) and \( x \mapsto -T_4(x) \), respectively. Furthermore, \( f_1 \) is the \( \text{the unique indecomposable subcover of the natural projection} \ f : \mathbb{P}^1 \to \mathbb{P}^1, \ x \mapsto T_4(x) \) corresponding to \( F \). Since \( h \) is of degree 2, it is Galois, and hence does not factor through \( h \). As pointed out in Section 1, this shows that the analogous result to Theorem 1.1 does not hold for polynomials with solvable monodromy.

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 \( \tilde{X} \cong \mathbb{P}^1 \) which is defined over \( k \) by \( x \mapsto (x + 1/x)^4 \) and factors as \( \tilde{f} = f \circ (x + 1/x) \). The arithmetic and geometric monodromy groups \( A \) and \( G \) of \( f \) are the dihedral group \( D_4 \) of degree 4, 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 \( f_s : \tilde{X}/\langle s \rangle \to \mathbb{P}^1 \). We next deduce (1) and (2) from:

**Claim 2.7.** \( h \) is equivalent to the covering \( f_{sr} : \tilde{X}/\langle sr \rangle \to \mathbb{P}^1 \).

By Corollary 2.5 it suffices to find the maximal intransitive subgroups \( D \leq A \) for which \( g_x \leq 1 \) and \( DG = A \). However, since \( \tilde{X} \) is of genus 0 and \( G = A \), the two conditions are immediate. Up to conjugacy the maximal intransitive subgroups of \( D_4 \) are \( \langle sr \rangle \), and \( \langle s, r^2 \rangle \), showing (1). Claim (2) then follows since the only proper subgroup of \( D_4 \) which contains \( \langle sr \rangle \) is \( \langle sr, r^2 \rangle \).

It remains to prove Claim 2.7. Note that the composition \( \tilde{f} := x^2 \circ \tilde{f} \) is a Galois covering with arithmetic monodromy group \( D_8 \) containing \( A = D_4 \) as a subgroup. Since \( x^2 \circ f = x^2 \circ h \), it follows that \( h \) is equivalent to \( \tilde{f}_H : \tilde{X}/H \to \mathbb{P}^1 \) for a subgroup \( H \leq A \) that is conjugate to \( H \) in \( D_8 \). It therefore suffices to show that \( H \) is not conjugate to \( \langle s \rangle \) in \( A \): note that such a conjugacy would imply the existence of a linear \( \mu \in \mathbb{C}[x] \) such that \( T_4(\mu(x)) = -T_4(x) \), contradicting the fact that \( t = 2 \) has an unramified preimage under \( T_4 \circ \mu \) and none under \( -T_4 \), proving the claim.

For an example over \( \mathbb{Q} \), see [15, §2],[16, 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 2.8.** 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 \( A = G \times B \) with a complement \( B \leq A_1 \). Then every maximal intransitive subgroup \( C \leq G \) normalized by \( B \) is contained in an intransitive subgroup \( D := CB \leq A \) satisfying \( DG = A \) and \( D \cap G = C \), showing that \( f_C : \tilde{X}/C \to \mathbb{P}^1 \) is defined over \( k \) by Remark 2.1. Indeed, \( D \) is a subgroup since
CB = BC, it is intransitive since the inequality \( CG_1 \neq G \) implies that
\[
DA_1 = CBA_1 = CA_1 \not\supseteq G.
\]

**Fiber products and pullbacks.** Let \( \tilde{f} : \tilde{X} \to Y \) be a Galois covering over \( k \) with arithmetic monodromy group \( A \). Let \( H, A_1 \leq A \) be subgroups and \( f_{A_1}, f_H \) the corresponding coverings \( f_{A_1} : \tilde{X}/A_1 \to Y \) and \( f_H : \tilde{X}/H \to Y \), 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 2.9.** The irreducibility of the fiber product \( X \# Z \) of \( f_{A_1} \) and \( f_H \) is equivalent to the linear disjointness of the function fields \( k(X) \) and \( k(Z) \) over \( \overline{k}(Y) \), which in turn is equivalent to the transitivity of \( H \) on \( A/A_1 \), that is, \( HA_1 = A \). In this case, 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 2.10.** Let \( f : X \to Y, h : Z \to Y \) be coverings with reducible fiber product. Then \( f = f_0 \circ f_1 \) where \( f_0 \) is a subcover of the Galois closure \( h \) 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 \( f \sim \tilde{g}_U \), \( h \sim \tilde{g}_V \), and \( h \sim \tilde{g}_N \) for \( U, V, N \leq A \) with \( N = \text{core}_A(V) < A \). Since the fiber product of \( f \) and \( h \) is reducible, \( UV \neq A \). Since \( N < A \), \( UN \) is a group, and as \( U \leq UN \), \( f \) factors through \( f_0 := \tilde{g}_{UN} : Z/(UN) \to Y \). 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. \( \square \)

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

**Remark 2.11.** Assume that the pullback \( f_h : W \to Z \) is irreducible, let \( \tilde{f}_h : \tilde{W} \to Z \) be its Galois closure and \( \Gamma \) its arithmetic monodromy group. We note that there is a natural embedding \( \varphi : \Gamma \to A \) and a 1-to-1 correspondence between subcovers \( \tilde{W}/U \to Z \) of \( \tilde{f}_h \) and coverings \( \tilde{X}/\varphi(U) \to \tilde{X}/\varphi(\Gamma) \), given by pulling back along the natural projection \( h_2 : Z \to \tilde{X}/\varphi(\Gamma) \).

Indeed, since \( k(W) \) is the compositum of \( k(X) \) and \( k(Z) \) by Remark 2.9, the Galois closure \( \Omega_W \) of \( k(W)/k(Z) \) is the compositum of the Galois closure \( \Omega_X \) of \( k(X)/k(Y) \) with \( k(Z) \). Hence Galois theory implies that the monodromy group \( \Gamma \) of \( f_h \) is isomorphic to a transitive subgroup of \( A \) via the restriction \( \varphi : \text{Gal}(\Omega_W/k(Z)) \to \text{Gal}(\Omega_X/k(Y)) \). In particular \( h \) factors as \( h_1 \circ h_2 \), where \( h_1 \) is the natural projection \( \tilde{X}/\varphi(\Gamma) \to Y \). The above 1-to-1 correspondence is then the correspondence from Galois theory between intermediate fields of \( \Omega_X/(k(\tilde{X}) \cap k(Z)) \) and intermediate fields of \( \Omega_W/k(Z) \).
Primitive groups. We describe the structure theory of primitive groups, following [2] and [18]. Assume $U$ is primitive and denote by $\text{soc}(U)$ the socle of $U$, that is, the product of minimal normal subgroups of $U$. In the case where $\text{soc}(U)$ is abelian, also known as the affine case, one has

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

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

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

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

Also note that a normal subgroup of a primitive group is transitive, and hence $\text{soc}(U) \cdot U_1 = U$, where $U_1$ is a point stabilizer.

Normal subgroups of $L^t$ are described using [2, (1.4)] as:

Lemma 2.12. Let $L$ be a 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 $\big( K \cap L^{O_1} \big) \times \cdots \times \big( K \cap L^{O_r} \big)$ where $O_1, \ldots, O_r$ is a partition of $I$, and $K \cap L^{O_j} \cong L$ for all $j = 1, \ldots, r$.

In case (C), $U$ acts transitively by conjugation on the minimal normal subgroups $L_1, \ldots, L_r$ of $L^t$. Finally, we shall also use the following version of Goursat’s lemma [26, Corollary 1.4]:

Lemma 2.13. 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 $N \triangleleft G$ is of the form $N = (N \cap A) \times (N \cap B)$.

Wreath products. We note that given two coverings $f : X \to \mathbb{P}^1, h : Y \to X$ 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 $G \leq S_J$ is given by permuting the $J$-copies of $H$; the action of $A$ is the natural imprimitive degree $m \cdot n$ action of $U \wr_J V$; $A$ maps onto $V$ under the projection modulo $U^J$; and the block stabilizer $A_0 := A \cap (U^J \rtimes S_J)_{\{0\}}$ maps onto $U$ under the projection to the 0-th coordinate, for every $0 \in J$. When considering imprimitive actions we shall henceforth embed $A$ into $U \wr_J V$ in such a way.

Ramification. The ramification type of a covering $f : X \to \mathbb{P}^1$ (over $\overline{k}$) at a point $P \in \mathbb{P}^1$ 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 over a geometrically irreducible cover $f$ over $k$ is simply defined as the ramification type of $f \times_k \overline{k}$.

**Polynomials.** A polynomial covering $f : \mathbb{P}^1 \to \mathbb{P}^1$ is a covering which satisfies $f^{-1}(\infty) = \{\infty\}$ in $\overline{k}$. In particular on the affine line it is given by a polynomial. The following theorem is the combination of [30] and [20, §1.2]:

**Theorem 2.14.** 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 $S_\ell$; 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 [36, Table 2]. These do not correspond to Siegel functions.
3. $f$ corresponds to the natural point stabilizer of $P\Gamma L_3(4)$ or $PSL_5(2)$. In each case there is exactly one more subcover $h$ of genus $\leq 1$.
4. $f$ is of degree $\leq 20$. The corresponding subcovers $h$ with $10 \leq \deg h \leq 20$ are also listed in [20, Theorem A.4.1].

**Remark 2.15.** Writing $f = u \circ v$ for polynomial covers $u, v$ of degree $m, n$, respectively, Abhyankar’s lemma implies that $e_u(Q/\infty) = m$ 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 $u$. In particular, the kernel of the natural projection from $\text{Mon}(f) \leq S_n \wr S_m$ to $\text{Mon}(u) \leq S_m$ is nontrivial.

**Remark 2.16.** The decompositions of a polynomial $f \in k[x]$ into indecomposables $f_1 \circ \ldots \circ f_r$ are described by Ritt’s theorems (see [38, 35]). 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 $f = g_1 \circ \ldots \circ g_s$ into indecomposables, one has $s = r$ and $g_i = \mu_i \circ f_i \circ \mu_{i-1}$ for linear polynomials $\mu_i$, $i = 1, \ldots, r$ with $\mu_0 = \mu_r = \text{id}$. Due to subsequent work of Fried and MacRae ([10, Theorem 3.5]), the linear polynomials may even be assumed to be over $k$.

**Remark 2.17.** In case (3) of Theorem 2.14, the arithmetic monodromy $A$ of $f$ over some field identifies with $G$. In case (2), either $A = G$ or $(A, G) = (S_n, A_n)$.

---

7More 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 [3].
In comparison, in case (2) there is only one indecomposable subcover of genus \( \ell \) or \( \ell \leq 2 \). The classification of monodromy groups. In the more general case of rational functions or low genus coverings \( f : X \to \mathbb{P}^1 \) we apply [20, 36, 37]:

**Theorem 2.18.** 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 action on 2-sets of degree \( n = \frac{\ell(\ell-1)}{2} \). For the latter, the ramification of \( f \) is given in [36, Table 4.2].

(2) \( A_\ell^2 \leq G \leq S_\ell \wr C_2 \) with the natural primitive action of degree \( n = \ell^2 \). The ramification of \( f \) is listed in [37, Table 3.1].

**Remark 2.19.** (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 intrinsively in the natural action, which implies that the fiber product of the above two subcovers is reducible, cf. Remark 2.9.

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 above list with [31, Theorem 3.3], we see that in the above 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 nonsolvable indecomposable Siegel function \( f \), 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.

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

\[
\begin{align*}
\ell, [a, \ell - a], [1^{\ell-2}, 2] \\
\ell, [1^3, 2^{(\ell-3)/2}], [1, 2^{(\ell-1)/2}], [1^{\ell-2}, 2] \\
\ell, [1^2, 2^{(\ell-2)/2}] \text{ twice}, [1^{\ell-2}, 2] \\
\ell, [1^3, 2^{(\ell-3)/2}], [2^{(\ell-3)/2}, 3] \\
\ell, [1^2, 2^{(\ell-2)/2}], [1, 2^{(\ell-4)/2}, 3] \\
\ell, [1, 2^{(\ell-1)/2}], [1^2, 2^{(\ell-5)/2}, 3] \\
\ell, [1^3, 2^{(\ell-3)/2}], [1, 2^{(\ell-5)/2}, 4] \\
\ell, [1^2, 2^{(\ell-2)/2}], [1^2, 2^{(\ell-6)/2}, 4] \\
\ell, [1, 2^{(\ell-1)/2}], [1^3, 2^{(\ell-7)/2}, 4]
\end{align*}
\]
The following lemma follows from the monodromy classification:

**Lemma 2.20.** Suppose \( f : X \to \mathbb{P}^1_k \) is an indecomposable covering with nonaffine monodromy group \( G \). If \( g_X \leq 1 \), then \( G \) has a unique minimal normal subgroup \( \text{soc}(G) \) and \( G/\text{soc}(G) \) is solvable.

**Proof.** Since \( G \) is assumed to be nonaffine, it is either of type (B) or (C). By [40], Type (B) does not occur with genus \( \leq 1 \), so that we may assume \( G \) has a unique minimal normal subgroup. Thus by [21, Theorem C1] and [1], the only case in which \( G/\text{soc}(G) \) 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 [21]. By [19, Theorem 7.1], a product type case with nonsolvable \( G/\text{soc}(G) \) and genus \( \leq 1 \) has to fulfill \( G/\text{soc}(G) \cong A_5 \) acting as a genus 0 group in the natural action, or \( G/\text{soc}(G) \cong S_5 \) with ramification type \([2^60],[4^{20}],[5^{24}]\), and \( G' \leq S_t \times S_5 \) with \( t \leq 10 \). The first case is already ruled out by [19, Theorem 8.6], whereas a computer check shows the second case does not occur either with genus \( g \leq 1 \). \( \square \)

Using the above classification of primitive (geometric) monodromy groups, Monderer–Neftin [27, 29] recently obtain a classification of all low genus actions of the key cases \( A_n \) and \( S_n \) as follows:

**Lemma 2.21.** Let \( g \geq 0 \), then there exists \( N_g > 0 \) such that for every \( n > N_g \), every covering \( f : X \to \mathbb{P}^1_k \) with monodromy group \( G \in \{A_n,S_n\} \) corresponds the action of \( G \) on cosets of one of the following subgroups \( H \):

\[
\begin{align*}
\text{a)} & \quad H \in \{A_{n-1},S_{n-1}\}, \\
\text{b)} & \quad A_{n-2} < H \leq S_{n-2} \times S_2.
\end{align*}
\]

If moreover \( f \) is a polynomial covering and \( g \leq 1 \), then one may take \( N_g = 20 \).

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

**Lemma 2.22.** 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:

\[
\begin{align*}
\text{a)} & \quad f \text{ is a polynomial covering of degree } n > 20, \\
\text{b)} & \quad f \text{ is a covering with almost-simple monodromy and of degree } > N \text{ for some absolute constant } N.
\end{align*}
\]

Suppose \( h \) is a nonsolvable subcover of \( \tilde{f} \) of genus \( \leq 1 \) which is indecomposable over \( k \). Then \( h \) is geometrically indecomposable. Moreover, \( h \times_k \overline{k} \) 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 maximal subgroup of \( A \) corresponding to the subcover \( h \).
To show the first assertion, it suffices to show that \( D \cap G \) is an intransitive maximal subgroup of \( G \). For unique definedness, it then suffices to verify the conditions of Remark 2.8.

Since both assertions of the lemma are trivial in the case \( G = A \), we assume \( G < A \).

Let \( C < G \) be a subgroup containing \( D \cap G \), maximal such that the action of \( G \) on cosets of \( C \) is nonsolvable. In case a), Theorem 2.14 then readily implies that \( A = S_n \), \( G = A_n \), and \( C \) is either conjugate to a point stabilizer \( G_1 = \text{Sym}\{2, \ldots, n\} \cap G \) or to the stabilizer of a 2-set \( G_2 = (\text{Sym}\{1, 2\} \times \text{Sym}\{3, \ldots, n\}) \cap G \). In case b), note that since \( A \) is almost simple, \( A/G \) is solvable. The nonsolvability of \( h \) implies the nonsolvability (and thus, faithfulness) of the action of \( G \) on cosets of \( D \cap G \). Since this yields a primitive genus-\( \leq 1 \) action, it follows from Theorem 2.18 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, we may therefore apply Lemma 2.21 to obtain \( D \cap G \in \{G_1, G_2\} \). In particular, \( D \cap G \) is maximal in \( G \), whence \( f \) is indecomposable over \( k \).

Furthermore, the conditions of Remark 2.8 hold with the decomposition \( A = G \rtimes \langle (3, 4) \rangle \), for both possibilities for \( C \). Since furthermore \( D := \langle (3, 4) \rangle \cdot C = A_1 \) or \( A_2 \) are the only subgroups satisfying \( DG = A \) and \( D \cap G = C \), the covering \( h \) is uniquely defined over \( k \) by Remark 2.1. \( \square \)

Remark 2.23. (1) Lemma 2.22 does not require the full force of Lemma 2.21. Indeed, [8, Theorem 5.2A and B] classify all subgroups of \( A_n \) and \( S_n \) of index \( < \left( \frac{n}{n/2} \right) \).

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 2.22, it therefore suffices to show that \( A_n \) does not have any \( g \leq 1 \) action of degree \( \geq \left( \frac{n}{n/2} \right) \).

(2) The proof of Lemma 2.22, together with the classifications of Theorems 2.14 and 2.18 in fact yields the following: If \( f \) is polynomial of degree \( n \geq 20 \) or of large degree \( n \) with monodromy group \( A_n \) or \( S_n \), then any subcover \( h \) as in Lemma 2.22 has reducible fiber product with \( f \).

3. Preliminary results on permutation groups

3.1. Normal subgroups. The following is a consequence of [2, (1.6),(2)-(3)]:

Lemma 3.1. Let \( G \leq U \wr V \) 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 \( \text{soc}(U) \cong L^J \), and \( K := G \cap U^J \) is nontrivial. Then

\[
\text{soc}(K) = K \cap \text{soc}(U)^J \cong (K \cap L^{O_1}) \times \cdots \times (K \cap L^{O_r}),
\]
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 $I \times J$.

Proof. First note that since $G$ is a subgroup of $U \wr V$, it has a natural action on $I \times J$, namely, the imprimitive action it inherits by being a subgroup of $S_I \wr S_J$, since $U \leq S_I$ via the conjugation action on the copies of $L$. To apply [2, (1.6)] (with $M = G$ and $D = \text{soc}(K)$) it suffices to show 1) that the projection of $\text{soc}(K)$ on the $j$-th coordinate is a power of $L$ for every $j \in J$, and hence $\text{soc}(K) \cong L^t$ for some $t \geq 1$ by Lemma 2.12, and 2) that $G$ acts transitively on $I \times J$, and hence the projection of $\text{soc}(K)$ onto each of the $I \times J$ coordinates contains $L$.

To show 1), first note that since $G$ acts transitively on $J$ and this action is equivalent to the conjugation action on the $U$-components of $K \leq U^J$, the images of the projections to $U$ are all isomorphic. Moreover, since by assumption the projection of the $j$-th block stabilizer $G_0$ onto the $j$-th copy of $U$ is onto, and since $K < G_0$, the projection of $K$ to the $j$-th coordinate is a normal subgroup of $U$. Since $U$ has a unique minimal normal subgroup by assumption, these images are either trivial or contain $\text{soc}(U)$. Thus 1) follows from $K \neq 1$.

To show 2), note that since $\text{soc}(U)$ is a normal subgroup of the primitive group $U$, it acts transitively on $I$, e.g. [8, Theorem 1.6A]. Since $V$ acts transitively on $J$, $G$ acts transitively on the blocks $J$, and as $K$ projects onto $\text{soc}(U)$, it acts transitively on each $I \times \{j\}, j \in J$, proving the transitivity of $G$. \qed

In particular, one has:

**Corollary 3.2.** In the setting of Lemma 3.1, $\text{soc}(K)$ is a minimal normal subgroup of $G$.

Proof. As in Lemma 2.12, decompose $\text{soc}(K)$ as $\prod_{i=1}^r \text{soc}(K) \cap L^{O_i}$ where $O_1, \ldots, O_r$ is a partition of $J \times J$, and $\text{soc}(K) \cap L^{O_i} \cong L$. Since $N$ is normal in $K$, Lemma 2.12 yields that $N \cap \text{soc}(K)$ 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 $N \cap \text{soc}(K) = \text{soc}(K)$ or $\{1\}$. \qed

Finally, the following lemma relates normal subgroups of an imprimitive $G$ to other partitions of its action.

**Lemma 3.3.** Let $G \leq U \wr V$ 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. Assume that $K := \bigcap_{g \in G} G_0^g \neq 1$.

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.
Proof. To show $G_1N \neq G_0N$, it suffices to show that $N' := N \cap G_0$ acts trivially on the cosets of $G_1$ in $G_0$, since then $(N \cap G_0)G_1 = N'G_1 \neq G_0$, and hence $G_0 \not\leq G_1N$.

Let $K_0 := \text{soc}(K)$, and let $M$ be the kernel of $K_0 \times N'$ in the action on cosets of $G_1$ in $G_0$, 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, $\text{soc}(U)$ and hence also $\text{soc}(K_0)$, are nontrivial powers of a nonabelian simple group. By Lemma 2.13, 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 $K_0 < G$, this shows that $K_0/(M \cap K_0)$ contains $\text{soc}(U)$. Moreover, since $U$ is of type (C), this forces $N'/(N' \cap M) = 1$, as desired.

It remains to note that $G_1N$ is not contained in $G_0$, since by assumption

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

while $K \neq 1$, giving $N \not\leq G_0$. \hfill $\square$

Note that the conclusion of Lemma 3.3 yields a refinement $G > G_0N > G_1N > G_1$ of the inclusion $G > G_1$ which is essentially different from $G > G_0 > G_1$ (due to neither of $G_1N$ and $G_0$ containing the other).

In particular, if $G$ is assumed to be the monodromy group of a polynomial map $f : \mathbb{P}^1 \to \mathbb{P}^1$, then the conclusion yields two essentially different decompositions of $f$ into indecomposable polynomials. Together with Remark 2.16, this gives:

**Corollary 3.4.** 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 $A \to \text{Mon}(f_1 \circ \cdots \circ f_{r-1})$. Then $\text{soc}(A) = \text{soc}(K)$.

As an application of the above we also get the following lemma. First, for a subgroup $H_0 \leq G$, we shall say that the action of $G$ on $G/H_0$ is solvable if $G/\text{core}_G(H_1)$ is a solvable group. For a subgroup $H \leq G$, there exists a unique minimal subgroup $H \leq H_{\text{sol}} \leq G$ such that $G/H_{\text{sol}}$ is solvable. Indeed, this follows since the solvability of the action on $G/H_1$ and $G/H_2$ implies that of $G/(H_1 \cap H_2)$.

**Lemma 3.5.** Let $V$ be a solvable permutation group on $J$, let $U$ be a primitive permutation group all of whose nontrivial quotients are solvable, 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 $H \supseteq G_1$. Then every nontrivial quotient of $G$ is solvable.

Proof. We note that the minimal $G_1 \leq H \leq G$ for which $G/H$ is solvable, is the block stabilizer $H = G_0$ of the block $0 \in J$ (to which the point belongs to). Indeed, since $G/G_0$ is solvable, and $G_0 \supseteq G_1$, we have $G_1 < H \leq G_0$. Since $G_1$ is maximal in $G_0$ by assumption and $G/G_1$ is nonsolvable, this gives $H = G_0$, as claimed.

Assume $M \triangleleft G$ is a nontrivial normal subgroup with $G/M$ nonsolvable, and consider the subgroup $G_1M$. To apply Lemma 3.3, we claim that $M \cap K = 1$. Assuming the claim we get that $G_1M$ does not contain $G_0$. On the other hand, the action of $G$ on $G/(G_1M)$ 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, 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 $\text{soc}(U)$. Since $G$ is transitive, we may replace $I$ by any other block, and deduce that the projection of $K$ onto each of the blocks contains $\text{soc}(U)$. We may therefore apply Lemma 3.1 to deduce that $\text{soc}(K) = K \cap \text{soc}(U)^d$, and that $K/\text{soc}(K)$ injects into $U^d/\text{soc}(U)^d$. Since $U$ has no nontrivial nonsolvable quotient, $U/\text{soc}(U)$ is solvable and hence $U^d/\text{soc}(U)^d$ and $K/\text{soc}(K)$ are solvable. Since $M \cap K$ is normal in $G$, Corollary 3.2 implies that either $M \cap K = 1$ or $M \supseteq \text{soc}(K)$. The latter case contradicts the assumption that $G/M$ is nonsolvable, proving the claim.

\[ \square \]

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

**Lemma 3.6.** Let $G \leq S_n$ be transitive with point stabilizer $H$, let $U < G$, and let $H_0 < H_1 < \cdots < H_r = G$ and $U_0 < U_1 < \cdots < U_s = G$ be two chains of maximal subgroups (with $r,s \geq 1$). Assume that for each $i \in \{1, \ldots, r\}$, the action of $H_i$ on cosets of $H_{i-1}$ is nonsolvable, whereas for each $i \in \{1, \ldots, s\}$ the action of $U_i$ on cosets of $U_{i-1}$ 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 nonsolvable 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, this gives the transitivity of $U$ on $G/H$.\[ \square \]
Let $\psi : H_1 \to \text{Sym}(H_1/H)$ 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 $\Gamma$, 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 without loss $\psi(U \cap H_1) = \{1\}$. 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 $\Gamma$ is solvable, a contradiction. \hfill $\square$

As a consequence concerning decompositions of coverings, we have:

**Corollary 3.7.** Let $f : X \to \mathbb{P}^1$ be a covering over a field $k$ of characteristic 0, written as $f = f_1 \circ \ldots \circ f_r$, where all $f_i$ are indecomposable with nonsolvable (arithmetic) monodromy. Assume that there exists a decomposition $f = g \circ h$, with covers $h : X \to Y$ 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 $f = f_1 \circ \ldots \circ f_r$. 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. Consider the smallest normal subgroup $A_0$ of $A$ with solvable quotient. By Lemma 3.6, $A_0$ is transitive on $A/H_r$, so $A_0H_r = A$. On the other hand, we have $H_r \subseteq U$ as well as $A_0 \subseteq U$, yielding $A_0H_r \subseteq U$, a contradiction. \hfill $\square$

Finally we state the analogous result when $H_i/H_{i+1}$ is more generally affine:

**Lemma 3.8.** Let $G \leq S_n$ be transitive with point stabilizer $H$, let $U < G$, and let $H =: H_0 < H_1 < \ldots < H_r = G$ and $U =: U_0 < U_1 < \ldots < U_s = G$ be two chains of maximal subgroups (with $r, s \geq 1$). Assume that each of the following holds:

i) For each $i \in \{1, \ldots, r\}$ the permutation group induced by the action of $H_i$ on cosets of $H_{i-1}$ is nonsolvable without a nontrivial nonsolvable quotient, whereas for each $i \in \{1, \ldots, s\}$ the action of $U_i$ on cosets of $U_{i-1}$ is affine.

ii) The block kernels $\bigcap_{g \in G} H_i^g$, $i = 0, \ldots, r-1$, are pairwise distinct.\(^8\)

Then $U$ is transitive in the action on cosets of $H$.

**Remark 3.9.** The proof relies on the following observation. In the setup of Lemma 3.8, for every $N \triangleleft G$, we claim that the group $U \cap N$ must contain all nonabelian composition factors of $N$.

First note that $U$ contains every nonabelian composition factor of $G$, including multiplicities. Indeed, this follows inductively since in every primitive affine action,

\(^8\)We suspect that this technical assumption 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 $\text{Mon}(f_1 \circ \ldots \circ f_i)$, $i = 1, \ldots, r$ for polynomial maps $f_i$, then due to ramification at infinity, it is automatic that $\bigcap_{g \in G} H_i^g$ can never be contained in $H_{i-1}$.
a point stabilizer has an elementary abelian complement and hence contains every nonabelian composition factor of that group.

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.** Set $K := \bigcap_{g \in G} H_g^g$ and note that $K \neq 1$. We prove the claim by induction on $r$. The base case being $r = 1$. In this case, Remark 3.9 implies that $U$ contains all nonabelian composition factors of $G$. Since by assumption $G$ is primitive of type (C), $U$ contains $\text{soc}(G)$. Since the quotient by $\text{soc}(G)$ is assumed to be solvable, this action is transitive by Lemma 3.6, giving the induction base.

It follows by induction that the block action of $UK/K$ on $U/U \cap H_1$ 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 $\text{soc}(K) \vartriangleleft G$, Remark 3.9 shows that $U$ must contain every nonabelian composition factor of $\text{soc}(K)$. Let $\Gamma$ denote the image of the action $\psi : H_1 \to \text{Sym}(H_1/H_0)$. Since $K \neq 1$, as in Lemma 3.1 the projection $\psi(\text{soc}(K))$ to any block is a nontrivial normal subgroup of $\Gamma$. Since by assumption $\Gamma$ has no proper nonsolvable quotients, the quotient by $\psi(\text{soc}(K))$ is solvable. Thus, by Lemma 3.6, $\psi(\text{soc}(K))$ and hence $U \cap H_1$ is transitive on $H_1/H_0$ as desired.

We obtain an immediate application to the polynomial case:

**Corollary 3.10.** Let $k$ be a field of characteristic 0, $A$ be the arithmetic monodromy group of a polynomial $f = f_1 \circ \cdots \circ f_r \in k[X]$, such that all $\text{Mon}(f_i)$ are nonsolvable. Let $U := U_0 < U_1 < \cdots < U_s = A$ be a chain of maximal subgroups such that for each $i \in \{1, \ldots, s\}$, the action of $U_i$ on cosets of $U_{i-1}$ is affine. Then $U$ is transitive on the roots of $f(X) - t$.

This follows directly from Lemma 3.8, noting that the the action of $\text{Mon}(f)$ is equivalent to its action on the roots of $f(x) - t$, and that Assumption (ii) of the lemma holds since for polynomials the block kernel is nontrivial, see Remark 2.15.

## 4. Main Theorem

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

**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 $f_i : X_i \to X_{i-1}, i = 1, \ldots, r$ whose monodromy groups $\Gamma_i$ have a unique minimal normal subgroup, the quotient by which is solvable. Suppose $h : Y \to \mathbb{P}^1$ is a minimal subcover of $\tilde{f}$ with nonsolvable monodromy group $\Gamma$, and that the proper quotients of $\Gamma$ are all 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 $\text{Mon}(f'_1)$ solvable and $f'_2$ indecomposable;
2. If moreover $\Gamma_1, \ldots, \Gamma_r$ are nonsolvable, then $f' = f'_2$ is indecomposable.

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

1. If $i \in \{1, \ldots, r\}$ is minimal such that $h$ is a subcover of the Galois closure of $f_1 \circ \cdots \circ f_i$, then $\text{Mon}(f_1 \circ \cdots \circ f_i)$ embeds into the direct product $\text{Mon}(f_1 \circ \cdots \circ f_{i-1}) \times \text{Mon}(f_i)$.
2. Conversely, given $i \in \{1, \ldots, r\}$, let $\tilde{g}_i$ denote the Galois closure of $f_1 \circ \cdots \circ f_i$. Then all minimal subcovers $h$ with nonsolvable monodromy group whose proper quotients are solvable, such that $h$ is a subcover of $\tilde{g}_i$ but not of $\tilde{g}_{i-1}$, have the same Galois closure with monodromy group isomorphic to $\text{Mon}(f_i)$.
3. With $i$ and $h$ as above, the cover $f_i$ is equivalent to the pullback of a subcover of $h$ along $f_1 \circ \cdots \circ f_{i-1}$.

**Remark 4.2.** (1) We note that the theorem does not assume genus 0, nor the reducibility of the fiber product of $f$ and $h$ (the intransitivity of the subgroup fixing $Y$). Its proof is of group theoretic nature.

2. Every minimal nonsolvable subcover $h$ of $\tilde{f}$, can be written as $h = h_1 \circ h_2$ with $\text{Mon}(h_1)$ solvable, and $\text{Mon}(h_2)$ primitive nonsolvable. The assumption on $\text{Mon}(h)$ to have no proper nonsolvable quotients is guaranteed once the proper quotients of $\text{Mon}(h_2)$ are solvable, by Lemma 3.5.

If $h_2$ is additionally assumed to be geometrically indecomposable and of sufficiently large degree, then Theorem 2.18 yields that, indeed, $\text{Mon}(h_2)$ has no proper nonsolvable quotients.

3. The assumptions on $\Gamma_i$, $i = 1, \ldots, r$ imply that it is primitive of type (A) or (C). The further assumption that $\Gamma_i$ is nonsolvable forces it to be of type (C).

**Example 4.3.** This example demonstrates that the assumption on the proper quotients of $\text{Mon}(h)$ 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_{m-1}^{m-1}) \times S_{m-1}, and the only intermediate subgroup between G_1 and G is the block kernel S_{n}^m \times 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 Mon(f_1) are solvable. Assume inductively that the assertion holds for r - 1.

Set \tilde{g} := f_1 \circ \ldots \circ f_{r-1}, so that f = \tilde{g} \circ f_r, set m := \deg \tilde{g}, and let \tilde{g} : \tilde{X}_{r-1} \to \mathbb{P}^1 denote the Galois closure of \tilde{g}. Let A be the (arithmetic) monodromy group of f, and K the kernel of the natural projection A \to Mon(g). In particular, A is a subgroup of \Gamma_r \cdot Mon(g), and K is a subgroup of \Gamma_r^m whose projection to each of the m components is the same and is either trivial or contains Q := soc(\Gamma_r), by Lemma 3.1.

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 \tilde{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 \leq A. Let \Gamma := Mon(h), and \phi : A \to \Gamma the restriction map. Note that by assumption \Gamma has no nontrivial nonsolvable quotients. In particular, \Gamma/\phi(K) is solvable, as long as K is not fully contained in ker \phi. As a summary consider the following diagram, where /K mean the quotient by K map.

\begin{tikzpicture}
  \node (X) at (0,0) {$X$};
  \node (Y) at (2,0) {$\mathbb{P}^1$};
  \node (Xr) at (0,-2) {$\tilde{X}_{r-1}$};
  \node (Yr) at (2,-2) {$\tilde{Y}$};
  \node (tildeX) at (0,2) {$\tilde{X}$};
  \node (tildeY) at (2,2) {$\tilde{Y}$};

  \draw[->] (X) to node [above] {} (Y);
  \draw[->] (Xr) to node [above] {} (Yr);
  \draw[->] (X) to node [above] {} (Y);
  \draw[->] (Xr) to node [above] {} (Yr);

  \draw[->] (X) to node [right] {$\phi$} (Y);
  \draw[->] (Xr) to node [right] {$\tilde{g}$} (Yr);
  \draw[->] (X) to node [right] {$f$} (Y);
  \draw[->] (Xr) to node [right] {$\tilde{f}$} (Yr);

  \draw[->] (tildeX) to node [above] {$/K$} (X);
  \draw[->] (tildeX) to node [above] {$/\ker \phi$} (Y);
  \draw[->] (tildeX) to node [above] {$/A_1$} (Xr);
  \draw[->] (tildeX) to node [above] {$/\ker \phi$} (Yr);

  \draw[->] (tildeY) to node [right] {$h$} (Y);
  \draw[->] (tildeY) to node [right] {$\tilde{h}$} (Yr);
\end{tikzpicture}

Step II: Reduction to the case K \cap ker \phi = 1, and hence \Gamma/\phi(K) solvable. Since K \cap ker \phi is a normal subgroup of A, Corollary 3.2 shows that either ker \phi \geq soc(K)
or \( \ker \varphi \cap \soc(K) = 1 \) 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 \( \ker \varphi \geq \soc(K) \). 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 \( K \leq D \). Assume otherwise that \( D \) is a proper subgroup of \( DK \).

As \( \core_A(D) = \ker \varphi \), this implies \( \ker \varphi \) is a proper subgroup of \( \ker \varphi \cdot K \), and hence the natural projection \( \tilde{Y}/\varphi(K) \to \mathbb{P}^1 \) is a nontrivial subcover of \( \tilde{h} \). Since \( \Gamma = \Mon(\tilde{h}) = \varphi(A) \) has no nontrivial nonsolvable quotients, the monodromy group \( \Gamma/\varphi(K) \) of the covering \( \tilde{Y}/\varphi(K) \to \mathbb{P}^1 \) is solvable.

On the other hand, \( \soc(K) = K \cap \soc(\Gamma)^m \). Since by assumption \( \Gamma_r/\soc(\Gamma) \) is solvable, this implies that \( K/\soc(K) \) is solvable. Since \( \ker \varphi \geq \soc(K) \) and \( K/\soc(K) \) is solvable, we get that \( \varphi(K) \) is solvable. The solvability of \( \varphi(K) \) and of \( \Gamma/\varphi(K) \) contradicts the nonsolvability of \( \Gamma \).

Henceforth assume \( \ker \varphi \cap K = 1 \), i.e., \( \varphi \) is injective on \( K \). In particular, \( K \) and \( \ker \varphi \) form their direct product in \( A \). We note that since \( \Gamma \) has no nontrivial nonsolvable quotient, \( \Gamma/\varphi(K) \) is solvable, and furthermore \( \varphi(K) \) must be nonsolvable, since \( \Gamma \) is. In particular, \( \Gamma_r = \Mon(\tilde{f}_r) \) 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 \( \Mon(f) \), 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 \( \varphi(K) \not\subset \Gamma \), 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 cosets of \( A_1 \), namely the action through the quotient \( \Gamma_r = \Mon(\tilde{f}_r) \) on \( A_0/A_1 \). 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 3.3 with \( N = \ker \varphi \). This proves the claim, and hence part (1).

**Step IV:** To deduce part (2), assume moreover that \( \Gamma_i, \ i = 1, \ldots, r \) are nonsolvable and conclude that \( f'_1 \) is an isomorphism, proving that \( f'_2 \) can be chosen to be \( f' \).

Since \( f' \) is a subcover of \( f \) and \( f'_1 \) has solvable monodromy, Corollary 3.7 implies that \( f'_1 \) is an isomorphism, showing the claim.

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

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. By our assumptions, this forces \( \varphi(K_0) \) to be trivial, and hence \( \Gamma \cong \text{Mon}(f_r) \). So \( \text{Mon}(f) \) has two quotients \( \text{Mon}(g) \) and \( \text{Mon}(f_r) \), and the corresponding kernels \( K \) and \( \ker(\varphi) \) are disjoint. This implies that \( \text{Mon}(f) \) embeds into the direct product \( \text{Mon}(g) \times \text{Mon}(f_r) \), giving (a). Moreover, since \( \varphi \) induces an isomorphism of abstract groups from \( \text{Mon}(f_r) = A_0/K_0 \) to \( \Gamma \), Remark 2.11 implies that the pullback of the natural projection \( \tilde{Y}/\varphi(A_1) \rightarrow \mathbb{P}^1 \) along \( g \) is equivalent to \( f_r : \tilde{X}_r/A_1 \rightarrow X_{r-1} \) where \( \tilde{X}_r \) is the Galois closure of \( f_r \).

**Step VI:** Deducing part (b) of the addendum. We may again restrict to the case \( i = r \) by induction. For each minimal subcover \( h \) with nonsolvable monodromy indecomposable, 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 this \( N \) is independent of \( f' \) (and hence of \( h \)).

Assume there were two such normal subgroups \( N_1 \) and \( N_2 \). Then

\[
N_1/(N_1 \cap (N_2 \text{soc}(K))) \cong N_1N_2 \text{soc}(K)/(N_2 \text{soc}(K)) \leq A/(N_2 \text{soc}(K))
\]

which is solvable. On the other hand, Lemma 2.13 gives

\[
N_1 \cap (\text{soc}(K) \times N_2) = (N_1 \cap \text{soc}(K)) \times (N_1 \cap N_2) = N_1 \cap N_2.
\]

Therefore, \( N_1/(N_1 \cap N_2) \cong N_1N_2/N_2 \) is a nontrivial solvable normal subgroup of \( A/N_2 \), contradicting our assumption on \( h \) which implies that \( A/N_2 \) has no such normal subgroup. This concludes the proof. \( \square \)

5. **Main conclusions**

5.1. **The polynomial case.** Let \( k \) be a finitely generated field of characteristic 0 with algebraic closure \( \overline{k} \). The following is our most general result concerning the geometric monodromy group in the case where \( f \) is a polynomial. In the following, \( \tilde{f} : \tilde{X} \rightarrow \mathbb{P}^1_{\overline{k}} \) denotes the Galois closure of \( f \) over \( \overline{k} \) and \( f_D : \tilde{X}/D \rightarrow \mathbb{P}^1_{\overline{k}} \) the covering corresponding to \( D \leq G \).

**Theorem 5.1.** Suppose \( f = f_1 \circ \ldots \circ f_r \in \overline{k}[x] \) for indecomposable polynomials \( f_i, i = 1, \ldots, r \) with nonsolvable monodromy groups. Let \( D \leq \text{Mon}_\overline{k}(f) \) be an intransitive subgroup whose corresponding covering \( f_D : \tilde{X}/D \rightarrow \mathbb{P}^1 \) is of genus \( \leq 1 \). Then there exists a subcover \( h \) of \( f_D \) with the same Galois closure as \( f_1 \).
Proof. Step I: Basic setup, following Theorem 4.1. Let \( G = \text{Mon}_F(f) \). By [30], all \( \text{Mon}_F(f_i) \) are nonabelian almost simple. Thus, the assumptions of Theorem 4.1 are fulfilled. By Corollary 3.10, \( f_D \) is not a composition of coverings with affine monodromy. There must therefore be a minimal subcover \( h_1 : Z_1 \to \mathbb{P}^1 \) of \( f_D \) with decomposition \( h_1 = h_0 \circ h' \) such that \( h_0 : Z_0 \to \mathbb{P}^1 \) is a composition of covers with affine monodromy and \( h' : Z_1 \to Z_0 \) is an indecomposable covering with nonaffine (in particular, nonsolvable) monodromy. We will show that \( h_1 \) has a subcover \( h \) with the same Galois closure as \( f_1 \) over \( k \).

As in the proof of Theorem 4.1, let \( K \) be the kernel of the projection \( G \to \text{Mon}(f_1 \circ \cdots \circ f_{r-1}) \) and \( \varphi \) the projection from \( G \) onto the monodromy group \( \Gamma \) of \( h \). Note that \( K \neq 1 \) by Remark 2.15, as \( f_1, \ldots, f_r \) are polynomials.

Let \( f'_1 : X'_1 \to Z_0 \) be the natural projection from the fiber product of \( f_1 \) and \( h_1 \) to \( Z_0 \). Inductively, define \( f'_{i+1} : X'_{i+1} \to X'_i \) to be the pullback of \( f_{i+1} \) along the natural projection \( X'_i \to X_i \). Since \( K \neq 1 \) and similarly \( \ker(\text{Mon}(f_1 \circ \cdots \circ f_i) \to \text{Mon}(f_1 \circ \cdots \circ f_{i-1})) \neq 1 \) for all \( i \), we may apply Lemma 3.8 and deduce that each \( X'_i \) is irreducible, and hence \( f'_i \) is a covering. Also note that \( Z_0 \) is of genus 0, since otherwise \( h' \) is a covering between genus 1 curves, hence with abelian monodromy [42, Theorem 4.10(c)], contradicting the assumption that its monodromy is nonaffine.

Step II: Applying Theorem 4.1 to \( h' \). Let \( f' := f'_1 \circ \cdots \circ f'_r \), let \( f'_1 \) be its Galois closure, and \( G' = \text{Mon}(f') \). We check that \( f' \) and \( h' \) have the necessary properties to apply Theorem 4.1.

\[
\begin{array}{ccccccccc}
X'_r & \to & \cdots & \to & X'_1 & \to & Z_0 & \to & Z_1 \\
\downarrow f'_r & & & & \downarrow f_1 & & \downarrow h_0 & & \downarrow h_1 \\
X_r & \to & \cdots & \to & X_1 & \to & \mathbb{P}^1 & & \\
end{array}
\]

Firstly, we note that the Galois closure of \( f' \) is the same as that of \( f \). Indeed, letting \( G_1 \) (resp. \( U \)) be the Galois group of the natural projection \( X \to X_r \) (resp. \( X \to Z_0 \)), it suffices to show that \( \bigcap_{u \in U} (U \cap G_1)^u = \{1\} \). But by Corollary 3.10, \( U \) is transitive, so \( \bigcap_{u \in U} (U \cap G_1)^u \subseteq \bigcap_{u \in U} G_1^u = \bigcap_{g \in G} G_1^g = \{1\} \), showing that \( G' = U \) as claimed.

Next, we show that \( \text{Mon}(f'_1) \) is almost simple with primitive action, for all \( i \). Let \( K' \) be the block kernel in \( G' \) under the projection to \( \text{Mon}(f'_1 \circ \cdots \circ f'_{r-1}) \). As in Remark 3.9, \( G' \) contains all nonabelian composition factors of \( G \), which in particular forces \( K' \) to contain \( \text{soc}(G) = \text{soc}(K) \). In particular, the projection of \( K' \) to a single
block, still contains \( \text{soc}(\text{Mon}(f_i)) \), and is therefore still primitive.\(^9\) Thus \( \text{Mon}(f_i') \) is almost simple with primitive action. Iteratively, the same holds for \( f_i' \), for all \( i \).

Finally, Lemma 2.20 verifies that the proper quotients of \( \Gamma' := \text{Mon}(h') \) are solvable. We may therefore apply Theorem 4.1 and deduce that \( h' \) has the same Galois closure as some indecomposable subcover of \( f' \).

**Step III:** Showing that \( h_1 \) factors through a nonsolvable subcover of \( f_1 \). First note that \( \text{soc}(K') = \text{soc}(K) \) is still a unique minimal normal subgroup of \( \text{soc}(G') \).\(^10\) Indeed, we have already seen in step II that \( K' \) and hence \( \text{soc}(K') \) contain \( \text{soc}(K) \). On the other hand, since \( \text{soc}(K) = \text{soc}(G) \) by Corollary 3.4, \( \text{soc}(K) \) has a trivial centralizer in \( G \), forcing \( \text{soc}(K') = \text{soc}(K) \). Furthermore, letting \( G_0 \) denote the Galois group of the covering \( X \to X_{r-1} \), Corollary 3.10 again implies that the (block) action of \( G' \) on \( G/G_0 \cong G'/\langle G_0 \cap G' \rangle \) is transitive. Hence \( \text{soc}(K') \) is a minimal normal subgroup of \( G' \) by Corollary 3.2.

It follows that either \( \ker \varphi \supseteq \text{soc}(K') \) or \( \ker \varphi \cap \text{soc}(K') = 1 \). In the latter case, since \( \text{soc}(K') \) is the unique minimal normal subgroup of \( G' \), it follows that \( \ker(\varphi) = 1 \).

So \( \Gamma' = G' \) has a faithful primitive action of genus \( \leq 1 \) without nontrivial nonsolvable quotients by step II. If \( r > 1 \), this contradicts the fact that \( \text{Mon}(f_1' \circ \cdots \circ f_r') \) is a proper nonsolvable quotient of \( G' \). In the case \( r = 1 \), this means that \( G \) is almost simple and the assertion is immediate.

We may therefore assume that \( \ker \varphi \supseteq \text{soc}(K') \) and \( r > 1 \). Thus, \( \varphi(K') \) is a solvable subgroup of \( \Gamma' \). Since by step II, \( \Gamma' \) has no normal solvable subgroups, it follows that \( \varphi(K') = 1 \), that is, \( \ker \varphi \supseteq K' \). This shows that \( h' \) is a subcover of the Galois closure of \( f_1' \circ \cdots \circ f_r' \). Iterating the above argument with \( 1 < i < r \), we get that \( h' \) is a subcover of \( f_1' \). In particular, since \( \text{Mon}(f_1') \) is almost simple and \( h' \) has nonsolvable monodromy, this shows \( \Gamma' = \text{Mon}(f_1') \).

As in Remark 2.11, \( \Gamma' = \text{Mon}(f_1') \) can therefore be identified with a subgroup of \( \text{Mon}(f_1) \). Furthermore, letting \( \Gamma_1' \) denote the point stabilizer in \( \Gamma' = \text{Mon}(f_1') \), the remark shows that \( h' \), which is equivalent to the covering \( \tilde{X}_1/\Gamma_1' \to \tilde{X}_1/\Gamma' \), is a pullback of the natural projection \( \tilde{X}_1/\Gamma_1' \to \tilde{X}_1/\Gamma' \). Thus, its composition with the natural projection \( \tilde{X}_1/\Gamma' \to \tilde{X}_1/\Gamma \) is a subcover \( h : \tilde{X}_1/\Gamma_1' \to \tilde{X}_1/\Gamma \) of \( h_1 \) whose Galois closure is \( \tilde{f}_1 \), as desired. \( \square \)

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

---

\(^9\)The last implication follows directly from the classification of primitive monodromy groups of polynomials, but can also be obtained using standard group-theoretical results: indeed, any primitive group with a full cycle is known to be either of prime degree (in which case the socle is trivially primitive) or 2-transitive; finally, the minimal normal subgroup of a non-affine 2-transitive group is known to be simple and primitive due to Burnside.

\(^{10}\)Since \( X_i' \) is not necessarily of genus 0, we cannot simply deduce this from Corollary 3.4.
Corollary 5.2. Let \( f = f_1 \circ \cdots \circ f_r \) be a decomposition of the polynomial \( f \in k[x] \) into indecomposable polynomials. Assume that none of the \( f_i \) has solvable monodromy, and that \( \deg(f_1) > 20 \). Then \( R_f \) and \( R_{f_1} \) differ only by a finite set. More precisely, one of the following holds:

1. \( R_f = f_1(k) \cup S \) for a finite set \( S \);
2. There exists a (single) covering \( f'_1 : X \to \mathbb{P}^1 \) over \( k \) with genus \( g_X \leq 1 \), such that \( R_f \) and \( f_1(k) \cup f'_1(X(k)) \) differ by a finite set. Moreover, \( f_1 \) is as in Table 1 or of monodromy group \( PGL_3(4) \) or \( PSL_5(2) \), and \( f'_1 \) is a subcover of the Galois closure of \( f_1 \).

If furthermore \( k \) is a number field with ring of integers \( \mathcal{O}_k \) and \( \text{Mon}(f_1) \notin \{ PGL_3(4), PSL_5(2) \} \),\(^\text{11}\) then \( R_f \cap \mathcal{O}_k = (f_1(k) \cap \mathcal{O}_k) \cup S' \) for a finite set \( S' \).

Proof. Let \( A \) and \( G \) denote the arithmetic and geometric monodromy group of \( f \). By Corollary 2.5 it suffices to determine the subcovers \( f_D : \bar{X}/D \to \mathbb{P}_k^1 \) for \( D \leq A \) such that \( \bar{X}/D \) is of genus \( \leq 1 \), and \( D \) is maximal intransitive with \( D \cdot G = A \). Letting \( C := D \cap G \) for such \( D \), Theorem 5.1 implies that \( f_C \) has a subcover \( h \) over \( \bar{k} \) with the same Galois closure as \( f_1 \).

Step I: From geometric to arithmetic. We claim that the cover \( f_D \) (over \( k \)) also has a subcover \( h' \) with the same Galois closure as \( f_1 \) (over \( k \)). We may then apply Lemma 2.22 to reduce the problem to enumerating the subcovers \( f_C \) over \( \bar{k} \) of the Galois closure of \( f_1 \). Indeed, since \( \deg f_1 > 20 \), Remark 2.23(2) after the lemma shows that the above minimally nonsolvable \( h' \) have reducible fiber product with \( f_1 \) (and a fortiori with \( f \)). Minimality in the definition of \( f_D \) therefore yields \( f_D = h' \). Moreover, the lemma implies that \( h' \) as a covering over \( \bar{k} \) is uniquely defined over \( k \). It follows that each minimal covering \( f_D \) as above corresponds to a unique indecomposable subcover \( f_C \) over \( \bar{k} \) of the Galois closure of \( f_1 \), as desired.

To show the claim, consider the image of \( D \) under the projection \( \pi \) from \( A \) onto \( \text{Mon}_k(f_1) \). We separate into two cases according to the solvability of the action of \( \text{Mon}_k(f_1) \) on cosets of \( \pi(D) \). In the nonsolvable case, since \( k \)-subcover \((f_1)_{\pi(D)} : \bar{X}_1/\pi(D) \to \mathbb{P}_k^1 \) of \( \bar{f}_1 \) is also a subcover of \( f_D \) by construction, we readily obtain the claim. Otherwise, the action on \( \text{Mon}_k(f_1)/\pi(D) \) is solvable. By Theorem 2.14, \((f_1)_{\pi(G \cap D)} : \bar{X}_1/\pi(G \cap D) \to \mathbb{P}_k^1 \) has a subcover \( f_C \) with nonsolvable monodromy. On the other hand, since \( \deg f_1 > 20 \), Remark 2.17 implies that either \( A = G \) or \((A, G) = (S_n, A_n) \). In both cases, \( \pi(D) \) contains the socle of \( A \) due to the solvability of the action of \( \text{Mon}_k(f_1)/\pi(D) \). Since \( \pi(D \cap G) \) is normal in \( \pi(D) \), either \( \pi(D \cap G) \) contains the socle as well, contradicting again the nonsolvability of \( \text{Mon}_k(f_C) \); or \( \pi(D \cap G) = 1 \) contradicting the fact that \( f_C \) is a cover of genus \( \leq 1 \).

\(^{11}\)Note that this extra assumption on \( \text{Mon}(f_1) \) is unnecessary for, e.g., \( k = \mathbb{Q} \), since those two groups do not occur as monodromy groups of polynomials with rational coefficients, see [30].
**Step II:** Enumeration of covers over $\overline{k}$. We claim that there are at most two equivalence classes for $h'$ over $\overline{k}$ (both of which have reducible fiber product with $f_1$).

The only possible nonsolvable monodromy groups for indecomposable $f_1$ of degree $>20$, which are not alternating or symmetric, are $\text{PGL}_3(4)$, $M_{23}$, and $\text{PSL}_5(2)$. A computer check shows that the only polynomial ramification type in $M_{23}$ does not have genus $\leq 1$ in any other permutation action of $M_{23}$, so in this case, (1) is fulfilled. In the same way, for $\text{PGL}_3(4)$ and $\text{PSL}_5(2)$, one verifies that the corresponding polynomials have only one nontrivial action with genus $\leq 1$, and its stabilizer $U$ acts intransitively, whence (2) is fulfilled. The ramification types of those $f_1$ with alternating or symmetric monodromy admitting more than one faithful action of genus $\leq 1$ are listed in Table 1. These admit one additional minimal nontrivial action of genus $\leq 1$, 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 covers $f_1'$ in case (2) are not Siegel functions by Theorem 2.14.

**Remark 5.3.** 1) We 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 $\leq 1$ subcovers of $\tilde{f}_1$ are listed in [20, Theorem A.4.1]. Adding this exceptional list to Theorem 1.1, as well as the list arising from [30], would lower the degree assumption on $f_1$ to merely $\deg f_1 \geq 10$.

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. Indeed, to obtain an exception, $\text{Mon}(f_1)$ needs to act as the monodromy group of another Siegel function $f_1'$ not equivalent to $f_1$. Since this action may be assumed minimally nonsolvable and $\text{Mon}(f_1)$ is almost simple, this means that either $\text{Mon}(f_1)$ must induce a Siegel function in a second action permutation-equivalent to the one on the roots of $f_1(X) - t$; or some subgroup between $\text{Mon}(f_1)$ and its socle must induce a Siegel function in a different primitive action. From the classification of primitive monodromy groups of Siegel functions in [31] (in particular Theorems 4.8 and 4.9), one extracts easily (aided by a computer check) that the first scenario happens only for $\text{Mon}(f_1) \in \{\text{PSL}_2(11), \text{PSL}_3(2), \text{PSL}_3(3), \text{PSL}_4(2), \text{PGL}_3(4), \text{PSL}_5(2)\}$, whereas the second one only happens for $\text{Mon}(f_1) \in \{A_5, S_5, \text{PSL}_3(2), \text{PGL}_2(9), M_{11}, \text{PSL}_4(2)\}$. Out of those possibilities, only the polynomials with monodromy group $S_5$ and $\text{PGL}_2(9)$ 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., [31, Section 4.4]). It follows for example that, for $k = \mathbb{Q}$, one may replace $\deg(f_1) > 20$ by $\deg(f_1) > 5$ for the statement about integral specializations.

Finally we apply Theorem 5.1 to prove Corollary 1.4:
Proof of Corollary 1.4. It is well known that the reducibility of \( u(x) - v(y) \in \mathbb{C}[x, y] \) implies the reducibility of the fiber product of the coverings \( u : \mathbb{P}^1 \to \mathbb{P}^1, v : \mathbb{P}^1 \to \mathbb{P}^1 \).

By Lemma 2.10, we may replace \( v \) by a polynomial subcover \( v_0 \) of the Galois closure \( \tilde{u} \), since its fiber product with \( u \) is still reducible. Theorem 5.1 then shows that there is a polynomial subcover \( w \) of \( v_0 \), with the same Galois closure as \( u_1 \). Since \( \deg u_1 > 31 \) the possibilities for \( w \) are described in Theorem 2.14 cases (1)-(2). Moreover, in case (2), \( w \) is never a polynomial. In case (1), \( w \) and \( u_1 \) are equivalent, and hence \( u \) factors through \( w \) as well, as desired. \( \square \)

We note that Remark 5.3.(1) applies similarly to Corollary 1.4.

Remark 5.4. The combination of a recent work by Wang and Zieve ([44]) with the classification of monodromy groups can be used to generalize Remark 2.16 (Ritt’s theorem) to rational functions, showing that (over an algebraically closed field) the decomposition of a rational function \( f = f_1 \circ \cdots \circ f_r \) into (geometrically) indecomposable rational functions is unique as soon as all \( f_i \) have nonsolvable monodromy of sufficiently large degree, and \( f_1 \) is not linearly related to a function of the form \( x^a(x - 1)^b \). By replacing \( \mathbb{Q} \) by a finite extension \( k \), we may assume the arithmetic monodromy is the same as the geometric. Repeating the above argument in this case then gives: Let \( f_1, \ldots, f_r \) be geometrically indecomposable rational functions over \( \mathbb{Q} \), with nonsolvable monodromy group of sufficiently large degree, and let \( f = f_1 \circ \cdots \circ f_r \). Then either \( f_1 \) is listed in [36, Table 4.2] or in [37, Table 3.1], or there exists some finite extension \( k'/\mathbb{Q} \) over which \( R_f \) is the union of \( R_{f_1} \) and a finite set. The complete result follows from the (anticipated) classification of arithmetic monodromy groups.

5.2. Composition of coverings with almost simple monodromy. Finally the following theorem strengthens Theorem 1.2:

Theorem 5.5. 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. Then there exist a finite extension \( k'/k \), nonsolvable indecomposable coverings \( h_i : Y_i \to \mathbb{P}^1_k \) of genus \( \leq 1 \), \( 1 \leq i \leq u \), and \( h'_j : Y'_j \to \mathbb{P}^1_{k'} \) of genus 0, \( 1 \leq j \leq v \), such that \( v \leq u \leq r \) and

\[
R_f(k') \subseteq \bigcup_{i=1}^u h_i(k') \cup \bigcup_{j=1}^v h'_j(k') \cup S
\]

for some finite set \( S \), with equality if all alternating or symmetric groups \( \text{Mon}(f_i) \) occur in the natural permutation action.

\[12\] For a rational function \( f(x) = \frac{p(x)}{q(x)} \), the term \( R_f \) means \( \text{Red}_F \) with \( F(t, x) = p(x) - tq(x) \).
More precisely, \( u \) is at most the number of \( i \in \{ 1, \ldots, r \} \) such that \( \text{Mon}(f_i) \) is isomorphic to an alternating or symmetric group and \( \text{Mon}(f_1 \circ \cdots \circ f_i) \) embeds into \( \text{Mon}(f_1 \circ \cdots \circ f_{i-1}) \times \text{Mon}(f_i) \); out of which \( v \) is the number of \( i \)'s for which the ramification of \( h_i \) is as in (1) of Theorem 2.18.

Proof. Set \( k' := k \cap \Omega \), where \( \Omega \) is the Galois closure of \( k(X)/k(\mathbb{P}_1^k) \), so that the arithmetic and geometric monodromy groups \( A := \text{Mon}_k(f) \) and \( G := \text{Mon}_\mathbb{F}(f) \) identify, cf. Remark 5.6. We shall henceforth replace \( k \) by \( k' \) and assume \( A = G \).

Let \( \tilde{f} : \tilde{X} \to \mathbb{P}_1^k \) be the Galois closure of \( f \). To deduce the assertion from Corollary 2.5, it suffices to find (up to equivalence) all minimal \( k \)-subcovers \( h : Z \to \mathbb{P}_1^k \) of \( \tilde{f} \) whose fiber product with \( f \) is reducible and for which \( Z \) is of genus \( \leq 1 \). By Lemma 3.6 we may and will restrict without loss of generality to minimal nonsolvable subcovers \( h \).

Step I: Choice of \( N \). By Theorem 2.18 (the classification of monodromy groups), there exists a constant \( N \) such that for every indecomposable covering \( h_\mathbb{F} : Z' \to \mathbb{P}_1^k \) with genus \( g_{Z'} \leq 1 \) and nonsolvable monodromy \( \Gamma \) of order \( \geq N \), the group \( \Gamma \) is nonsolvable without proper nonsolvable quotients. Furthermore by Remark 2.19, for large \( N \), there are at most two minimally nonsolvable (and, in fact, necessarily indecomposable) subcovers of \( h_\mathbb{F} \) with genus \( \leq 1 \), and at most one such subcover if the ramification of \( h_\mathbb{F} \) does not appear in Theorem 2.18. Note that in case there are two such subcovers and \( \Gamma \) is almost simple, Remark 2.19 implies that \( \Gamma \) is alternating or symmetric (and in fact, from [36], 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 composition of rational functions with solvable monodromy and \( h_2 : Z \to \mathbb{P}_1^k \) is nonsolvable of large degree. Since \( A = G \), Theorem 2.18 implies that \( \text{Mon}_k(h_2) \) and hence \( \Gamma \) do not have a proper nonsolvable quotient. 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 \( \text{Mon}_k(f_i) \) for some \( i \). Also note that since by Theorem 2.18, \( \Gamma \) is alternating or symmetric, and \( h \) is of genus \( \leq 1 \) is 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 \( u_f := u \) and \( v_f := v \) 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 contained in the Galois closure of \( g \), or in the Galois closure of a uniquely determined indecomposable subcover \( h' \) of \( f \) with \( \text{Mon}(h') \cong \text{Mon}(f_r) \).

Therefore, our choice of \( N \) implies:

1. If \( h' \) as above exists, then \( \text{Mon}_k(f_r) \cong \text{Mon}_k(h') \) is isomorphic to an alternating
or symmetric group. In particular, if $\text{Mon}_k(f_r)$ is nonalternating and nonsymmetric, then $u_f = u_g$, $v_f = v_g$, and $m_f = m_g$, as desired;

(2) If $\text{Mon}_k(f_r)$ is alternating or symmetric, the Galois closure $\tilde{h}'$ contains at most two minimal subcovers $h : Z \to \mathbb{P}^1$ with genus $g_Z \leq 1$ and nonsolvable monodromy, and at most one such subcover if its ramification does not appear in Theorem 2.18. 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 rather than just inclusion in (5.1), it suffices to show that all occurring covers $h_i$ and $h'_i$ in fact have reducible fiber product with $f$, see Remark 2.9. For each $i \in \{1, \ldots, u\}$, denote by $f'_i$ the subcover of $f$ whose Galois closure equals the one of $h_i$, ensured by Theorem 4.1. It of course suffices a fortiori to show that the fiber product of $h_i$ and (if exists) of $h'_i$ with $f'_i$ is reducible. The latter is in general not true if $\text{Mon}(f'_i)$ is alternating or symmetric in a “nonnatural” primitive action. However, from Theorem 2.18, it is true as soon as that action is the natural one, concluding the proof. □

Remark 5.6. (1) In Theorem 5.5, one shall in fact be able to take $k'$ to be $k$. Indeed, the only place where the proof uses the assumption $A = G$ is in order to verify that the monodromy group $\tilde{A} := \text{Mon}_k(h_2)$ 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, which does not happen in our scenario. Note that the assertions in Step I are already available by Lemma 2.20.

(2) Let $k$ be a number field with ring of integers $O_k$. Note that by using Corollary 2.5 to describe $R_f \cap O_k$, we furthermore get that the coverings $h_1, \ldots, h_s$ are Siegel functions. Recall that Remark 2.19 asserts that the Galois closure of a geometrically indecomposable cover $h$ of large degree factors through at most one Siegel subcover with nonsolvable monodromy. Hence, the same argument 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 $f$, where $s \leq u$, with $u$ as defined above.

(3) The assumption that $\text{Mon}(f_i)$ is almost simple in Theorem 5.5 can be relaxed with some extra effort. The maximal number of coverings needed to describe $R_f$ should then be $3r$ (rather than $2r$), due to the fact that, given a large degree indecomposable covering $h : Z \to \mathbb{P}^1$ of genus $g_Z \leq 1$ and nonsolvable monodromy, $\tilde{h}$ factors through at most three minimal subcovers of genus $\leq 1$ and nonsolvable monodromy (and the fiber product of any two of those is reducible), as pointed out in Remark 2.19.
THE REDUCIBILITY OF $F(t_0,x)$

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, 14, 15
[3] P. Cassou-Noguès, J. Couveignes, Factorizations explicites de $g(y) − h(z)$, Acta Arith. 87 (1999), 291–317. 11
[4] H. Davenport, D. J. Lewis, A. Schinzel, Equations of the form $f(x) = g(y)$. Quarterly J. of Math. 12 (1961), 304–312. 5
[5] H. Davenport, A. Schinzel, Two problems concerning polynomials. J. Reine Angew. Math. 214 (1964), 386–391. 5
[6] P. Dèbes, M. D. Fried, Integral specialization of families of rational functions. Pacific J. Math., 190 (1999), 45–85. 2
[7] 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 Vol. 63 (2012),
141–162. 6
[8] J. D. Dixon, B. Mortimer, Permutation Groups. Springer GTM 163 (1996). 14, 15
[9] P. Dèbes, Y. Walkowiak, Bounds for Hilbert’s irreducibility theorem. Pure Appl. Math. Q. 4
(2008), Special Issue: In honor of Jean-Pierre Serre. Part 1, 1059–1083. 1
[10] M. D. Fried, R. E. MacRae, On the invariance of chains of fields. Illinois J. Math. 13(1969),
165–171. 6, 11
[11] M. Fried, The field of definition of function fields and a problem in the reducibility of polyno-
mials in two variables. Illinois J. of Math. 17 (1973), 128–146. 5
[12] M. D. Fried, On Hilbert’s irreducibility theorem. J. Number Theory 6 (1974), 211–231. 2
[13] M. D. Fried, Applications of the classification of simple groups to monodromy, part ii: Daven-
port and Hilbert–Siegel problems, preprint (1986), 1–55. 2
[14] 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. 5
[15] M. D. Fried, On the Sprindzuk-Weissauer approach to universal Hilbert subsets. Israel J. Math.
51 (1985) 347–363. 8
[16] 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
[17] M. D. Fried, I. Gusić, Schinzel’s problem: imprimitive covers and the monodromy method.
Acta Arith. 155 (2012), 27–40. 5
[18] R. Guralnick, Monodromy Groups of Coverings of Curves. Galois Groups and Fundamental
Groups, MSRI Publications 41 (2003). 10
[19] R. Guralnick, M. Neubauer, Monodromy groups of branched coverings: the generic case. Contemp.
Math. 186 (1995), 325–352. 13
[20] 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). 4, 11, 12, 27
[21] R. Guralnick, J. Thompson, Finite groups of genus zero. J. Algebra 131 (1990), 303–341. 4, 13
[22] J. König, D. Neftin, The admissibility of $M_{11}$ over number fields. J. Pure Appl. Alg. 222 (2018),
2456–2464. 7
[23] J. König, On the reducibility behavior of Thue polynomials. J. Number Theory 176 (2017), 37–45.
[24] D. Krumm, N. Sutherland, Galois groups over rational function fields and explicit Hilbert irreducibility. arXiv:1708.04932.
[25] K. Langmann, Werteverhalten holomorpher Funktionen auf Überlagerungen und zahlen-theoretische Analogien II. Math. Nachr. 211 (2000), 79–108.
[26] 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).
[27] T. Monderer, Genus 0 subfields of symmetric and alternating extensions. M.Sc. Thesis. 2018.
[28] T. Monderer, Families of polynomials and extensions under specialization. Ph.D. Thesis. In preparation.
[29] T. Monderer, D. Neftin, Genus zero subfields of symmetric and alternating extensions. Preprint, December 2019.
[30] P. Müller, Primitive monodromy groups of polynomials. Recent developments in the inverse Galois problem, Contemp. Maths. 186, 385–401, Amer. Math. Soc., 1995.
[31] 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.
[32] P. Müller, Hilbert’s irreducibility theorem for prime degree and general polynomials. Israel J. Math. 109, (1999), 319–337.
[33] P. Müller, Finiteness results for Hilbert’s irreducibility theorem. Ann. Inst. Fourier 52 (2002), 983–1015.
[34] P. Müller, Reducibility behavior of polynomials with varying coefficients. Israel J. Math. 94 (1996), 59–91.
[35] P. Müller, M. Zieve, On Ritt’s polynomial decomposition theorems. Preprint, arXiv:0807.3578.
[36] D. Neftin, M. Zieve, Monodromy groups of indecomposable coverings of bounded genus. Preprint, July 12, 2016.
[37] D. Neftin, M. Zieve, Monodromy groups of product type. Preprint, July 12, 2016.
[38] J. F. Ritt, Prime and composite polynomials. Trans. Amer. Math. Soc. 23 (1922), 51–66.
[39] A. Schinzel, Some unsolved problems on polynomials. Mate. Biblioteka 25 (1963), 63–70.
[40] T. Shih, A note on groups of genus zero. Comm. Algebra 19 (1991), 2813–2826.
[41] J.-P. Serre, Topics in Galois theory. Second edition. Springer, 2008.
[42] J. H. Silverman, The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Second Edition.
[43] Y. Walkowiak, Théorème d’irréductibilité de Hilbert effectif. Acta Arithmetica 116 (2005), 343–362.
[44] F. Wang, M. Zieve, Report, PRIME project 2016.