THE DAVENPORT–LEWIS–SCHINZEL PROBLEM ON THE REDUCIBILITY OF $f(X) - g(Y)$

ANGELOT BEHAJAINA, JOACHIM KÖNIG, AND DANNY NEFTIN

Abstract. We solve the problem of Davenport–Lewis–Schinzel (DLS), originating in the 1950s, regarding the reducibility of $f(X) - g(Y) \in \mathbb{C}[X, Y]$. This yields an almost-complete solution to the Hilbert–Siegel problem: For a polynomial map f whose composition factors avoid only very specific low-degree polynomials, we explicitly describe over which integers the fibers of f are reducible. We further apply the solution to stability of iterates of f in arithmetic dynamics, and to solving the functional equation $f(X) = g(Y)$ in $X, Y \in \mathbb{C}(z)$.

1. Introduction

Reducibility of polynomials is a central topic of interest in number theory, cf. [Sch00]. In a prominent paper [Sch63], Schinzel poses nine problems concerning reducibility of polynomials. As Zannier notes in [Sch07, Part E], the first three are "substantial, involving several mathematical fields," owing to their relation to monodromy, combinatorial group theory, and the classification of finite simple groups (CFSG). The first problem originates in the late 1950s [Ehr58], cf. [Cas68, Pg. 2], and is first stated by Davenport–Lewis–Schinzel [1] in [DLS61]. We henceforth refer to it as the DLS problem. The second problem concerning the irreducibility of $(f(X) - f(Y))/(X - Y)$ was solved by Fried [Fri70, Thm. 1], while the third problem concerning the reducibility of separated polynomials $f(X_1, \dots, X_m) - g(Y_1, \dots, Y_n) \in \mathbb{Q}[X_1, \dots, Y_n]$ was reduced to the DLS problem [DS64, Thm. 2]. As we shall see below, the DLS problem arises naturally in several topics including Hilbert's irreducibility, low degree points in fibers, stability in arithmetic dynamics, functional equations, Kronecker equivalence [Mü98], intersections of lemniscates [Pak23a], expanding polynomials [Tao12, Tao15], and sum-product estimates [BT12, Pf. Thm. 6].

The DLS problem is deceptively easy to state:
"For which polynomials $f, g \in \mathbb{C}[X]$ of degree ≥ 2, is $f(X) - g(Y) \in \mathbb{C}[X, Y]$ reducible?"
This is equivalent to the reducibility of the curve $f(X) = g(Y)$, as well as to the reducibility of the fiber product of the maps $f, g : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. Trivially, (a) $f(X) - f(Y)$ has a diagonal factor $X - Y$, and (b) if $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ is reducible, then so is the substitution $f_1(f_2(X)) - g_1(g_2(Y))$ for $f_2, g_2 \in \mathbb{C}[X] \setminus \mathbb{C}$ with $(\deg(f_2), \deg(g_2)) \neq (1, 1)$. A pair f, g for which $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is reducible but is not of the form (b) is called *minimally reducible*. Among such pairs, those not arising from (a) via linear substitutions are called *nontrivial*. The problem is then to classify the nontrivial minimally reducible pairs f, g.

[1] The problem is sometimes attributed solely to Schinzel, see e.g. [FG12, Fri12].

The first nontrivial pair $(f, g) = (T_4, -T_4)$ was given by Davenport, Lewis, and Schinzel [DLS61], where T_n is the degree-n Chebyshev polynomial satisfying $T_n(X + 1/X) = X^n + 1/X^n$. The close relation of the DLS problem with monodromy groups of polynomials was then revealed by Cassels–Guy [Cas68], proving the existence of nontrivial pairs where $\deg(f) = \deg(g)$ is 7 or 11. The degree-7 polynomials, for example, arise from the inequivalent actions of their monodromy group $\mathrm{Mon}(f) = \mathrm{PSL}_3(2)$ on points and lines in the Fano plane, or equivalently, on lines and hyperplanes in $\mathbb{F}_2^3$, arising from an outer automorphism of $\mathrm{PSL}_3(2)$. Explicit such polynomials were known by Klein's work [Kle79b, Kle79a], and an extended family was given by Birch [Cas68, Pg. 14]. After extensive work on the case where $f, g \in \mathbb{C}[X]$ are indecomposable polynomials (i.e., cannot be written as a composition of two polynomials of degree > 1), e.g. [Sch67, Tve68], Fried showed that the reducibility of $f(X) - g(Y) \in \mathbb{C}[X, Y]$ for such f, g implies that $\deg(f) = \deg(g)$ is $7, 11, 13, 15, 21$, or 31. This was announced in [Fri73] contingent on the CFSG, and the proof is given in [Fri86b]. As above, the source of all such examples lies in outer automorphisms of $\mathrm{Mon}(f)$. The indecomposable polynomials of these degrees were then given by Cassou-Noguès–Couveignes [CNC99]. Throughout many of the above stages, it was speculated and sometimes conjectured that no further minimally reducible pairs exist. The potentially-existing minimally reducible pair of polynomials with ≥ 4 branch points is also referred to as a "Cassels monster" [Cas68, Pg. 15].

For decomposable polynomials, the problem has so far remained largely open. Illustrating the difficulty of the decomposable case, Fried posed the $(2, 3)$-problem [Fri86b], cf. [Fri12, Prob. 7.31],[Fri87, Pg. 15]: given an elliptic curve $Y^2 = p(X)$, where $p \in \mathbb{C}[X]$ is simply-branched of degree 3, is there a substitution $Y \mapsto g(Y)$, $X \mapsto f(X)$ for $f, g \in \mathbb{C}[X] \setminus \mathbb{C}$ such that $g(Y)^2 = p(f(X))$ is reducible over $\mathbb{C}$? More generally, for integers $m, n \geq 2$, not both 2, the (m, n)-problem is stated similarly, replacing Y^2 and $p(X)$ by simply-branched polynomials of degrees m, n, resp., with disjoint branch loci. The decomposable case has been further studied including in determining when $f(X) - g(Y) \in \mathbb{C}[X, Y]$ admits a quadratic factor by Bilu [Bil99]; and in studying when $f(X) - (\alpha \circ f)(Y)$ is reducible for $\alpha \in \mathbb{C}[X]$ of degree 1 by Avanzi–Zannier [AZ03] and Fried–Gusić [Fri12, FG12]. Further references and context can be found on MathOverflow [Rur12, Tao12].

So far, all known minimally reducible pairs arise from the pair $(T_4, -T_4)$ or one of the above indecomposable pairs. On the other hand, little was known about the existence of decomposable minimally reducible pairs: the $(2, 3)$-problem has remained widely open, and it was even unclear whether minimally reducible pairs could be of unbounded degree.

We prove there exist no further examples, thereby solving the DLS problem:

Theorem 1.1. *Let $f, g \in \mathbb{C}[X]$ be of degree > 1. Then $f(X) - g(Y)$ is reducible in $\mathbb{C}[X, Y]$ if and only if one of the following holds for some $f_1, g_1, \mu \in \mathbb{C}[X] \setminus \mathbb{C}$ with $\deg(\mu) = 1$:*

(1) f and g have a common left composition factor $h \in \mathbb{C}[X]$ of degree at least 2, that is, $f = h \circ f_1$ and $g = h \circ g_1$;
(2) $f = (\mu \circ h_1) \circ f_1$ and $g = (\mu \circ h_2) \circ g_1$, where (h_1, h_2) is one of the pairs of polynomials of degrees 7,11,13,15,21, or 31 given in [CNC99, §5]*;*
(3) $f = (\mu \circ T_4) \circ f_1$ and $g = (\mu \circ (-T_4)) \circ g_1$.

The problem is solved more generally over an arbitrary field k of characteristic 0 in Theorem 6.1, which specializes to Theorem 1.1 for $k = \mathbb{C}$. In particular, this solves the (m, n)-problem for all relevant m, n, see Corollary A.1. Since all minimally reducible pairs in Theorem 1.1 have three branch points, this also rules out the existence of a Cassels monster. Theorem 1.1 also proves [Fri12, Conj. 7.29], cf. [FG12, §1.4], concerning the reducibility of $f(X) - (\alpha \circ f)(Y)$ for $\alpha \in \mathbb{C}[X]$ of degree 1. It also extends [KN24, Thm. 1.2] which restricts to nonsolvable decomposition factors, see §1.1 for more on their relation.

We next discuss consequences to some of the topics mentioned in the first paragraph.

Reducible fibers and the Hilbert–Siegel problem. For $f \in \mathbb{Q}[X]$ of degree $d \geq 2$, Hilbert's Irreducibility Theorem (HIT) asserts the existence of infinitely many $a \in \mathbb{Z}$ such that the fiber $f^{-1}(a) \subseteq \mathbb{C}$ is irreducible[2] over $\mathbb{Q}$, that is, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for any $\alpha \in f^{-1}(a)$. The Hilbert–Siegel problem [Fri86a, Pg. 2], cf. [Fri12, §7.1.3], asks to determine, up to a finite set, the set of integral exceptions for Hilbert's theorem:

$$\mathrm{Red}_f(\mathbb{Z}) := \{a \in \mathbb{Z} \mid f^{-1}(a) \text{ is reducible over } \mathbb{Q}\}.$$

The problem is closely related to the DLS problem: Indeed, as in the proof of HIT, the problem reduces to determining the values sets $g(\mathbb{Q})$ for which $g(\mathbb{Q}) \cap \mathrm{Red}_f(\mathbb{Z})$ is infinite, or equivalently to determining when is the curve $f(X) = g(Y)$ reducible for a *Siegel function* $g \in \mathbb{Q}(X)$, that is, a rational function whose value set $g(\mathbb{Q})$ contains infinitely many integers. For a polynomial $g \in \mathbb{Q}[X]$, this is equivalent to the reducibility of $f(X) - g(Y) \in \mathbb{Q}[X, Y]$, that is, to the DLS problem over $\mathbb{Q}$.

Clearly, $\mathrm{Red}_f(\mathbb{Z})$ contains every integer in $f(\mathbb{Q})$, and furthermore every integer in $f_1(\mathbb{Q})$ for a decomposition $f = f_1 \circ f_2$ in $\mathbb{Q}[X]$ with $\deg(f_1) > 1$. The problem is then to determine whether $\mathrm{Red}_f(\mathbb{Z}) \setminus \bigcup f_1(\mathbb{Q})$ is finite, where the union runs over all left composition factors f_1 of f with $\deg(f_1) > 1$. For indecomposable $f \in \mathbb{Q}[X]$ of degree > 5, the finiteness of $\mathrm{Red}_f(\mathbb{Z}) \setminus f(\mathbb{Q})$ was shown in [Fri86a, Thm. 1.2] by Fried, extending [Fri74]. Degree-5 examples $f \in \mathbb{Q}[X]$ for which this set is infinite were constructed by Dèbes–Fried [DF99]. Several variants of the problem have been since considered, see §1.2. However, the original Hilbert–Siegel problem has so far remained largely open for decomposable polynomials.

We give a uniform approach to the DLS and Hilbert–Siegel problems, yielding an almost-complete solution of the latter:

Theorem 1.2. *Let $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ be a nonlinear polynomial such that f does not factor through an indecomposable of degree 2 or 4. Then one of the following holds:*

(1) $\mathrm{Red}_f(\mathbb{Z})$ *is the union of* $\bigcup_{f_1} (f_1(\mathbb{Q}) \cap \mathbb{Z})$ *with a finite set, where* $f_1 \in \mathbb{Q}[X]$ *runs through all (nonlinear) indecomposable left factors* $f = f_1 \circ h$, $h \in \mathbb{Q}[X]$, *of* f.

(2) $f = f_1 \circ h$ *for a polynomial* $f_1 \in \mathbb{Q}[X]$ *of degree* 5 *belonging to the family* [DF99, (1.8)].

This is proved in §6.2 with an approach that mostly applies over general number fields, see Remark 6.11(1). The theorem substantially extends [KN24, Thm. 1.1], which applies only when all the indecomposable factors of f admit nonsolvable monodromy, cf. §1.1.

[2]Equivalently, $f^{-1}(a)$ is irreducible if it is irreducible as a scheme over $\mathrm{Spec}(\mathbb{Q}(a))$, or simply if $f(X) - a \in \mathbb{Q}(a)[X]$ is irreducible.

Stability in arithmetic dynamics. Stability of polynomials under iterates is a central topic in arithmetic dynamics [BIJ+19, §19]. A polynomial $f \in \mathbb{Q}[X]$ is called *stable* over $a \in \mathbb{Q}$, if the fibers over a of the n-fold iterates $f^{\circ n} := f \circ \cdots \circ f$ are irreducible for all $n \in \mathbb{N}$. In particular, when the fiber over a of $f^{\circ(n-1)}$ is irreducible whereas the one of $f^{\circ n}$ is not, $f^{\circ n}$ is called newly reducible over a; cf. [CCF+12] and [IJO+21] for investigations of this phenomenon. It is natural to ask whether $f^{\circ n}$ can be newly reducible over infinitely many $a \in \mathbb{Z}$. In other words, when is $\mathrm{Red}_{f^{\circ n}}(\mathbb{Z}) \setminus \mathrm{Red}_{f^{\circ n-1}}(\mathbb{Z})$ infinite? As a direct consequence of Theorem 1.2, we obtain:

Corollary 1.3. *Let $f \in \mathbb{Q}[X]$ be a polynomial of degree > 1 that does not factor through a polynomial of degree 2 or 4, and let $n \geq 2$. Then $\mathrm{Red}_{f^{\circ n}}(\mathbb{Z}) \setminus \mathrm{Red}_f(\mathbb{Z})$ is finite.*

Allowing quadratic factors, counterexamples with $n = 2$ exist, the simplest example being $f = X^2$, due to the factorization $X^4 + 4Y^4 = (X^2 - 2XY + 2Y^2)(X^2 + 2XY + 2Y^2)$.

Functional equations. For which polynomials $f, g \in \mathbb{C}[X]$ of degree ≥ 2, does the functional equation $f(X) = g(Y)$ have a solution in rational functions $X = X(z), Y = Y(z) \in \mathbb{C}(z)$? The question admits several variants and draws its motivation from number theory, functional equations, Nevanlinna theory, and dynamical systems, see §1.2.

Attempts to answer this question and its variants naturally divide into two cases according to the reducibility of $f(X) - g(Y) \in \mathbb{C}[X, Y]$. However, with the exception of the cases $g = cf$ for $c \in \mathbb{C}^\times$, and cases where $\deg(f) \gg \deg(g)$, see [Pak23b, Thm. 1.3],[Pak09, Thm. 1.2], and [Fri23], little appears in the literature on the reducible case of the question.

The combination of Theorem 1.1 with [AZ03, Thm. 1] gives the following simple resolution of the reducible case. First, we dispose of solutions that are not genuinely new. Clearly, if $f_1(X) = g_1(Y)$, for $f_1, g_1 \in \mathbb{C}[X]$, has a solution $X(z), Y(z) \in \mathbb{C}(z) \setminus \mathbb{C}$, then this is also a solution to $(w \circ f_1)(X) = (w \circ g_1)(Y)$ for $w \in \mathbb{C}[X]$. Such solutions satisfy $q(X(z), Y(z)) = 0$ for an irreducible factor $q(X, Y)$ of $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ (and not only of $f(X) - g(Y)$). Say an irreducible factor $q(X, Y)$ of $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is *right-reduced* if it is not a factor of $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ for any decomposition $f = w \circ f_1$, $g = w \circ g_1$ with $w, f_1, g_1 \in \mathbb{C}[X] \setminus \mathbb{C}$ and $\deg(w) > 1$. A solution is *reduced* if it annihilates a right-reduced factor. The goal is then to determine when reduced solutions exist.

Corollary 1.4. *Let $f, g \in \mathbb{C}[X] \setminus \mathbb{C}$ be polynomials. Suppose that $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is reducible and admits a reduced solution $f(X(z)) = g(Y(z))$ in $X(z), Y(z) \in \mathbb{C}(z) \setminus \mathbb{C}$. Then one of the following holds for some $\mu, \lambda_1, \lambda_2 \in \mathbb{C}[X]$ with $\deg(\mu) = \deg(\lambda_1) = \deg(\lambda_2) = 1$:*

(1) $f = \mu \circ T_n \circ \lambda_1$ and $g = \mu \circ (-T_m) \circ \lambda_2$ for $m, n \geq 3$ with $\gcd(m, n) > 2$;
(2) $f = \mu \circ P_i \circ \lambda_1$ and $g = \mu \circ P_i \circ \lambda_2$, for $i \in \{1, 2, 3\}$, where

$$P_1(X) = X^a(X-1)^b,\ \gcd(a,b) = 1,\ a + b \geq 4,$$

$$P_2(X) = X^3(X^2 + 5X + 40),\ \textit{and}$$

$$P_3(X) = X(X+1)^3(X+a+3)^3,\ \textit{where } a^2 + a + 2 = 0;$$

(3) $f = \mu \circ h_1 \circ \lambda_1$ *and* $g = \mu \circ h_2 \circ \lambda_2$*, where* $\{h_1, h_2\}$ *is one of the pairs of degree-*7 *or degree-*13 *polynomials appearing in §5.1 or §5.3, respectively, of* [CNC99].

The degree-7 and 13 polynomials in (3) are given in Remark 6.12. For these polynomials, and those in (1) and (2), we verify that $f(X) = g(Y)$ indeed has a reduced solution, yielding the converse statement.

Note that over number fields k, classifications of $f, g \in k[X]$ for which the curve $f(X) = g(Y)$ admits an irreducible component of genus ≤ 1 over $\mathbb{C}$ were announced, cf. [Zie12], in the irreducible case [DHH$^+$12] and the reducible case [CDH$^+$12], but have yet to appear in the literature. We suspect that Theorem 6.1, which applies over general fields, will be useful in developing a simple approach to our question and its variants over number fields k, and would therefore have broad applications to the above-mentioned subjects.

1.1. **On the proof.** A major reason why the DLS problem was previously deemed inaccessible for arbitrary decomposable polynomials is the complexity of monodromy groups of decomposable polynomials in comparison to indecomposable ones. This is especially true for polynomials f with solvable monodromy $\mathrm{Mon}(f)$, where the "largeness" of monodromy from [KNR24] does not apply, and no analogous constraints are known.

Instead, in the solvable case, we observe that the minimal reducibility of a pair $f, g \in \mathbb{C}[X]\backslash\mathbb{C}$ imposes heavy constraints on their monodromy. More specifically, writing $f = h \circ f_r$ and $h = h_2 \circ f_{r-1}$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$, the kernel K of the restriction map $\mathrm{Mon}(f) \to \mathrm{Mon}(h)$ naturally embeds into Γ^d, where $\Gamma := \mathrm{Mon}(f_r)$ and $d = \deg(h)$. If $\deg(f_r) > 2$, we show that minimal reducibility forces K to be diagonal, that is, its d projections to Γ are injective. When $\deg(f_r) = 2$, we show that K embeds in $C_2 \times C_2$. This is carried out in §4.

In contrast, we obtain lower bounds on the rank of K via the following two main ideas: Firstly, we consider the monodromy group $\Gamma_2 := \mathrm{Mon}(f_{r-1} \circ f_r)$ of a two-step right-factor of f. We use "largeness properties" for the kernel $K_2 = \ker(\Gamma_2 \to \mathrm{Mon}(f_{r-1}))$, developed in the companion paper [BKN26]. If for example $\mathrm{Mon}(f_r) \cong C_q$ for a prime q, these show that K_2 contains an abelian subgroup of rank at least $d_{r-1} - 1$, where $d_{r-1} = \deg(f_{r-1})$. We further apply these properties to obtain bounds on the image of the 2-step kernel $\ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h_2))$ in K_2 by exploiting the representations of $\mathrm{Mon}(f_{r-1})$ over $\mathbb{F}_q$ obtained from its action on corresponding subgroups of $K_2 \leq C_q^{d_{r-1}}$. Since the resulting bounds do not suffice when $\deg(f_{r-1}), \deg(f_r)$ are very small, we develop a 3-step analogue of such an argument. This is carried out in §3.

Secondly, we observe that the above lower bounds on 2-step (or 3-step) kernels also lead to meaningful lower bounds on the kernels K of arbitrarily long compositions, contradicting the aforementioned diagonality requirements except in a few very concrete low-degree cases. Length-3 right-factors of degrees 8 and 16 then require a separate argument (Proposition 5.4), which uses the database of transitive groups of these degrees, our only essential use of Magma [BCP97] through the above argument. This is the heart of the proof of the solvable case of the DLS problem, carried out in §5. We expect such largeness arguments would be useful far beyond the problems discussed here. Based on [KN24], we give a much simpler

argument for polynomials of nonsolvable monodromy in §6.1, improving [KN24, §4]. Its combination with the solvable case yields the main Theorem 6.1.

Most considerations also apply to the Hilbert–Siegel problem and are given along with the above. This problem amounts to determining the minimally reducible pairs $f \in \mathbb{Q}[X]$ and $g \in \mathbb{Q}(X)$, where g is a Siegel function (and not merely a polynomial). Our strategy breaks when f has factors of degree 2 or 4 (of solvable monodromy), see Remark 6.11. Further ideas are required to classify such examples. Finally, we derive the consequence to functional equations in §6.3.

The CFSG is used in the proof of Theorem 6.1 only in the very last step to assert that indecomposable $f_1, g_1 \in \mathbb{C}[X] \setminus \mathbb{C}$ of nonsolvable monodromy with the same Galois closure, must be one of the aforementioned pairs of degrees $7, 11, 13, 15, 21$ or 31, see Remark 6.7.

1.2. **Related work.** Several variants of the original Hilbert–Siegel problem have been considered. Firstly, it is natural to consider degree-d maps $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ from an arbitrary (smooth projective) curve X of positive genus. In the general case, where $\mathrm{Mon}_{\mathbb{Q}}(f) = S_d$, the set of reducible fibers $\mathrm{Red}_f(\mathbb{Z})$ is in fact finite, see Müller [Mü99], and [Mü02] for other cases. For indecomposable $f \in \mathbb{Q}[X]$ with $\deg(f) > 20$, the analogous set $\mathrm{Red}_f(\mathbb{Q})$, of rational values with reducible fibers, is the union of $f(\mathbb{Q})$ and a finite set, by the combination of theorems of Müller [Mü95] and Guralnick–Shareshian [GS07], see [KN24, Thm. 5.4]. Similar results were shown for indecomposable rational functions $f \in \mathbb{Q}(X)$ of sufficiently large degree [Mon24, Thm. 1.2], using [NZ24]. The question also recently arose in the context of algebraic points of fixed degree d in fibers of maps $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ over rational points, as considered by Derickx–Rawson [DR25]. Over fields k of positive characteristic, except for the classification of $f, g \in k[X]$ for which $f(X) - g(Y)$ has a quadratic factor [KMS07], little appears in the literature. The above variants of DLS and Hilbert–Siegel, involving more general rational maps, remain wide-open.

As for the DLS problem [DLS61], much of the motivation for studying the functional equation $f(X(z)) = g(Y(z))$ comes from the question: for which $f, g \in \mathbb{Q}[X]$ is the set $f(\mathbb{Q}) \cap g(\mathbb{Q})$ infinite? The existence of a solution $X = X(z), Y = Y(z)$ for $f(X) = g(Y)$ is equivalent to the existence of an irreducible component of genus 0 in a curve[3] $\mathcal{C}$ birational to $f(X) = g(Y)$, whereas if $f(\mathbb{Q}) \cap g(\mathbb{Q})$ is infinite, then $\mathcal{C}$ admits an irreducible component of genus ≤ 1 by Faltings' theorem. The pairs f, g for which $f(\mathbb{Z}) \cap g(\mathbb{Z})$ is infinite were determined by Bilu–Tichy [BT00]; For these, Siegel's theorem implies that $\mathcal{C}$ has an irreducible component of genus 0, and further constraints on the number of preimages of infinity. Moreover, the solvability of the functional equation $f(X) = g(Y)$ in meromorphic (resp. entire) functions $X = X(z), Y = Y(z)$ is equivalent to $\mathcal{C}$ admitting an irreducible component of genus ≤ 1 by Picard's theorem (resp. reduces to our question [Pak10] with rational $X(z), Y(z)$). Variants of the equation also arise in studying intersections of orbits in arithmetic dynamics, see [BIJ+19, §7]. Further motivation, coming from other subjects, is described in [DZ22, Pg. 2]. See also [AZ01, Pak18, HT23] for further details on this functional equation and its variants.

[3]Equivalently, there exists a (parametrization) map $\mathbb{P}^1_{\mathbb{C}} \to \mathcal{C}$ given by $z \mapsto (X(z), Y(z))$ on affine charts.

The DLS problem is also closely related to Davenport's problem concerning polynomials $f, g \in \mathbb{Q}[X]$ with the same image $f(\mathbb{Z}/p) = g(\mathbb{Z}/p)$ for all but finitely many primes p. More specifically, this condition implies, $f(X) - g(Y) \in \mathbb{Q}[X, Y]$ has to be reducible [MV96, §7].

Acknowledgments. The first and third authors were supported by the Israel Science Foundation, grant no. 353/21. The first author is also grateful for the support of a Technion fellowship, of an Open University of Israel post-doctoral fellowship. He also acknowledges the support of the CDP C2EMPI, as well as the French State under the France-2030 programme, the University of Lille, the Initiative of Excellence of the University of Lille, the European Metropolis of Lille for their funding and support of the R-CDP-24-004-C2EMPI project. The second author was supported by the National Research Foundation of Korea (NRF Basic Research Grant RS-2023-00239917).

2. Basic setup and Preliminaries

2.1. **Basic setup.** Throughout the paper, k is a field of characteristic 0 and $\overline{k}$ its algebraic closure. A *map* $f : \mathcal{X} \to \mathcal{Y}$ *over* k is a finite (dominant and generically unramified) morphism of (smooth irreducible projective) varieties defined over k. This induces a field extension $k(\mathcal{X})/k(\mathcal{Y})$ via the pullback $f^* : k(\mathcal{Y}) \to k(\mathcal{X})$, given by $h \mapsto h \circ f$. The *degree* $\deg(f)$ of f is then defined as $[k(\mathcal{X}) : k(\mathcal{Y})]$. We say f is *indecomposable* if it is of degree > 1 and is not a composition of two maps of degree > 1. Say that the function field $\overline{k}(\mathcal{X})$ has *genus* g if the curve[4] $\mathcal{X}$ has genus g.

A rational function $f \in k(X) \setminus k$, then induces an $k(x)/k(t)$ of rational functions fields such that $f(x) = t$. The degree of f is then $\max\{\deg(f_1), \deg(f_2)\}$, where $f = f_1/f_2$ for coprime $f_1, f_2 \in k[X]$. We say $f, g \in k(X) \setminus k$ are *linearly related over* k if there exist $\mu, \nu \in k(X)$ of degree 1 (also called *linear fractionals*) such that $f = \mu \circ g \circ \nu$. We shall denote k-rational places of $k(t)$ by $t \mapsto a$ for $a \in \mathbb{P}^1(k) = k \cup \{\infty\}$.

Permutation groups. All group actions are left actions. Recall that a permutation group $G \leq S_n$ is *primitive* if it preserves no nontrivial block system. It is *affine* if it has an elementary-abelian regular normal subgroup; equivalently, G embeds as $V \leq G \leq \mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ for a finite vector space V. For $G \leq S_n$, $H \leq S_m$, the wreath product $H \wr G$ is defined as $H^n \rtimes G$, where G acts on H^n by permuting the n copies. It is naturally an imprimitive permutation group of degree mn. It also has a natural primitive action of degree m^n, the *product type* action. This is the action on $\{1, \dots, m\}^n$ in which G acts by permuting the coordinates and H^n acts coordinatewise. We denote by $G = A.H$ a group extension of H with kernel A (which is not necessarily split). If A is abelian, we will regard it as an H-module via the action of H by conjugation in G. Also recall that the socle $\mathrm{soc}(G)$ is the subgroup of G generated by minimal normal subgroups of G.

[4]Recall that smooth projective curves with isomorphic function fields are isomorphic [Har77, II.6.8].

2.2. **Monodromy groups.** Let $f : \mathcal{X} \to \mathcal{Y}$ be a map of degree d defined over k. The *monodromy group* $\mathrm{Mon}_k(f) = \mathrm{Mon}(f)$ of f is $\mathrm{Gal}(\Omega/k(\mathcal{Y}))$, where Ω is the Galois closure of the extension $k(\mathcal{X})/k(\mathcal{Y})$. It is a permutation group of degree d, via the action on the generic fiber of f, or equivalently via the action on the roots of a minimal polynomial for $k(\mathcal{X})$ over $k(\mathcal{Y})$. If $f = f_1/f_2$ is a rational map for coprime $f_1, f_2 \in k[X]$, then $\mathrm{Mon}_k(f)$ is just the Galois group of $f_1(X) - tf_2(X) \in k(t)[X]$. We refer to a root x of the last polynomial, for brevity as a root of $f(X) - t$ in an extension of $k(t)$. Recall that f is indecomposabe if and only if $\mathrm{Mon}_k(f)$ is primitive.

When $\mathcal{X}$ and $\mathcal{Y}$ are geometrically irreducible, letting $f_{\overline{k}} : \mathcal{X} \otimes_k \overline{k} \to \mathcal{Y} \otimes_k \overline{k}$ be the map induced by f over $\overline{k}$, the *geometric monodromy group* $\mathrm{Mon}_{\overline{k}}(f_{\overline{k}}) = \mathrm{Gal}(\Omega\overline{k}/\overline{k}(\mathcal{X}))$ is isomorphic to the image of the action of the étale fundamental group $\pi_1^{\text{ét}}(\mathcal{Y} \setminus \mathrm{Br}(f))$ on the fiber $f^{-1}(y_0)$ of a base point $y_0 \in \mathcal{Y}(\overline{k})$ over which f is unramified, that is, the classical definition of monodromy. Here, $\mathrm{Br}(f) \subset \mathcal{Y}(\overline{k})$ denotes the branch locus of f.

Polynomial monodromy. A polynomial $f \in k[X] \setminus k$ with cyclic geometric monodromy group is well known to be linearly related to X^n over $\overline{k}$. Similarly, every polynomial $f \in k[X] \setminus k$ with dihedral geometric monodromy group is linearly related over $\overline{k}$ to the Chebyshev polynomial of degree $n = \deg(f)$ [ZM08, Lemma 3.3], that is, the unique degree-n polynomial T_n for which $T_n(X + 1/X) = X^n + 1/X^n$. We shall also let $D_{n,\alpha}$ denote the n-th degree Dickson polynomial with parameter α, defined via $D_{n,\alpha}(x + \frac{\alpha}{X}) = X^n + \left(\frac{\alpha}{X}\right)^n$.[5] Note that in the above examples of f, the group $\mathrm{Mon}_k(f)$ contains a regular cyclic normal subgroup C_n of order n, and hence $\mathrm{Mon}_k(f)$ is isomorphic (as a permutation group) to a subgroup of $\mathrm{AGL}_1(n) := \mathbb{Z}/n \rtimes (\mathbb{Z}/n)^\times$, that is, of the holomorph of C_n.

Monodromy groups of indecomposable polynomials were completely classified by Müller [Mü95]. While this result uses the CFSG, the following important partial result does not, cf., e.g., [KN24, Theorem 2.1].

Proposition 2.1. *Let $f \in k[X]$ be an indecomposable polynomial. If $\mathrm{Mon}_k(f)$ is solvable, then either f is linearly related over $\overline{k}$ to X^p or T_p for a prime p, or $\mathrm{Mon}_k(f) = S_4$. If $\mathrm{Mon}_k(f)$ is nonsolvable, then it is an almost-simple group with primitive socle.*

In the solvable cases of Proposition 2.1, $\mathrm{Mon}_k(f)$ is affine, and moreover it embeds into $\mathrm{AGL}_1(p)$ or $\mathrm{Mon}_k(f) = S_4 \cong \mathrm{AGL}_2(2)$, respectively. Another characterizing property of these groups is that they contain a regular elementary abelian normal subgroup:

Lemma 2.2. *Let $d \geq 2$, p a prime with $(p, d) \neq (2, 2)$, and let $G \leq S_{p^d}$ be a transitive group containing a cyclic transitive subgroup. Then G cannot contain a p-elementary-abelian regular normal subgroup.*

Proof. Assume on the contrary that $N \cong C_p^d$ is an elementary-abelian regular normal subgroup of G. Then $G \cong N \rtimes G_1$, where $G_1 \leq G$ is a point stabilizer, and moreover G embeds as a permutation group into the affine linear group $\mathrm{AGL}_d(p)$. This group does not have a cyclic transitive subgroup unless $d = 1$ or $(p, d) = (2, 2)$ [Mü13, Lemma 3.6]. □

[5]Note that $D_{n,0} = X^n$, whereas for $\alpha \neq 0$, the polynomial $D_{n,\alpha}$ is linearly related to T_n over $k(\sqrt{\alpha})$.

The following group-theoretic version of the well-known Capelli's lemma, see e.g. [Ost25, §2.1], characterizes intransitive subgroups of $\mathrm{AGL}_1(n)$:

Lemma 2.3. *Let $n \geq 1$ be an integer and $U \leq \mathrm{AGL}_1(n)$ be an intransitive subgroup. Then:*
(1) If $n = p$ is prime, $U \leq \mathrm{AGL}_1(p)$ fixes a point.
(2) If n is a composite number, then there exists a divisor $d|n$ which is either prime or equal to 4 such that U projects to an intransitive subgroup of $\mathrm{AGL}_1(d)$.

Siegel functions. Let k be a number field with ring of integers O_k and $\varphi : \mathcal{X} \to \mathbb{P}^1_k$ a map defined over k. By a famous theorem of Siegel, if $\varphi(\mathcal{X}(k)) \cap O_k$ is infinite, then firstly, $\mathcal{X}$ is birational to $\mathbb{P}^1_k$, i.e. φ is given by a rational function $f \in k(X)$, and furthermore $|\varphi^{-1}(\infty)| \leq 2$, see [Mü02, Prop. 3.2]. When $k = \mathbb{Q}$, it is furthermore necessary for the preimages of ∞ to be algebraically conjugate. Motivated by this, we call a rational function $f \in k(X)$ over an arbitrary field k of characteristic 0 a *Siegel function* if $|f^{-1}(\infty)| \leq 2$, and for $k = \mathbb{Q}$, we call f a *Siegel function over* $\mathbb{Q}$ if additionally either $|f^{-1}(\infty)| = 1$ or the two preimages of ∞ are algebraic conjugates[6].

As in the case of indecomposable polynomials, a full classification of monodromy groups of indecomposable Siegel functions was obtained by Müller [Mü13], invoking the classification of finite simple groups. As noted in [KN24, Theorem 2.2], the following useful partial result can be obtained relying on the classification only in a "mild" way, namely via certain bounds on the outer automorphism groups of simple groups.

Proposition 2.4. *Let $f \in k(X)$ be an indecomposable Siegel function. Then $\mathrm{Mon}_k(f)$ is either affine, or almost-simple, or contained in $(\mathrm{Aut}(S) \times \mathrm{Aut}(S)) \rtimes C_2$ for a simple group S. In all cases, $\mathrm{Mon}_k(f)$ contains a unique minimal normal subgroup.*

We shall also use the following elementary property of composite Siegel functions.

Lemma 2.5. *Let $g, h \in k(X) \setminus k$ be such that $f = g \circ h$ is a Siegel function. Then either $|g^{-1}(\infty)| = 1$ or $\mathrm{Mon}_{\overline{k}}(h)$ is cyclic.*

Proof. Assume that $g^{-1}(\infty) = \{a, b\}$ consists of two elements. Since $|f^{-1}(\infty)| \leq 2$, this enforces $|h^{-1}(a)| = |h^{-1}(b)| = 1$, i.e., the rational function h is totally ramified over these two points. Thus, the Riemann–Hurwitz formula shows that h has no further branch points. By composing h with linear fractionals, we may obtain a rational map totally ramified over $0, \infty$ with preimages $0, \infty$, resp., forcing it to be cX^n, where $n = \deg(h)$ and $c \in \overline{k}[X]$. Thus, h is linearly related over $\overline{k}$ to X^n and $\mathrm{Mon}_{\overline{k}}(h)$ is cyclic. □

2.3. **Composing maps.** Recall that the monodromy group $\mathrm{Mon}_k(f)$ of a composition $f = g \circ h$ of two maps $g : \mathcal{Y} \to \mathcal{Z}, h : \mathcal{X} \to \mathcal{Y}$ is a subgroup of $A \wr B := A^d \rtimes B$, where $A := \mathrm{Mon}_k(h)$ and $B := \mathrm{Mon}_k(g)$. In particular, B is a natural quotient of $\mathrm{Mon}_k(f)$. Letting B act on the set of roots $\mathcal{B}$ of a minimal polynomial of $k(\mathcal{Y})/k(\mathcal{Z})$, the *stabilizer* of a block $b \in \mathcal{B}$ is the subgroup of $\mathrm{Mon}_k(f)$ fixing b under its action through B. The *block kernel* is the kernel of the action of $\mathrm{Mon}_k(f)$ on $\mathcal{B}$. Letting $\Omega' \subseteq \Omega$ be the Galois

[6]Note that slightly different notions exist in the literature. However, importantly, the defining property used here is implied by the diophantine property of Siegel functions used in §1.

closures of g^*, and f^*, resp., the block kernel coincides with $\mathrm{Gal}(\Omega/\Omega')$, while the block stabilizer coincides with $\mathrm{Gal}(\Omega/F(b))$, where $F = k(\mathcal{Z})$ and $F(b)$ is the conjugate of $k(\mathcal{Y})$ corresponding to b.

The block kernel for polynomials maps. We shall often use the following observation:

Lemma 2.6. *Suppose $f = g \circ h \in k[X] \setminus k$. Then the block kernel $K = \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(g))$ contains an element of order $\deg(h)$.*

We deduce the lemma from the following:

Lemma 2.7. *Let L/K be a degree-n extension totally ramified over a place P of perfect residue, with Galois closure Ω, and Galois group $G := \mathrm{Gal}(\Omega/K)$. Let M/K be a Galois extension in which P is unramified. Then:*

(1) $N = \mathrm{Gal}(\Omega M/M)$ is a normal subgroup of G containing a cyclic transitive subgroup, upon identifying it with its image under restriction. In particular, $[LM : M] = [L : K]$.
(2) For $n = 4$ and $G = S_4$, one has $N = S_4$ as well.

This is often applied together with the following consequences of Abhyankar's lemma:

Remark 2.8. Let L_1/K and L_2/K be finite extensions of degrees m, n, resp. Let P be a place of K with a perfect residue field. Abhyankar's lemma asserts that the ramification index of every place Q of L_1L_2 over K is $\mathrm{lcm}(e_1, e_2)$, where e_i is the ramification index of $Q \cap L_i$ in L_i/K, see e.g. [DZ22, Cor. 5.2]. It follows that:

(1) Assume $n = m$ and let Ω be the Galois closure of L_1L_2/K. Then every place Q of Ω above P has ramification index n in Ω/K, but is unramified in Ω/L_1. Indeed, the first statement follows by applying Abhyankar's lemma repeatedly to conjugates of L_1 and L_2 in Ω, and the second one from the multiplicativity of ramification indices.

(2) Assume that P is totally ramified in L_1/K but unramified in L_2/K. Then:
  a) L_1/K and L_2/K are linearly disjoint.
  b) Any place Q of L_2 lying above P is totally ramified in L_1L_2/L_2.

Indeed: a) Otherwise, by the multiplicativity of ramifications indices, the ramification index of a place R of L_1L_2 over P would be at most $[L_1L_2 : L_2] < m$, contradicting the fact that it must be divisible by the ramification index of $R \cap L_1$ over P, which is $[L_1 : K] = m$. For b), let R be a place of L_1L_2 lying above Q. By Abhyankar's lemma, the ramification index of R over P is m. Since P is unramified in L_2/K, the ramification index of R over Q is also m. Since $[L_1L_2 : L_2] \leq m$, it follows that $[L_1L_2 : L_2] = m$ and that Q is totally ramified in L_1L_2/L_2.

(3) Let P be a place of K that is ramified in L_1/K. If every place of L_2 above P is unramified in L_1L_2/L_2, then P is ramified in L_2/K. Indeed, otherwise, by the multiplicativity of ramification indices, P would then be unramified in L_1L_2/K, a contradiction.

Remark 2.9. If L_1/K and L_2/K are linearly disjoint extensions, and Ω is the Galois closure of L_1/K. Then the Galois closure of L_1L_2/L_2 is ΩL_2, e.g. by [KN24, Lemma 2.12 and Remark 2.13]. We shall therefore often identify $\mathrm{Gal}(\Omega L_2/L_2)$ with its image in $\mathrm{Gal}(\Omega/K)$ under the restriction map.

Proof of Lemma 2.7. 1) Since L/K is totally ramified at P while P is unramified in M/K, the two extensions are linearly disjoint by Remark 2.8(2). Thus, Remark 2.9 implies that the Galois closure of LM/M is the compositum ΩM, and that we may identify $N := \mathrm{Gal}(\Omega M/M)$ with its image in G. Moreover, since M/K is Galois, N is normal in G.

Since M/K is unramified over P, and L/K is totally ramified over P, the extension LM/M is also totally ramified (of the same ramification index n) over places of M lying over P by Remark 2.8(2). Thus, the inertia groups over such places are of order n. Consequently, N contains a cyclic transitive subgroup.

2) Since $N \lhd S_4$ and contains a 4-cycle by 1), it follows that $N = S_4$. □

Proof of Lemma 2.6. Let x be a root of $f(X) = t$, let $w = h(x)$, let $\Omega/k(t)$ be the Galois closure of $k(x)/k(t)$, and Ω^K the fixed field of K. Since ∞ is unramified in $\Omega^K/k(w)$ by Remark 2.8(1), and is totally ramified in $k(x)/k(t)$, Lemma 2.7 gives the claim. □

Ritt moves. Recall that Ritt's theorems relate *complete decompositions* of f, that is, decompositions $f = f_1 \circ \cdots \circ f_r$ for indecomposable polynomials $f_1, \ldots, f_r \in k[X]$ [ZM08, Theorem 2.1.]. Two complete decompositions $f = f_1 \circ \cdots \circ f_r$ and $f = \tilde{f}_1 \circ \cdots \circ \tilde{f}_r$ are related by a *Ritt move* if $f_j = \tilde{f}_j$ for $j \notin \{i, i+1\}$, while $f_i \circ f_{i+1} = \tilde{f}_i \circ \tilde{f}_{i+1}$ for some $1 \le i < r$, and there is no linear $\mu \in k[X]$ such that $f_i = \tilde{f}_i \circ \mu$ and $f_{i+1} = \mu^{-1} \circ \tilde{f}_{i+1}$. Given a pair of complete decompositions for a polynomial, Ritt's first theorem then asserts that it is possible to pass from one to another by a sequence of consecutive Ritt moves. Moreover, a complete decomposition $f = f_1 \circ \cdots \circ f_r$, $f_i \in \overline{k}[X]$, over $\overline{k}$ has to be defined over k by Fried–MacRae [FM69], that is, there exist linear $\ell_1, \ldots, \ell_{r-1} \in \overline{k}[X]$ such that $f_1 \circ \ell_1, \ell_{r-1}^{-1} \circ f_r, \ell_{i-1}^{-1} \circ f_i \circ \ell_i \in k[X]$ for all $2 \le i \le r-1$.

We shall mainly use the following consequence of Ritt's theorems, which follows from the above since the degrees in a Ritt move are coprime [ZM08, Corollary 2.11]. Say that $v \in k[X]$ is a *right-unique* factor if, for every complete decomposition $f = f_1 \circ \cdots \circ f_r$, $f_i \in k[X]$, there exists some i and a linear $\mu \in k[X]$ such that $\mu \circ v = f_{i+1} \circ \cdots \circ f_r$. In this case, we also call a decomposition $f = u \circ v$ right-unique. The decomposition is further called *strongly-unique* if furthermore it does not have a right-factor[7] that is linearly related to X^{p^2} or T_{p^2} over $\overline{k}$.

Corollary 2.10. *Let $f = h \circ f_r \in k[X] \setminus k$ be a decomposition with $h, f_r \in k[X]$ and $f_r \in k[X]$ indecomposable. If f_r is not a right-unique factor, then there exist indecomposable $u, u', v' \in k[X]$ for which $u \circ f_r = v' \circ u'$ is a right-factor of f that is a Ritt move. Moreover, $\deg(u) = \deg(u')$ and $\deg(f_r) = \deg(v')$ are coprime.*

We say that $f \in k[X] \setminus k$ is *simply branched* if each of its finite branch points has a unique ramified f-preimage and this preimage has ramification index 2. This is the type of ramification occuring generically.

Remark 2.11. In Appendix A, we shall also use Ritt's second theorem [ZM08, Theorem 2.17] directly: If $a \circ b = c \circ d$ for $a, b, c, d \in \mathbb{C}[X]$ of degree > 1 with $\gcd(\deg(a), \deg(b)) =$

[7] In this terminology $X^{p^2} = X^p \circ X^p$ and $T_{p^2} = T_p \circ T_p$ are right-unique but not strongly-unique.

$\gcd(\deg(c), \deg(d)) = 1$, then (up to switching a, b and c, d), there exist $\ell_j \in \mathbb{C}[X]$ of degree 1 such that $(\ell_1 \circ a \circ \ell_2^{-1}, \ell_2 \circ b \circ \ell_3^{-1}, \ell_1 \circ c \circ \ell_4^{-1}, \ell_4 \circ d \circ \ell_3^{-1})$ is either (1) (T_m, T_n, T_n, T_m) or (2) $(X^n, X^s h(X^n), X^s h(X)^n, X^n)$, for some coprime $m, n > 1$, some $s \geq 1$ coprime to n, and $h \in \mathbb{C}[X] \setminus X\mathbb{C}[X]$. In particular, simply-branched polynomials of degree ≥ 4 do not occur as left factors of Ritt moves. It also follows immediately that two left-factors involved in a Ritt step must share a finite branch point. In (1) and (2), these are -2 and 0, resp.

We shall also use the following part of Ritt's first theorem which applies more generally to maps (or their corresponding extensions) with a totally ramified point.

Lemma 2.12. *Let L/K be a finite extension with Galois closure M/K, and P be a place of K that is totally ramified in L/K with a perfect residue field. Let I be the inertia group at a place of M above P in $G = \mathrm{Gal}(M/K)$, and let $H = \mathrm{Gal}(M/L)$. Then $G = HI$ and $H \cap I = 1$. Moreover, for any intermediate subgroup $H \leq T \leq G$, we have $T = H(T \cap I)$.*

Proof. The extension M/L is unramified at any place of L over P by Remark 2.8(1), which implies that $H \cap I = 1$. Since P is totally ramified in L/K, it follows that $G = HI$. The last assertion then follows directly, see [ZM08, Lemma 2.5]. □

2.4. **Reducibility.** Given $f, g \in k(X) \setminus k$, the curve $f(X) = g(Y)$ is birational to the fiber product $\mathbb{P}^1 \#_{f,g} \mathbb{P}^1$ of $f : \mathbb{P}^1 \to \mathbb{P}^1$ and $g : \mathbb{P}^1 \to \mathbb{P}^1$. Moreover, this fiber product is irreducible over k if and only if the root fields $k(x)$ and $k(y)$ of $f(X) - t$ and $g(Y) - t$ over $k(t)$, respectively, are linearly disjoint over $k(t)$. We shall repeatedly use the group-theoretic translation of this condition via the Galois coorespondence: letting Ω denote the Galois closure of $k(x, y)/k(t)$, and setting $G = \mathrm{Gal}(\Omega/k(t)), H = \mathrm{Gal}(\Omega/k(x)), H' = \mathrm{Gal}(\Omega/k(y))$, the linear disjointness of $k(x)/k(t)$ and $k(y)/k(t)$ is equivalent to the transitivity of H on G/H', that is, to $H \cdot H' = G$.

The following well-known lemma shows that minimally reducible pairs have a common Galois closure. As for polynomials, say that two extensions M/K and L/K, which are not linearly disjoint, form a *minimally reducible pair* if M_1/K and L_1/K are linearly disjoint for any $K \subset L_1 \subset L$ and $K \subset M_1 \subset M$ such that $L \neq L_1$ or $M \neq M_1$.

Lemma 2.13. *Let L/K and M/K be finite separable extensions forming a minimally reducible pair. Then their Galois closures coincide.*

Remark 2.14. Letting Ω/K be the Galois closure of L/K, since L/K and M/K are not linearly disjoint, so are L/K and $M \cap \Omega/K$, see e.g.[8] [KN24, Lemma 2.11].

Proof of Lemma 2.13. Suppose on the contrary M is not contained in the Galois closure Ω of L/K. Since L and M are not linearly disjoint over K, so are L and $M \cap \Omega$ by Remark 2.14. Since $M_1 := M \cap \Omega$ is properly contained in M, the fact that M_1/K and L/K are not linearly disjoint contradicts the minimal reducibility of M/K and L/K. □

Corollary 2.15. *If $f, g \in k[X] \setminus k$ is a minimally reducible pair, then $\deg(f) = \deg(g)$ and the branch loci of f and g coincide.*

[8]The proof is given for curves. Replacing these by their function fields, it clearly applies to general fields.

Proof. Letting $k(x), k(y)$ be root fields of $f(X)-t, g(X)-t$, resp., their Galois closures Ω coincide by Lemma 2.13. By Remark 2.8(1), the ramification index $\deg(f)$ (resp., $\deg(g)$) of ∞ in $k(x)/k(t)$ (resp., $k(y)/k(t)$) coincides with that in $\Omega/k(t)$. Thus $\deg(f)=\deg(g)$. Moreover, the remark implies the branch loci of $k(x)/k(t)$, $k(y)/k(t)$ and $\Omega/k(t)$ coincide. □

In particular, one deduces the examples appearing in Theorems 1.1 and 6.1:

Example 2.16. Let $f,g:\mathbb{P}^1_k\to\mathbb{P}^1_k$ be polynomial maps having the same Galois closure $\tilde{X}$, which has genus 0 and monodromy group $G=D_4$. Then one of the following holds:
(1) $\mathrm{Mon}^{-}_{\overline{k}}(f)=D_4$. In this case, $\{\mu\circ f\circ\eta_1,\mu\circ g\circ\eta_2\}=\{D_{4,\alpha},-\frac{1}{4}D_{4,2\alpha}\}$ for some $\mu,\eta_1,\eta_2\in k[X]$ of degree 1 and $\alpha\in k^\times$, with $D_{4,\alpha}=X^4-4\alpha X^2+2\alpha^2$ the degree-4 Dickson polynomial with parameter α. Indeed, it is well known that f must be of the given shape, see, e.g., [GMS02, Theorem 5.2]. For g, one notes that:

$$D_{4,\alpha}(X)+\frac{1}{4}D_{4,2\alpha}(Y)=\left(X^2-XY+\frac{1}{2}Y^2-2\alpha\right)\left(X^2+XY+\frac{1}{2}Y^2-2\alpha\right), \tag{2.1}$$

so that $D_{4,\alpha}$ and $-(1/4)D_{4,2\alpha}$ is a minimally reducible pair. Letting s be a reflection and r a rotation in D_4, note that $\langle rs\rangle$ is the only maximal subgroup of D_4 which is intransitive on $D_4/\langle s\rangle$ and does not contain a conjugate of $\langle s\rangle$. It follows that the unique minimally reducible pair of degree-4 maps with Galois closure $\tilde{X}$ is $\tilde{X}/\langle s\rangle\to\tilde{X}/G$ and $\tilde{X}/\langle rs\rangle\to\tilde{X}/G$, up to automorphisms of $\tilde{X}/G,\tilde{X}/\langle rs\rangle,\tilde{X}/\langle s\rangle\cong\mathbb{P}^1_k$ given by degree-1 polynomials. Thus, up to swapping f,g, they are related to $D_{4,\alpha}$, $-(1/4)D_{4,2\alpha}$, resp., by linear $\mu,\eta,\eta'\in k[X]$ as claimed.
(2) $\mathrm{Mon}^{-}_{\overline{k}}(f)=C_4$. In this case, $\{\mu\circ f\circ\eta_1,\mu\circ g\circ\eta_2\}=\{X^4,-\frac{1}{4}X^4\}$ for some $\mu,\eta_1,\eta_2\in k[X]$ of degree 1. Indeed, the Riemann-Hurwitz formula shows instantly that f has exactly one finite branch point P, whose ramification index equals 4. Since k-conjugates of branch points of $f\in k[X]$ are also branch points, this shows that P is k-rational. Thus, f is linearly related to X^4 over k. The pair of projections $\tilde{X}\to\tilde{X}/\langle s\rangle,\tilde{X}\to\tilde{X}/\langle rs\rangle$ is again the unique minimally reducible pair of degree 4 polynomial maps with Galois closure $\tilde{X}$, up to composing with automorphisms of $\tilde{X}/G,\tilde{X}/\langle rs\rangle,\tilde{X}/\langle s\rangle\cong\mathbb{P}^1_k$ given by degree-1 polynomials. Since $X^4,-\frac{1}{4}X^4$ is a minimally reducible pair of monodromy D_4 and geometric monodromy C_4, up to swapping f,g, it follows as in (1) that these are related to $X^4,-\frac{1}{4}X^4$ by linear polynomails as claimed. Moreover, in this case one necessarily has $\sqrt{-1}\notin k$, since otherwise the polynomial X^4-t would have Galois group C_4, rather than D_4, over $k(t)$. Note that $X^4=D_{4,0}$, whence this case may be in fact be seen as a degeneration of the family in Case (1).

The following proposition restricts right factors of minimally reducible pairs.

Proposition 2.17. *Let $f,g\in k(X)\setminus k$ be a minimally reducible pair with decompositions $f=f_1\circ f_2$, $g=g_1\circ g_2$ such that $n=\deg(f_2)\geq 2$, and $m=\deg(g_2)\geq 2$.*
(1) If $n\neq 4$ is composite, then f_2 is not linearly related over $\overline{k}$ to X^n,T_n.
(2) If $n=4$, then $\mathrm{Mon}_k(f_2)$ is noncyclic.

(3) *The integers m, n have a nontrivial common divisor.*
(4) *When $f, g \in k[X]$ are polynomials and $f_2, g_2 \in k[X]$ are indecomposable, then furthermore $m = n$ or $\{m, n\} = \{2, 4\}$. In particular, f_2 is right-unique.*
(5) *If $f \in k[X]$ is a polynomial, $g \in k(X)$ is a Siegel function, and f_2, g_2 are indecomposable, then f_2 is right-unique.*

Proof. Let x, y be roots of $f(X) - t, g(X) - t$, respectively. Let Ω be the common Galois closure of $k(x)/k(t)$ and $k(y)/k(t)$ given by Lemma 2.13. Set $u = f_2(x)$ and $v = g_2(y)$. Let $\tilde{\Omega}$ be the Galois closure of $k(x)/k(u)$. Since $k(y, u)/k(u)$ and $k(x)/k(u)$ are not linearly disjoint, $L = k(y, u) \cap \tilde{\Omega}$ is not linearly disjoint from $k(x)$ over $k(u)$ by Remark 2.14.
(1) Suppose on the contrary that f_2 is linearly related over $\overline{k}$ to T_n or X^n, so that $\mathrm{Mon}_k(f_2) \leq \mathrm{AGL}_1(n)$. Since $n \neq 4$ is composite, Lemma 2.3 and the Galois correspondence imply there exists an intermediate field $k(u) \subsetneq k(u') \subsetneq k(x)$ such that $L/k(u)$ and hence $k(y, u)/k(u)$ are not linearly disjoint from $k(u')/k(u)$, contradicting the minimal reducibility of f and g.
(2) Assume on the contrary $\mathrm{Mon}_k(f_2) = C_4$. Then $\tilde{\Omega} = k(x)$ and $L \subseteq k(x)$. Since L and $k(x)$ are not linearly disjoint over $k(u)$, the extension $L/k(u)$ is nontrivial, and hence contains the quadratic subextension $k(u')/k(u)$ of $k(x)/k(u)$, contradicting the minimal reducibility of f and g.
(3) Since f, g are minimally reducible, $k(x)$ and $k(v)$ are linearly disjoint over $k(t)$, so that $[k(x, v) : k(u, v)] = [k(x) : k(u)] = n$ and similarly $[k(u, y) : k(u, v)] = [k(y) : k(v)] = m$. If m and n are coprime, the extensions $k(x, v)/k(u, v)$ and $k(u, y)/k(u, v)$ are linearly disjoint, contradicting the minimal reducibility of the pair f, g.
(4) We first claim that $\mathrm{soc}(\mathrm{Mon}_k(f_2))$ and $\mathrm{soc}(\mathrm{Mon}_k(g_2))$ coincide. Denote by Ω_u and Ω_v the Galois closure of $k(u)/k(t)$ and of $k(v)/k(t)$, respectively. Then the ramification index of $t \mapsto \infty$ in the Galois closure of $k(u, v)/k(t)$, and hence in particular in $\Omega_v(u)$ divides $\deg(f)/p$ by Remark 2.8 (Abhyankar's lemma), for some prime divisor p of $\gcd(m, n)$, which exists by (3). In particular, $\Omega_v\tilde{\Omega}/\Omega_v(u)$ must be nontrivial, and hence its Galois group identifies via restriction with a nontrivial normal subgroup of the primitive group $\mathrm{Mon}_k(f_2)$. Thus it must contain the transitive subgroup $\mathrm{soc}(\mathrm{Mon}_k(f_2))$. In particular, this transitivity implies that $\Omega_v\tilde{\Omega}/\Omega_v(u)$ is the Galois closure of $\Omega_v(x)/\Omega_v(u)$. In the same way, the Galois group of the Galois closure of $\Omega_u(y)/\Omega_u(v)$ must contain $\mathrm{soc}(\mathrm{Mon}_k(g_2))$. Since $k(x, v)/k(u, v)$ and $k(u, y)/k(u, v)$ are not linearly disjoint, this implies that $\mathrm{Mon}_k(g_2)$ must contain a copy of $\mathrm{soc}(\mathrm{Mon}_k(f_2))$ and vice versa, yielding the claim by Proposition 2.1.

If one (and hence both) of $\mathrm{Mon}_k(f_2), \mathrm{Mon}_k(g_2)$ is solvable, it follows that $m = n$ or $\{m, n\} = \{2, 4\}$ by Proposition 2.1. For nonsolvable $\mathrm{Mon}_k(f_2)$, we may use the classification in [Mü95] to verify that the only instance of noncoprime degrees $m \neq n$ for which $\mathrm{Mon}_k(f_2), \mathrm{Mon}_k(g_2)$ share their nonabelian composition factor is $\{m, n\} = \{6, 10\}$ (and $\mathrm{soc}(\mathrm{Mon}_k(f_2)) \cong A_6$). But note that the index-10 subgroups of A_6 still act transitively on 6 points, contradicting linear disjointness of $k(x, v)/k(u, v)$ and $k(u, y)/k(u, v)$. Finally, assume f_2 is not right-unique. Then $f = f_1' \circ f_2'$ for an indecomposable $f_2' \in k[X] \setminus k$ of degree n' coprime to $n = \deg(f_2)$ by Corollary 2.10. But clearly $m = n$ or $\{m, n\} = \{2, 4\}$ implies that m is coprime to n', a contradiction.

(5) Suppose on the contrary f_2 is not right-unique. Then there must be another right factor f_2' of f of degree coprime to $\deg(f_2)$ by Corollary 2.10. It follows from (3) that an indecomposable right factor g_2 of g must have a primitive monodromy group of degree not a prime power, which is thus necessarily nonsolvable by Galois' theorem [Cox12, Theorem 14.3.17]). The same would hold for *any* indecomposable right factor of g. Using an analog of Ritt's theorem for Siegel functions [Pak10, Theorem 1.1], it follows that g_2 must be right-unique, since in particular a Ritt move for such functions cannot involve two indecomposables with nonsolvable monodromy group. Since $\deg(g_2)$ is not a prime power, it follows from Proposition 2.4 that $\mathrm{Mon}_k(g_2)$ is either almost-simple or of product-type, and in particular has a unique and nonsolvable minimal normal subgroup S^d for a simple group S. Together with the right-uniqueness of g_2, it follows from [KNR24, Proposition 3.3] that $\mathrm{soc}(\ker(\mathrm{Mon}_k(g) \to \mathrm{Mon}_k(g_1)))$ is the unique minimal normal subgroup of $\mathrm{Mon}_k(g) = \mathrm{Mon}_k(f)$, and is a power of the simple group S. But by Ritt's theorems one of f_2 and f_2' (say, f_2) has solvable monodromy group, meaning that $\ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(f_1))$ is a nontrivial solvable normal subgroup of $\mathrm{Mon}_k(f)$, a contradiction. □

The CFSG is used in parts (4)-(5) of the above proof. The proof of Theorems 1.1 and 6.1 apply part (4) only when $\mathrm{Mon}(f) = \mathrm{Mon}(g)$ is solvable, where the CFSG is not applied.

Finally, we will also need the following description of right quadratic factors[9]:

Lemma 2.18. *Let $f, g \in k[X]$ be a minimally reducible pair such that f, g have right composition factors f_r, g_s, resp., where f_r is a composition of two quadratic polynomials. Then g has a quadratic right composition factor.*

Proof. Let Ω be the common Galois closure of $k(x)/k(t)$ and $k(y)/k(t)$ given by Lemma 2.13, where x, y are roots of $f(X) - t, g(X) - t$, respectively. Let $u = f_r(x)$, and $v = g_s(y)$ for an indecomposable right factor g_s of g. Note that since f, g are minimally reducible, by Proposition 2.17(4), g_s is right-unique and $\deg(g_s)$ is 2 or 4. Assume on the contrary $\deg(g_s) = 4$ and hence $\mathrm{Mon}_k(g_s) = S_4$.

Let Ω' be the Galois closure of $k(u, v)/k(t)$. Since both $k(u)/k(t)$ and $k(v)/k(t)$ are totally ramified over ∞ of the same degree $m := \deg(f)/4$, this is also the ramification index of ∞ in $\Omega'/k(t)$ by Remark 2.8. Moreover, since ∞ is unramified in $\Omega'/k(u)$ and $\Omega'/k(v)$, the remark shows these extensions are linearly disjoint from $k(x)$ and $k(y)$, resp.

Let $\Omega_u \subseteq \Omega'$ be the Galois closure of $k(u)/k(t)$. Since Ω is the splitting fields of $f_r(X) - u'$ over Ω_u when u' ranges over conjugates of u (similarly to Lemma 2.19 below), Ω/Ω_u is a compositum of 2-extensions, and hence $\mathrm{Gal}(\Omega/\Omega_u)$ and $\mathrm{Gal}(\Omega/\Omega')$ are 2-groups. This contradicts that the Galois closure of $\Omega'(y)/\Omega'$ has group S_4 by Lemma 2.7(2). □

2.5. **Subdirect powers.** Say $G \leq \prod_{i \in I} H_i$ is a subdirect product, for some groups H_i indexed by a set I, if the projection of G to H_i is surjective for each $i \in I$. We say that K is a subdirect power of $\overline{K}$ if it is a subdirect product of $\prod_{i \in I} \overline{K}$ for some I.

[9]The assertion can be strengthened as follows: If f_r is a composition of r quadratics, then g has a right factor which is a composition of $r - 1$ quadratics. However, we shall not make use of such an extension.

Lemma 2.19. *Let $f = g \circ h : \mathcal{X} \to \mathcal{Z}$ be a composition of maps. Let K be the kernel of the projection $\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(g)$. Let $M \leq K$ be normal in $\mathrm{Mon}_k(f)$, and $\overline{M}$ its image in $\mathrm{Mon}_k(h)$ via the action on some fixed block. Then M is a subdirect power of $\overline{M}$.*

In particular, the lemma applies to $M = K$ and $M = \mathrm{soc}(K)$.

Proof. Let t be the generic point of $\mathcal{Z}$. For every $y \in g^{-1}(t)$, let $\mathcal{X}_y$ be the set of $x \in f^{-1}(t)$ with $h(x) = y$. Let $y_0 \in g^{-1}(t)$ be our fixed block. Since M is normal in $G = \mathrm{Mon}_k(f)$ and the latter is transitive on $g^{-1}(t)$, for every $y \in g^{-1}(t)$, there is an element of G that sends y_0 to y, and hence conjugation by that element maps $\overline{M}$ isomorphically to the image M_y of the action of M on $\mathcal{X}_y$. Since M acts faithfully on $\bigcup_{y\in\mathcal{Y}} \mathcal{X}_y$, it embedds in $\prod_{y\in\mathcal{Y}} M_y \cong \prod_{y\in\mathcal{Y}} \overline{M}$ with surjective projections, so that M is a subdirect power of $\overline{M}$. □

The following is our key consequence to relating the 1-step and 2-step kernels.

Corollary 2.20. *Let $f = f_1 \circ f_2 \circ f_3 : \mathcal{X} \to \mathcal{W}$ be a composition of (nonconstant) maps f_1, f_2, f_3. Let K, N be the kernels in the action of $G := \mathrm{Mon}_k(f)$ through $\mathrm{Mon}_k(f_1 \circ f_2), \mathrm{Mon}_k(f_1)$, resp., and $M \leq N$ be normal in G. Let $\overline{K}, \overline{M}, \overline{K \cap M}$ be the images of $K, M, K \cap M$, resp., in the action of $G_2 := \mathrm{Mon}_k(f_2 \circ f_3)$ on a fixed block, and K_2 the kernel of the action of G_2 through $\mathrm{Mon}_k(f_2)$. Then $M/(K \cap M)$ is a subdirect power of $\overline{M}/(K_2 \cap \overline{M})$. In particular, $\overline{M}/\overline{K \cap M}$ is a quotient of a subdirect power of $\overline{M}/(K_2 \cap \overline{M})$.*

Proof. Let t be the generic point of $\mathcal{W}$, and $z_0 \in f_1^{-1}(t)$ our fixed block. Then K is the kernel of the action of G on $(f_1 \circ f_2)^{-1}(t)$, and N is the kernel of the action of G on $f_1^{-1}(t)$. Thus, N/K and its subgroup $M/(K \cap M)$ act faithfully on $(f_1 \circ f_2)^{-1}(t)$. Write $(f_1 \circ f_2)^{-1}(t)$ as a disjoint union of blocks $\mathcal{Y}_z := f_2^{-1}(z)$, $z \in f_1^{-1}(t)$. Since the kernel of the action of $\overline{M}$ on each block $\mathcal{Y}_z$ is $\overline{M} \cap K_2$, the image of the action of M on $\mathcal{Y}_{z_0}$ is $\overline{M}/(K_2 \cap \overline{M})$. Thus, $M/(K \cap M)$ is a subdirect power of $\overline{M}/(K_2 \cap \overline{M})$ by Lemma 2.19 applied to the G/K-action on $(f_1 \circ f_2)^{-1}(t)$. The last conclusion follows since $\overline{M}/\overline{K \cap M}$ is a quotient of $M/(K \cap M)$. □

The following describes the socle of subdirect powers of $\mathrm{AGL}_1(p)$ and $\mathrm{AGL}_2(2) \cong S_4$.

Lemma 2.21. *Let p be a prime, and suppose either $(r, p) = (2, 2)$ or $r = 1$. Let $K \leq \mathrm{AGL}_r(p)^n$ be a subgroup whose component projections contain C_p if $r = 1$ (resp. the A_4 copy in $S_4 \cong \mathrm{AGL}_2(2)$ if $r = 2$). Then $\mathrm{soc}(K) = K \cap C_p^{rn}$.*

Proof. Since K is solvable by our assumptions on r, p, $\mathrm{soc}(K)$ is the direct product of elementary abelian q-subgroups H_q for various primes q. Since the component projections of each H_q are abelian normal subgroups of a transitive subgroup of $\mathrm{AGL}_r(p)$, and hence contained in C_p^r, it follows that $H_q = 1$ for every $q \neq p$. Thus, $\mathrm{soc}(K) \subseteq C_p^{rn} \cap K$.

For the reverse inclusion, note that C_p^n is a semisimple module under the action of $K/(C_p^{rn} \cap K)$ if $r = 1$. Similarly if $r = 2$, since the Klein group $V_4 \cong C_2^2$ forms an irreducible module under the A_4-action and since the component projection contains A_4, the module V_4^n is semisimple under the action of $K/(V_4^n \cap K)$. Thus in both cases, the submodule $K \cap C_p^{rn}$ is also semisimple, and hence its submodule $\mathrm{soc}(K)$ has a complement N, which in particular is normal in K. By the definition of the socle, this implies $N = 1$. □

The smallest subdirect powers are the diagonal ones: say that a subdirect power $K \leq H^n$ is *diagonal* if each of its n projections $K \to H$ is injective. The following remark shows that the diagonaliy of $\mathrm{soc}(K)$ implies that of K.

Remark 2.22. Suppose $K \leq \overline{K}^m$ is a subdirect power, and $\mathrm{soc}(K) \leq \mathrm{soc}(\overline{K})^m$ is diagonal. Then $K \leq \overline{K}^m$ is diagonal. Indeed, the kernel C of the coordinate projection $K \to \overline{K}$ is a normal subgroup which is disjoint from the diagonal subgroup $\mathrm{soc}(K)$, and hence $C = 1$ by definition of $\mathrm{soc}(K)$, as desired.

If G acts on a power A^d of a group A by acting transitively on the d copies of A (supported only on one of the coordinates)[10]. Then there is a unique diagonal G-invariant copy of A in A^d which we refer to as *the diagonal subgroup of A^d with respect to the G-action.*

On the other extreme, if $A = C_q$ and A^d is a permutation G-module, the following submodule is among the largest submodules. Throughout the paper, we denote by $I_d(q)$ the G-submodule of all $(x_1, \dots, x_d) \in A^d$ with sum $\sum_{i=1}^d x_i = 0$.

2.6. **Wreath products of affine groups.** For polynomial maps $f, g \in k[X]$ of degrees d and q, resp., with q prime and $\mathrm{Mon}_k(g)$ solvable we have $\mathrm{Mon}_k(f \circ g) \leq A \wr B$, where $C_q \leq A \leq \mathrm{AGL}_1(q)$ and $B \leq S_d$ (see §2.3); more precisely, we take $A = \mathrm{Mon}_k(g)$ and $B = \mathrm{Mon}_k(f)$. This section presents preliminary results on subgroups of $A \wr B$ for such A, B.

We describe normalizers and commutator subgroups of transitive subgroups of $G := \mathrm{AGL}_1(q) \wr S_d$ as follows. For $C, H \leq G$, let $\mathcal{N}_C(H)$ denote the elements of C normalizing H, and $[C, H] \leq G$ the commutator subgroup, generated by commutators $[c, h], c \in C, h \in H$.

Proposition 2.23. *Let $V \leq S_d$ be a group containing a cyclic transitive subgroup, let q be a prime, let $G \leq C_q \wr V$ be a subgroup surjecting onto V, and $H = C_q^d \cap G \trianglelefteq G$. Let $U \leq C_q^d$ be such that $H \leq U \leq \mathcal{N}_{C_q^d}(G)$. Then the following hold:*

(1) H is an $\mathbb{F}_q[V]$-submodule of U under the action $\overline{\sigma} \cdot u := \sigma u \sigma^{-1}$, where $G \to V$, $\sigma \mapsto \overline{\sigma}$ is the projection.
(2) Letting $Z := \mathrm{diag}(C_q^d) \cap U$, we have an embedding of modules $U/Z \hookrightarrow H$.
(3) In particular, $[U : H]$ divides q.

Proof. Regarding 1), let $u \in U$ and $\sigma \in G$ be arbitrary. Then $u\sigma^{-1}u^{-1} \in G$. By considering projection modulo C_q^d, it follows that $u\sigma^{-1}u^{-1} = \sigma^{-1}h$ for some $h \in C_q^d \cap G = H$. Hence,

$$\sigma u \sigma^{-1} u^{-1} \in H. \tag{2.2}$$

Thus $\sigma U \sigma^{-1} \subseteq HU = U$, showing i).

Regarding 2), choose $\sigma \in G$ as a preimage of a generator of a cyclic transitive subgroup of V. Note that due to (2.2), H contains the $\mathbb{F}_q[\overline{\sigma}]$-module $[U, \langle\sigma\rangle]$. Note that when identifying the $\mathbb{F}_q[\overline{\sigma}]$-permutation module C_q^d with $\mathbb{F}_q[\overline{\sigma}]$, the commutator $[u, \sigma] = u\sigma u^{-1}\sigma^{-1} = u(\overline{\sigma} \cdot u^{-1}) \in U$ identifies with $u - \overline{\sigma}u = (1 - \overline{\sigma})u \in \mathbb{F}_q[\overline{\sigma}]$. Now $\varphi : U \to [U, \langle\sigma\rangle]$, $u \mapsto [u, \sigma]$ is a homomorphism of submodules of the $\mathbb{F}_q[\overline{\sigma}]$-permutation module, whose kernel $\ker(\varphi) = \ker(1 - \overline{\sigma})$ is clearly the diagonal Z.

[10]Equivalently, the action of G on A^d has a partition that corresponds to the action of G on $\{1, \dots, d\}$.

Finally, 3) is an immediate consequence of 2), since $\dim(Z) \leq 1$. □

Corollary 2.24. *Let q be a prime and d an integer. Let $G \leq \mathrm{AGL}_1(q) \wr S_d$, and let $N \trianglelefteq G$ be a normal subgroup. Set $G_q := G \cap C_q^d$ and $N_q := N \cap C_q^d$. Assume that N contains an element σ whose image $\overline{\sigma}$ in S_d is a d-cycle, and $\sigma^d \in N_q$. Then the following hold:*

(1) G_q/Z embeds into N_q, where $Z \leq G_q$ denotes the intersection of G_q with the diagonal under the action of σ. In particular $[G_q : N_q] \mid q$.
(2) If σ is a qd-cycle and $(d, q) = 1$, then $G_q = N_q$.

Proof. To see 1), note that $\langle N_q, \sigma\rangle \trianglelefteq \langle G_q, \sigma\rangle$, and hence $G_q \leq \mathcal{N}_{C_q^d}(\langle N_q, \sigma\rangle)$: Indeed, for any $a \in G_q$, we have $a\sigma a^{-1} \in N$ since $\sigma \in N \lhd G$, so $a\sigma a^{-1}\sigma^{-1} \in N \cap C_q^d = N_q$, and thus $a\sigma a^{-1} \in \langle N_q, \sigma\rangle$. Now 1) follows from Proposition 2.23.

For 2), note that if $(d, q) = 1$, the $\mathbb{F}_q[\overline{\sigma}]$-module G_q is semisimple and, being a submodule of the permutation module $\mathbb{F}_q[\overline{\sigma}]$, contains at most one copy of the trivial module. Thus, if $N_q \subsetneq G_q$, then by 1), we must have $\dim(Z) = 1$, and by the above, G_q/Z contains no trivial module under the action of $\overline{\sigma}$. However, when σ is a dq-cycle, the d-th power of σ generates such a one-dimensional trivial module inside N_q, making $G_q/Z \cong N_q$ impossible. Therefore $G_q = N_q$. □

The following consequence is useful when dealing with permutation groups of prime power degree.

Corollary 2.25. *Let q be a prime and $d = q^r$ a power of q ($r \geq 1$). Let $G \leq \mathrm{AGL}_1(q) \wr S_d$ and let $\sigma \in G$ be an element mapping to a d-cycle under the projection $G \to S_d$. Set $G_q := G \cap C_q^d \lhd G$ and let e be the rank of the elementary-abelian group G_q. Let $Q \leq G$ be a q-Sylow subgroup. Then Q has nilpotency class at least e.*

Proof. Up to replacing $\langle\sigma\rangle$ by its q-Sylow subgroup and conjugating in G, we may assume that $\sigma \in Q$ and furthermore that $e \geq 2$. Let $Q_0 := Q$ and $Q_i := [Q_{i-1}, Q]$, $i \geq 1$ be the descending central series of Q (so that the nilpotency class is defined as the smallest index i with $Q_i = \{1\}$). Set $\widehat{Q}_i := \langle Q_i \cap G_q, \sigma\rangle$, $i \geq 0$. Note that $\widehat{Q}_i \trianglelefteq \widehat{Q}_{i-1}$ for all i, since indeed $[Q_{i-1} \cap G_q, \langle\sigma\rangle] \subseteq [Q_{i-1}, Q] \cap G_q \subseteq Q_i \cap G_q$. Thus $[\widehat{Q}_{i-1} : \widehat{Q}_i] \mid [\widehat{Q}_{i-1} \cap G_q : \widehat{Q}_i \cap G_q] \mid q$ by Corollary 2.24. As $\widehat{Q}_0 \cap G_q = G_q$, it follows that $\widehat{Q}_{e-2} \cap G_q = \langle Q_{e-2} \cap G_q, \sigma\rangle \cap G_q$ must still be of order $\geq q^2$. Since $\langle\sigma\rangle \cap G_q$ is either trivial or the diagonal under the action of σ, the subgroup $Q_{e-2} \cap G_q$ must still be nondiagonal. As $[\widehat{Q}_{e-2} : \widehat{Q}_{e-1}] \mid q$, this implies $Q_{e-1} \neq \{1\}$, i.e., Q is of nilpotency class at least e. □

3. Lower bounds on solvable monodromy groups of polynomials

Let k be a field of characteristic 0. Our method for proving Theorem 6.1 relies on "largeness" properties for monodromy groups of polynomials from [BKN26]. For indecomposable $f, g \in k[X]$, we say that a subgroup $N \leq \mathrm{Mon}_k(f \circ g)$ has a *large kernel* if either

$$\mathrm{soc}(\mathrm{Mon}_k(g))^{\deg(f)} \leq \ker(N \to \mathrm{Mon}_k(f)),$$

or

$$\mathrm{soc}(\mathrm{Mon}_k(g)) \text{ is cyclic and } \mathrm{soc}(\mathrm{Mon}_k(g))^{\deg(f)-1} \leq \ker(N \to \mathrm{Mon}_k(f)).$$

We say that $f \circ g$ has a *large kernel* if $\mathrm{Mon}_k(f \circ g)$ has a large kernel.

Theorem 3.1 (Theorems 1.2 and 2.1 in [BKN26])**.** *Let $f, g \in k[X]$ be indecomposable with solvable monodromy. Then either $f \circ g$ has a large kernel or it is linearly equivalent over $\overline{k}$ to a monomial, a Chebyshev polynomial or one of only two other cases holds:*

- $\mathrm{Mon}_{\overline{k}}(f \circ g) = C_3 \times S_4 \leq S_{12}$ *with a Ritt move;*
- $\mathrm{Mon}_{\overline{k}}(f \circ g) = \mathrm{GL}_2(3) \leq S_8$ *with no Ritt move.*

In the large kernel case, if moreover, f is linearly related over $\overline{k}$ to X^p or T_p, and g is linearly related over $\overline{k}$ to X^q or T_q, for primes $p, q \geq 2$, then $\ker(\mathrm{Mon}_k(f \circ g) \to \mathrm{Mon}_k(f))$ *contains C_q^p.*

We shall need the following extension of Theorem 3.1, which takes into account normal subgroups of $\mathrm{Mon}_k(f \circ g)$ and strengthens the largeness assertions in some cases.

Corollary 3.2. *Let $f, g \in k[X]$ be indecomposable with solvable monodromy of degrees $p := \deg(f)$ and $q := \deg(g)$, respectively, and such that $f \circ g$ is not among the exceptional cases of Theorem 3.1. Let $N \trianglelefteq \mathrm{Mon}_k(f \circ g)$ be a normal subgroup containing a cyclic transitive subgroup. Then the following hold:*

(1) $\ker(N \to \mathrm{Mon}_k(f))$ *is large.*

(2) If either $q = 4$ or p, q are distinct primes, then more strongly $\ker(N \to \mathrm{Mon}_k(f)) \geq \mathrm{soc}(\mathrm{Mon}_k(g))^p$.

(3) If $\mathrm{Mon}_{\overline{k}}(g)$ *is noncyclic, and either $q = 4$ or $p > 2$ is prime, then more strongly* $\mathrm{soc}(\mathrm{Mon}_k(g))^p$ *is a minimal normal subgroup of* $\mathrm{Mon}_k(f \circ g)$.

Proof. Since we will show 3) (which implies 2) and 1)) for $q = 4$, we first assume $q \neq 4$. Since we are not in the exceptional cases, either $K := \ker(G \to \mathrm{Mon}_k(f))$ contains C_q^p by Theorem 3.1 or ($p = 4$ and K contains a subgroup C_q^3). Since N contains a cyclic transitive subgroup, 1) and 2) then follow directly from Corollary 2.24, together with the observation that the $\mathbb{F}_2[S_4]$-permutation module has no submodule of dimension 2, to deal with the case $(p, q) = (4, 2)$.

Assume now that $\mathrm{Mon}_{\overline{k}}(g)$ is noncyclic (allowing also $q = 4$) and $p > 2$ is prime. Set $G := \mathrm{Mon}_k(f \circ g)$. It then follows from refinements of Theorem 3.1, namely [BKN26, Theorem 2.1] (in case p, q prime) and [BKN26, Theorem 2.3] (in case $q = 4$ and p prime), that $\ker(G/\mathrm{soc}(K) \to \mathrm{Mon}_k(f))$ contains a subgroup $C_2^{p-1} \leq \mathrm{Aut}(C_q)^p$ (when q prime) or a subgroup $C_3^{p-1} \leq (S_4/V_4)^p \cong S_3^p$ (when $q = 4$)). Therefore, [BKN26, Lemma 3.8] implies that K contains $K_0 := \mathrm{soc}(\mathrm{Mon}_k(g))^p$ as a *minimal* normal subgroup, showing 3) in all cases except for $(p, q) = (2, 4), (4, 4)$. Those last two cases are treated by a direct inspection with Magma. □

We shall need the following addition for compositions of three polynomials. The reader might choose to skip part (4) as it is applied only with $q = p = 3$ (a case that is also verified directly with Magma). For a prime q and an integer $n \geq 2$, recall that $I_n(q)$ denotes the

augmentation ideal of the module $\mathbb{F}_q^n$, viewed as the permutation module under a fixed cyclic group C_n.

Proposition 3.3. *Let $f = f_1 \circ f_2 \circ f_3$, where $f_1, f_2, f_3 \in k[X]$ are indecomposable of degrees m, p, q, respectively, with $\mathrm{Mon}_{\overline{k}}(f)$ solvable and $\mathrm{Mon}_{\overline{k}}(f_3) = C_q$ (for q prime). Assume $f_1 \circ f_2$ and $f_2 \circ f_3$ are either strongly-unique or have monodromy group D_4 over k. Assume moreover that none of $\Gamma := \mathrm{Mon}_k(f_1 \circ f_2)$ and $G_2 := \mathrm{Mon}_k(f_2 \circ f_3)$ equals $\mathrm{GL}_2(3)$. Let N be a normal subgroup of $G_3 := \mathrm{Mon}_k(f)$ containing a cycle σ of length mpq, and K, M the kernels of the maps $G_3 \to \Gamma = \mathrm{Mon}_k(f_1 \circ f_2)$ and $G_3 \to \mathrm{Mon}_k(f_1)$, respectively.*

(1) If $p \neq q$ is a prime, then $N \cap K$ properly contains $I_p(q)^m$.
(2) If $p = 4$, then $N \cap K$ contains $I_4(q)^m$, and if additionally $q > 2$, this containment is proper.
(3) If $p = q$ and $m \neq 4$, then $N \cap K$ contains an index-q subgroup of $I_p(q)^m$. If moreover $p = q = 2 \neq m$, then the subgroup $(N \cap M)^2$, generated by squares in $N \cap M$, contains $I_2(2)^m \cong C_2^m$.
(4) If $p = q$ and $m = 4$, then $N \cap K \supseteq C_q^{3q-4}$. More precisely, if $\widehat{N}_0 \leq S_{3q^2}$ denotes the image of the stabilizer $N_0 \leq N$ of a root of $f_1(X) - t$ in its natural action on $3q^2$ points, then the image $\widehat{N_0 \cap K}$, of $N_0 \cap K$ in S_{3q^2}, contains an index-q subgroup of $I_q(q)^3$.

The proofs of parts (3) and (4) require the following lemma.

Lemma 3.4. *Let q be a prime, $m \geq 2$ an integer, $H \leq S_m$ a primitive group and $G_3 \leq \mathrm{AGL}_1(q) \wr \mathrm{AGL}_1(q) \wr H$. Let M, K be the kernels of the projections $\psi : G_3 \to H$ and $\pi : G_3 \to \mathrm{AGL}_1(q) \wr H$, respectively. Assume that 1) $\pi(G_3)$ contains C_q^m, and 2) the image of $M \leq (\mathrm{AGL}_1(q) \wr \mathrm{AGL}_1(q))^m$ under projection to a component contains $C_q \wr C_q$. Then there exists an index-q subgroup U of $I_q(q)^m$ such that $U \leq [M_q, M_q] \cap K$ for a q-Sylow subgroup $M_q \leq M$. If moreover $q = 2$, then $U \leq M^2$, where M^2 denotes the subgroup generated by all elements x^2, for $x \in M$.*

Proof. The existence of such an index-q subgroup U of $I_q(q)^m$ such that $U \leq [M_q, M_q] \cap K$ is an immediate consequence of [BKN26, Lemma B.3 with Example B.5]. The additional assertion for $q = 2$ follows since every commutator $[x, y] = x^2(x^{-1}y)^2y^{-2}$ is a product of squares. □

Proof of Proposition 3.3. Due to the assumptions on $\Gamma = G_3/K$, one of the following holds by Theorem 3.1 together with the strengthening [BKN26, Theorem 2.3] for Case iii) below:

i) m and p are both prime, and G_3/K contains $C_p^m.C_m$.
ii) p is prime, $m = 4$, and G_3/K contains $V.S_4$, where $V \subset \mathbb{F}_p^4$ is a 3-dimensional submodule.
iii) $p = 4$, m is prime, and G_3/K contains $U.C_m$, where $U \leq S_4^m$ contains an index-3 subgroup of A_4^m (resp., contains A_4^2 in the case $m = 2$).
iv) $p = m = 4$, and G_3/K contains V_4^4, where $V_4 \cong C_2 \times C_2$ is the Klein 4-group.

Similarly, the assumptions on $G_2 = \mathrm{Mon}_k(f_2 \circ f_3)$ imply that G_2 contains $C_q^p.C_p$ when p is prime, resp. contains $W.S_4$ when $p = 4$, where $W = I_4(q) \subset \mathbb{F}_q^4$ is a 3-dimensional

submodule. Since the image $\overline{M}$ of M in G_2 under projection to a component is a normal subgroup of G_2 containing a cyclic transitive subgroup, Corollary 2.24 yields that $\overline{M}$ contains $I_p(q).C_p$ for $p \neq 4$. Analogously, when $p = 4$, Corollary 2.24 implies that $\overline{M}$ contains $W.S_4$ with $W = I_4(q)$ as above, since W becomes a permutation module under the action of $A_4 \leq S_4$ with no submodule of dimension 2.

(1) Assume $p \neq q$ is a prime. Then the C_p-module $C_q^p \cong \mathbb{F}_q[C_p]$ is semisimple[11], and a generator of C_p acts nontrivially on every irreducible submodule of $I_p(q)$. When m is prime, since G_3/K contains the full C_p^m by i) and C_p acts faithfully on every nontrivial submodule of $I_p(q)$, it follows directly from [BKN26, Lemma 3.9] that G_3 contains an extension $I_p(q)^m.C_p^m.C_m$.

Similarly by ii), when $m = 4$, the group G_3/K contains two elements $x_1, x_2 \in C_p^m$ whose supports have exactly one element in common; again, [BKN26, Lemma 3.9] implies that G_3 contains $I_p(q)^m.V.S_4$. Since $I_p(q)^m$ does not contain the diagonal submodule, Corollary 2.24 implies that $N \cap K$ still contains $I_p(q)^m$. On the other hand, the mp-th power of the cyclic transitive subgroup from the assumptions generates the diagonal submodule inside $N \cap K$. Since $p \neq q$, this implies $N \cap K$ properly contains $I_p(q)^m$.

(2) Now assume $p = 4$ and $G_2 \ncong \mathrm{GL}_2(3)$. When $m \neq 4$, the kernel of $\psi : \Gamma \to \mathrm{Mon}_k(f_1)$ contains an index-3 subgroup of A_4^m (resp., contains all of A_4^2 for $m = 2$) by iii), which in particular projects to an index-3 subgroup of $C_3^m \cong A_4^m/V_4^m$. Hence, it induces a subspace of codimension ≤ 1 in $\mathbb{F}_3^m$ which intersects any two-dimensional subspace (resp., induces $\mathbb{F}_3^2$). Thus there exist two elements of order 3 in $\ker(\psi) \leq S_4^m$ whose supports have exactly one element in common. Similarly, when $m = 4$, a direct check using Magma[12] shows that the kernel of $\psi : \Gamma \to \mathrm{Mon}_k(f_1)$ contains a subgroup $C_3^2 \subseteq S_4^4$ in which all nonidentity elements are supported on exactly 3 components. Thus there exist three elements of order 3 in $\ker(\psi)$ whose supports have only one element in common. In all cases, it follows from [BKN26, Lemma 3.9] for $q \geq 3$, and from [BKN26, Lemma B.1 with Example B.2] for $q = 2$, that K contains $I_4(q)^m \cong C_q^{3m}$. For $q \geq 3$, since $I_4(q)^m$ does not contain the diagonal, as in Case (1), it follows from Corollary 2.24 that $N \supseteq I_4(q)^m$, and that this containment is even proper. For $q = 2$, Corollary 2.24(1) implies $[I_4(2)^m : N \cap I_4(2)^m] \leq 2$. On the other hand, the intersection of N with the submodule $W_1 \cong I_4(2)$ of $I_4(2)^m$, consisting of elements supported only on the first component, would have to be a submodule of W_1 of codimension at most 1. However, since $I_4(2)$ is the augmentation ideal of the $\mathbb{F}_2[S_4]$-permutation module, it has no submodule of codimension 1. Thus N contains all of W_1, and by transitivity of the action on components, $N \supseteq I_4(2)^m$.

(3) Next, assume that $m \neq 4$ and $q = p$. By i), G_3/K contains $C_q \wr C_m$, and G_2 contains $C_q \wr C_q$.

As long as $q \neq 2$, we first claim that the image $\overline{M}$ of M in G_2 contains $C_q \wr C_q$. Indeed, the image of the stabilizer $G_z \leq \mathrm{Mon}_{\overline{k}}(f)$ of a root z of $f_1(X) - t \in \overline{k}(t)[X]$ maps onto

[11]In fact $C_q^p \cong \mathbb{F}_q[x]/(x^p - 1)$ where σ acts by multiplication by x. As $x^p - 1$ is separable for $p \neq q$, the module is semisimple with the trivial module $\mathbb{F}_q[x]/(x - 1)$ appearing with multiplicity 1.

[12]To do so we run over all subgroups $P \leq S_4 \wr S_4$ surjecting onto S_4, with block kernel acting on a block as S_4, and with a cyclic transitive subgroup (there are only four different such P).

$\tilde{G}_2 := \mathrm{Mon}_{\overline{k}}(f_2 \circ f_3) \supseteq C_q \wr C_q$ via its action on the roots of $(f_2 \circ f_3)(X) - z$. Since $\mathrm{Mon}_{\overline{k}}(f_1) \in \{C_m, D_m\}$, the image $\overline{M \cap G_z}$ of $M \cap G_z$ in $\tilde{G}_2$ is of index ≤ 2, and hence $[\tilde{G}_2 : \overline{G_z \cap M}] \leq 2$. As $q \neq 2$ and $\tilde{G}_2 \supseteq C_q \wr C_q$, the claim follows immediately.

Suppose that $q > 2$, or $q = 2$ and $\overline{M} = C_2 \wr C_2$. Then, G_3 fulfills the assumptions of Lemma 3.4. Thus, by the lemma, there exists a q-Sylow subgroup $M_q \leq M$ and a subgroup $U \leq [M_q, M_q]$ of index at most q in $I_q(q)^m$. To show that U is contained in $N \cap K$ as asserted, it therefore suffices to show that $N \supseteq [M_q, M_q]$. We will achieve this via a twofold application of Corollary 2.24. First, an application of Corollary 2.24(1) with $N/(N \cap K) \cong NK/K$ (resp. G_3/K) in the role of N (resp., of G) shows that the q-Sylow group of $(N \cap M)/(N \cap K)$ is of index dividing q in the one of M/K. Next, an application of Corollary 2.24(1) to $N \trianglelefteq NK$ shows that the q-Sylow subgroup of $N \cap K$ is of index dividing q in that of K. Both observations together show that the Sylow subgroup $N \cap M_q$ of $N \cap M$ is of index dividing q^2 in M_q. Moreover, $N \cap M_q \lhd M_q$. It follows that $M_q/(N \cap M_q)$ is abelian, and hence $N \supseteq [M_q, M_q] \supseteq U$, as claimed. When $q = p = 2 \neq m$, the element $\sigma^{2m} \in (N \cap M)^2$ is diagonal and, in particular is supported on an odd number of components of the $\mathbb{F}_2[C_m]$-module $I_2(2)^m \cong C_2^m$. Therefore $(N \cap M)^2$ contains not only the (unique) index-2 submodule, but in fact the whole $I_2(2)^m$.

To complete the proof of (3), it remains to treat the case $q = p = 2$ when the image of M in G_2 is not equal to the full group $C_2 \wr C_2$. Since this image nevertheless contains a cyclic transitive subgroup, it must be C_4. Therefore, $M \leq C_4^m$, and $M/K = C_2^m$ by (i) above. Now, in case $m = 2$, since $\langle \sigma^4 \rangle \leq N \cap K$ is the diagonal submodule of $I_2(2)^m$, and is of index 2 in it, $N \cap K$ indeed contains an index-2 subgroup of $I_2(2)^m$. If instead $m > 2$ is odd, note that $N/(N \cap K) \leq G_3/K$ is a normal subgroup containing a $(2m)$-cycle and hence contains $C_2 \wr C_m$ by Corollary 2.24.(2) and (i) above. Since in addition $M/K = C_2^m$ and $NK \cap M = (N \cap M)K$ (as $K \leq M$), we get that $(N \cap M)/(N \cap K) \cong (NK \cap M)/K = C_2^m$. Hence $N \cap M = C_4^m$, and therefore $(N \cap M)^2 = C_2^m$.

(4) In case $\mathrm{Mon}_k(f_1 \circ f_2) = G_3/K$ contains all of C_q^4, we may argue just as in Case (3) to obtain that $N \cap K$ contains an index-q subgroup of $I_q(q)^4$, and consequently the projection of $N_0 \cap K$ to its orbit of length $3q^2$ (where $N_0 = N \cap M.S_3$ denotes the stabilizer in N of a root of $f_1(X) - t$) contains an index-q subgroup of $I_q(q)^3$.

In view of iii) at the beginning of the proof, we may thus assume $\ker(\mathrm{Mon}_k(f_1 \circ f_2) \to \mathrm{Mon}_k(f_1))$ to have a q-Sylow group isomorphic to C_q^3.

In order to be able to apply Lemma 3.4, we now descend to the stabilizer $H_3 = M.S_3 \leq G_3$ of a root z of $f_1(X) - t$ in G_3. This group acts transitively on $3q^2$ elements, namely, the roots of $f(X) - t$ not mapping to the given root z of $f_1(X) - t$ under $f_2 \circ f_3$. Denote by $\widehat{H}_3$ (resp., $\widehat{M}$, resp. $\widehat{K}$) the image of H_3 (resp., M, resp., K) in this action, so that $\widehat{M}$ and $\widehat{K}$ preserve a maximal and a minimal block system in $\widehat{H}_3$, respectively, and they are in fact the full block kernels of these actions: for $\widehat{M}$ this is obvious since an element of G_3 stabilizing 3 out of 4 maximal blocks must stabilize the last as well; if $\widehat{K}$ were not the full block kernel in the action on the minimal block system, there would have to be an element of $\ker(\mathrm{Mon}_k(f_1 \circ f_2) \to \mathrm{Mon}_k(f_1))$ acting nontrivially only on the q roots of $f_1(f_2(X)) - t$ mapping to the fixed root z of $f_1(X) - t$ (which is not "seen" by $\widehat{H}_3$) while fixing all others.

However, this would imply $\ker(\mathrm{Mon}_k(f_1 \circ f_2) \to \mathrm{Mon}_k(f_1))$ having full q-part C_q^4, which we have excluded above.

We aim to repeat the argument of (3) with $\widehat{H}_3$ in place of G_3. This will show the minimal block kernel $\widehat{K}$ of $\widehat{H}_3$ contains a subgroup $C_q^{3(q-1)-1}$, which a fortiori implies the same for K (and with the descent argument from $\widehat{K}$ to $\widehat{N_0 \cap K}$ unchanged). To verify the assumptions of Lemma 3.4, first note that, due to G_3/K containing a subgroup C_q^3 and surjecting to S_4, the group $\widehat{H}_3/\widehat{K}$ contains $C_q^3.C_3 \cong C_q \wr C_3$, since indeed if the projection of $V \cong C_q^3$ to the union of three (out of four) blocks were not injective, we would obtain $\ker(\mathrm{Mon}_k(f_1 \circ f_2) \to \mathrm{Mon}_k(f_1)) \supseteq C_q^4$, contradicting our assumptions. Moreover, the image of the maximal block kernel $\widehat{M} \trianglelefteq \widehat{H}_3$ under projection to any given of the three components equals the image $\pi(M)$ of $M \trianglelefteq G_3$ under projection to any of the four maximal blocks. But the image $\pi(H_3)$ of a maximal block stabilizer $H_3 = M.S_3$ still fulfills $C_q \wr C_q \leq \pi(H_3) \leq AGL_1(q) \wr AGL_1(q)$ by Theorem 3.1, and $\pi(H_3)/\pi(M)$ must be a quotient of $H_3/M \cong S_3$; for $q \geq 5$, this shows instantly that $\pi(M) \supseteq C_q \wr C_q$, whereas for $q = 3$, the same conclusion is easily verified upon noting additionally that $\pi(M)$ acts transitively. Now the argument is completely analogous to Case (3); one should merely note that, since G_3/K contains C_q^3, the group $\widehat{N_0}/\widehat{K}$ contains all of $C_q \wr C_3$, and in particular contains a $3q$-cycle. □

4. Diagonality of the kernel

Let k be a field of characteristic 0. We start with the following key theorem on the diagonality of the block kernel for minimally reducible pairs.

Theorem 4.1. *Suppose that $f \in k[X]$ and a Siegel function $g \in k(X)$ form a minimally reducible pair, and that $f = h \circ f_r$ for an indecomposable $f_r \in k[X]$ of solvable monodromy. If $g \notin k[X]$, assume further $\deg(f)$ is odd. Then $K := \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(h))$ is either a diagonal subgroup of $\mathrm{Mon}_k(f_r)^{\deg(h)}$ or ($\deg(f_r) = 2$ and $K \cong C_2 \times C_2$).*

Remark 4.2. We shall moreover see in the proof below that the case ($\deg(f_r) = 2$ and $K \cong C_2 \times C_2$) can only occur if there is a complete decomposition $g = g_1 \circ \cdots \circ g_s$ such that either $\mathrm{Mon}_k(g_s) = S_4$ or $\mathrm{Mon}_k(g_{s-1} \circ g_s) = D_4$.

The key ingredient in the proof is the following proposition:

Proposition 4.3. *Let $f \in k[X]$, $g \in k(X)$ be a minimally reducible pair, and Ω the common splitting field of $f(X) - t, g(X) - t$ over $k(t)$. Assume $f = h_1 \circ f_r$, $g = h_2 \circ g_s$ for indecomposable $f_r \in k[X], g_s \in k(X)$ with solvable $\mathrm{Mon}_k(f_r)$. Let $K = \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(h_1))$ and $\Omega' = \Omega^{\mathrm{soc}(K)}$. Let y be a root of $g(X) - t$.*

(1) If $\deg(f_r)$ is prime, then $\Omega'(y) = \Omega$;
(2) If $g \in k[X]$ and $\mathrm{Mon}_k(g_s) = S_4$, then $\Omega'(y) = \Omega$;
(3) If $g \in k[X]$ and $\mathrm{Mon}_k(g_s) = C_2$, then $\Omega'(y, y') = \Omega$ for some conjugate y' of y.

Note that group theoretically, the equality $\Omega'(y) = \Omega$ means that $V := \mathrm{Gal}(\Omega/k(y))$ and $\mathrm{soc}(K)$ generate a subgroup isomorphic to a semidirect product $\mathrm{soc}(K) \rtimes V$. Also note that in (3), the last assumption implies that $\Omega'(y)/\Omega'$ is quadratic and hence the conclusion is that Ω/Ω' is at most biquadratic.

To prove Proposition 4.3, we shall need the following lemmas.

Lemma 4.4. *With the notation of Proposition 4.3, let $k(v) = \Omega' \cap k(y)$, and assume additionally that $v = v(y) \in k(y)$ is linearly equivalent over $\overline{k}$ to a polynomial map. Then $[k(y) : k(v)]$ is either a prime or is 4.*

Proof. Set $d_r := \deg(f_r)$. Since f_r is indecomposable, either $\mathrm{Mon}_k(f_r) \leq \mathrm{AGL}_1(p_r)$ where $d_r = p_r$ is a prime, or $\mathrm{Mon}_k(f_r) = S_4$ and $d_r = 4$, by Proposition 2.1. If $d_r = 4$, set $p_r = 2$. Note that K is a subdirect power of its image $\overline{K} \leq \mathrm{Mon}_k(f_r)$ by Lemma 2.19. Moreover $\overline{K} = S_4$ if $d_r = 4$ by Lemma 2.7.(2) and Remark 2.8(1). Hence, $\overline{K}$ contains C_{p_r} if $d_r = p_r$ (resp. A_4 if $d_r = 4$), by Lemma 2.6. Hence $\mathrm{soc}(K)$ is a p_r-elementary abelian group by Lemma 2.21. Since $k(y)/k(v)$ and $\Omega'/k(v)$ are linearly disjoint, it follows that $[k(y) : k(v)] = [\Omega'(y) : \Omega']$ is a power of p_r.

Since $v = v(y)$ is then linearly related over $\overline{k}$ to a polynomial of prime power degree by assumption, $\mathrm{Mon}_k(v)$ contains a cyclic transitive subgroup, but also contains the regular p_r-elementary-abelian normal subgroup $\mathrm{Gal}(\Omega'(y)/\Omega')$, where the latter is identified via restriction with a subgroup of $\mathrm{Mon}_k(v)$. By Lemma 2.2, this implies that $[k(y) : k(v)]$ equals p_r or 4. □

Lemma 4.5. *Suppose that $f \in k[X]$ and $g \in k(X)$ form a minimally reducible pair. Write $f = h \circ f_r$ and $g = g_1 \circ g_2$ for indecomposable f_r and $\deg(g_2) > 1$, and assume $\mathrm{Mon}_k(f_r)$ is solvable with $p_r := \deg(f_r)$ prime. Then the fiber product $\mathbb{P}^1 \#_{g,h} \mathbb{P}^1 \to \mathbb{P}^1$ of g and h factors through f. Equivalently, letting x, y be the roots of $f(X) - t$ and $g(X) - t$, resp., in an extension of $k(t)$, and setting $u = f_r(x)$, there exists a $k(t)$-conjugate x_0 of x such that $k(x_0) \subseteq k(u, y)$. Furthermore, x_0 can be chosen as a $k(u)$-conjugate of x.*

Proof. Let $v = g_2(y)$. Since f and g is a minimally reducible pair, $k(x)$ and $k(v)$ (resp., $k(y)$ and $k(u)$) are linearly disjoint over $k(t)$. Let $\Omega_x/k(u, v)$ (resp., $\Omega_y/k(u, v)$) be the Galois closure of $k(v, x)/k(u, v)$ (resp., $k(u, y)/k(u, v)$). Since $k(u, v)$ and $k(x)$ are linearly disjoint over $k(u)$, we identify $\mathrm{Gal}(\Omega_x/k(u, v))$ with a subgroup of $\mathrm{Mon}_k(f_r)$, as in Remark 2.9. Since f_r is indecomposable of degree $\neq 4$ with solvable monodromy, these subgroups identify with subgroups of $\mathrm{AGL}_1(p_r)$, where $p_r = \deg(f_r)$ is prime, by Proposition 2.1. Since p_r is prime and $k(v, x)/k(u, v)$ and $k(u, y)/k(u, v)$ are not linearly disjoint, we have $k(v, x) \subseteq \Omega_y$ and hence $\Omega_x \subset \Omega_y$. Since the image of $\mathrm{Gal}(\Omega_y/k(u, y))$ in $\mathrm{Gal}(\Omega_x/k(u, v)) \leq \mathrm{AGL}_1(p_r)$ is intransitive, Lemma 2.3 gives a root x_0 of $f_r(X) - u$ fixed by this image. This root is a $k(u)$-conjugate of x that is contained in $k(u, y)$, yielding the desired inclusion $k(v, x_0) \subseteq k(u, y)$, cf. Figure 1. As $k(u, y)$ is the compositum of the linearly disjoint extensions $k(y)/k(t)$ and $k(u)/k(t)$, it is the function field of the fiber product of g and h, so that the inclusion $k(x_0) \subseteq k(u, y)$ implies that this fiber product factors through f. □

Proof of Proposition 4.3. Let x be a root of $f(X) - t \in k(t)[X]$, and set $u = f_r(x)$ and $k(v) = \Omega' \cap k(y)$.

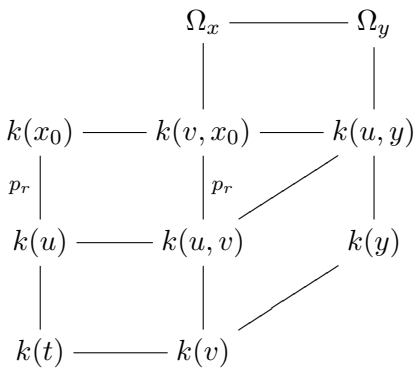

FIGURE 1. Diagram of relevant field extensions in the proof of Lemma 4.5

(1) Assume first $p_r = \deg(f_r)$ is prime. Since in addition $\Gamma_r = \mathrm{Mon}_k(f_r)$ is solvable, it embeds into $\mathrm{AGL}_1(p_r)$ by Proposition 2.1. Thus, $\mathrm{Mon}_k(f)$ is a subgroup of $\mathrm{AGL}_1(p_r) \wr \mathrm{Mon}_k(h_1)$. As in the proof of Lemma 4.4, K is a subdirect power of its image $\overline{K} \leq \mathrm{AGL}_1(p_r)$ by Lemma 2.19, and $\overline{K}$ contains C_{p_r} by Lemma 2.6. Hence, by Lemma 2.21, $\mathrm{soc}(K) = C_{p_r}^{\deg(h_1)} \cap K$, and in particular $\mathrm{soc}(K)$ is a p_r-elementary abelian group. .

On the one hand, note that for any $k(t)$-conjugate u_0 of u and roots x_1, x_2 of $f_r(X) - u_0$, we have $\Omega'(x_1) = \Omega'(x_2)$: Indeed, since $\Omega'/k(t)$ is Galois (as $\mathrm{soc}(K) \leq K$ is characteristic) and $\Omega' \neq \Omega$, we have $k(x_1) \not\subset \Omega'$, and hence $\Omega'/k(u_0)$ and $k(x_1)/k(u_0)$ are linearly disjoint. This implies that $f_r(X) - u_0$ is irreducible over Ω'. As $\mathrm{soc}(K)$ is abelian, $\Omega'(x_1)/\Omega'$ is Galois, and hence $\Omega'(x_1) = \Omega'(x_2)$.

On the other hand, since $k(y)/k(t)$ and $k(u)/k(t)$ are linearly disjoint, $h_1(X) - t$ remains irreducible over $k(y)$, and hence $V := \mathrm{Gal}(\Omega/k(y))$ acts transitively on the $k(t)$-conjugates of u. To apply Lemma 4.5, note that $k(y)/k(v)$ is nontrivial since Ω is the Galois closure of $k(y)/k(t)$ and since $\Omega' \neq \Omega$ (as $p_r \mid \mathrm{soc}(K)$). Thus the lemma implies that some $k(u)$-conjugate x_0 of x is contained in $k(y, u)$. Hence, $k(v, x_0^\sigma) \subset k(u^\sigma, y) \subset \Omega'(y)$ for every $\sigma \in V = \mathrm{Gal}(\Omega/k(y))$. Note that since $\Omega'(y)/\Omega'$ is abelian, and x_0^σ is contained $\Omega'(y)$, so is every $k(u^\sigma)$-conjugate of x_0^σ. Combining this with the transitivity of $V = \mathrm{Gal}(\Omega/k(y))$ on $k(t)$-conjugates of u, we see that $\Omega'(y)$ contains all $k(t)$-conjugates of x, that is, $\Omega'(y) = \Omega$.

(2) Assume $g \in k[X]$ and $\mathrm{Mon}_k(g_s) = S_4$. Since the conclusion follows from (1) if $\deg(f_r)$ is prime, we may assume $\mathrm{Mon}_k(f_r) = S_4$ in view of Proposition 2.1. Let Ω_u, Ω_v and Ω_x, Ω_y be the Galois closures of $k(u)/k(t), k(v)/k(t)$, and $k(x)/k(u), k(y)/k(v)$, respectively.

Since f, g form a minimally reducible pair, g_s is right-unique by Proposition 2.17(5). Thus, Lemma 4.4 implies that $k(v) = k(g_s(y))$. Moreover, $\deg(f) = \deg(g)$ by Corollary 2.15. Denote this degree by n. Since $\deg(h_1) = \deg(h_2) = n/4$, this is also the ramification index of $\Omega_u\Omega_v/k(t)$ over ∞ by Remark 2.8(1) (Abhyankar's lemma). Hence $\mathrm{Gal}(\Omega_x \cdot \Omega_u\Omega_v/\Omega_u\Omega_v)$ and $\mathrm{Gal}(\Omega_y \cdot \Omega_u\Omega_v/\Omega_u\Omega_v)$ are also S_4 by Lemma 2.7(2), and hence so are $\mathrm{Gal}(\Omega_x\Omega_u(v)/\Omega_u(v))$, $\mathrm{Gal}(\Omega_y\Omega_u(v)/\Omega_u(v))$.

We next show that $\Omega_y\Omega_u \supseteq \Omega_x$. Since $k(x,v)/k(u,v)$ and $k(u,y)/k(u,v)$ are not linearly disjoint but both are linearly disjoint from $\Omega_u(v)$, the extensions $\Omega_u(x,v)/\Omega_u(v)$ and $\Omega_u(y)/\Omega_u(v)$ are not linearly disjoint as well. As $\Omega_x\Omega_u(v)/\Omega_u(v)$ and $\Omega_y\Omega_u/\Omega_u(v)$ are both S_4-extensions, this implies $\Omega_x\Omega_u(v) = \Omega_y\Omega_u$. In particular $\Omega_y\Omega_u \supseteq \Omega_x$.

We claim that $\Omega_y\Omega_u = \Omega$. As V preserves Ω_u and fixes y and v, it also preserves $\Omega_u(v), \Omega_u(y)$ and hence also the Galois closure $\Omega_y\Omega_u$ of $\Omega_u(y)/\Omega_u(v)$. By the minimal reducibility assumption, $k(y)/k(t)$ and $k(u)/k(t)$ are linearly disjoint, and hence V is transitive on the conjugates of u. As $\Omega_y\Omega_u \supseteq k(x)$, for every conjugate u' of u, by applying an element of V, we get that $\Omega_y\Omega_u$ contains $\Omega_u(x')$ for a root x' of $f_r(X) - u' \in k(u')[X]$. Moreover, since $\Omega_y\Omega_u$ contains the Galois closure Ω_x of $k(x)/k(u)$, this implies that $\Omega_y\Omega_u$ also contains the Galois closure of $k(x')/k(u')$. Since V is transitive on $k(t)$-conjugate of u, it follows that $\Omega_y\Omega_u$ contains all conjugates x' of x, proving the claim.

Finally to derive (2), note that Ω' and $k(y)$ are linearly disjoint over $k(v)$, and hence the compositum $\Omega_y\Omega'$ coincides with the Galois closure of $\Omega'(y)/\Omega'$ by Remark 2.9. However, as $\mathrm{soc}(K)$ is a 2-elementary abelian group, $\Omega'(y)/\Omega'$ is Galois, and hence $\Omega'(y) = \Omega_y\Omega'$ which contains Ω by the last claim.

(3) Since the conclusion follows from (1) if $\deg(f_r)$ is prime, we may assume $\mathrm{Mon}_k(f_r) = S_4$ by Proposition 2.1. Since $g \in k[X]$, the right factor g_s is right unique by Proposition 2.17(4). Due to Lemma 4.4, $[k(y) : k(v)]$ is either 2 or 4; in the latter case, however, $v = v(y)$ would be a composition of two quadratic polynomials (since g_s is a right-unique factor), contradicting Lemma 2.18. Thus, $[k(y) : k(v)] = 2$, and therefore $k(v) = k(g_s(y))$. Since $k(x,v)$ contains the quadratic extension $k(u,y)/k(u,v)$ by minimal reducibility and since $\Omega' \supseteq k(u,v)$, we have $\Omega'(x) \supseteq \Omega'(y)$. Since $\Omega'/k(t)$ is Galois, $[k(y') : \Omega' \cap k(y')] = 2$ for any $k(t)$-conjugate y' of y, so $\Omega'(y') \subseteq \Omega'(x)$ by the same argument. Thus $\Omega'(x) = \Omega$. Therefore either $[\Omega'(x) : \Omega'] = 2$, in which case $\Omega = \Omega'(x) = \Omega'(y)$, or $[\Omega'(x) : \Omega'] = [k(x) : k(u)] = 4$, in which case $\Omega = \Omega'(x) = \Omega'(y, y')$ for some $k(t)$-conjugate y' of y. □

Proof of Theorem 4.1. Let x, y be roots of $f(X) - t, g(X) - t$, respectively, in an extension of $k(t)$. As in Proposition 4.3, let $u = f_r(x)$, let Ω' be the fixed field of $\mathrm{soc}(K)$ and $k(v) = \Omega' \cap k(y)$.

Assume at first that g is not a polynomial, but merely a Siegel function, and thus by assumption that $\deg(f)$ is odd. In particular, $\mathrm{Mon}_k(f_r) \leq \mathrm{AGL}_1(p_r)$ for an odd prime $p_r = \deg(f_r)$ by Proposition 2.1. It follows that $\mathrm{soc}(K) = C_{p_r}^{\deg(h)} \cap K$ by Lemmas 2.19 and 2.21, and in particular $[k(y) : k(v)] = [\Omega'(y) : \Omega'] = p_r^\ell$ is odd.

We claim that $v = v(y)$ is linearly related over $\overline{k}$ to a polynomial of odd degree. Indeed, write $g = h \circ v$ for some $h \in k(X) \setminus k$ and pick $\lambda \in h^{-1}(\infty)$. Since Ω is the Galois closure of $k(y)/k(t)$, and its ramification over ∞ is the same as of the totally ramified extension $k(x)/k(t)$ by Remark 2.8(1) (Abhyankar's lemma), the ramification index for g over ∞ is odd as well. Hence so is the ramification index for v at each place in $v^{-1}(\lambda)$. If $|v^{-1}(\lambda)| = 2$, it follows that $\deg(v)$ is even, contradicting $\deg(v) = p_r^\ell$ is odd. Since $|v^{-1}(\lambda)| \leq 2$ by assumption, we get $|v^{-1}(\lambda)| = 1$, and hence v is indeed linearly related over $\overline{k}$ to a polynomial of odd degree.

Lemma 4.4 now shows that v is in fact of prime degree p_r. This implies $|\operatorname{soc}(K)| = p_r$ by Proposition 4.3, and thus the diagonality of K by Remark 2.22.

Henceforth assume g is a polynomial. The argument in the last paragraph applies when $p_r = \deg(f_r)$ is odd, even when g is a polynomial.

We may therefore assume $\{\deg(f_r), \deg(g_s)\} \subseteq \{2, 4\}$ by Proposition 2.17(4). By Lemma 4.4, v is either indecomposable or the composition of two quadratic polynomials. Moreover, if $v = v_1 \circ v_2$ with v_1, v_2 quadratic, then $p_r = \deg(f_r) = 2$ by Lemma 2.18 and the fact that f_r is right-unique by Proposition 2.17(5). In particular, if $\operatorname{Mon}_k(f_r) = S_4$, then v is indecomposable of degree 2 or 4 and hence $\Omega = \Omega'(y, y')$ is a quadratic or biquadratic extension of Ω' for a conjugate y' of y, by Proposition 4.3, parts (2) and (3). Thus in the latter case either $\operatorname{soc}(K) \cong C_2$ or $C_2 \times C_2$ as desired. Hence $\operatorname{soc}(K)$ is diagonal by Lemma 2.19, and hence so is K by Remark 2.22.

Henceforth assume $\operatorname{Mon}_k(f_r) = C_2$, so that $\Omega = \Omega'(y)$ by Proposition 4.3(1). If v is indecomposable and $\operatorname{Mon}_k(g_s) = C_2$ (resp., $\operatorname{Mon}_k(g_s) = S_4$), it further follows that $|K| = |\operatorname{soc}(K)| = [\Omega : \Omega'] = [k(y) : k(v)] = 2$ (resp., $= 4$), and hence K is diagonal by Lemma 2.19 (resp., $K \cong C_2 \times C_2$). Finally assume that $v = v_1 \circ v_2$ is a composition of two quadratics. It then follows that $|K| = |\operatorname{soc}(K)| = [k(y) : k(v)] = 4$ and $K \cong \operatorname{soc}(K) \cong C_2 \times C_2$. Note that in this case $\operatorname{Mon}_k(v) \neq C_4$ by Proposition 2.17(2), and hence $\operatorname{Mon}_k(v) = D_4$. □

5. The solvable case of Theorem 1.1

Let k be a field of characteristic 0. In this section, we focus on the solvable case of Theorem 1.1, while the nonsolvable case is discussed in §6.

Theorem 5.1. *Suppose $f(X) - g(Y) \in k[X, Y]$ is reducible for $f, g \in k[X] \setminus k$ with solvable monodromy groups. Then either 1) $f = h \circ f_1, g = h \circ g_1$ have a nontrivial common left composition factor $h \in k[X]$, $\deg(h) \geq 2$ for some $f_1, g_1 \in k[X] \setminus k$; or 2) $f = (\mu \circ D_{4,\alpha}) \circ f_1$ and $g = (\mu \circ (-\frac{1}{4} D_{4,2\alpha})) \circ g_1$, for some linear $\mu \in k[X]$ and $\alpha \in k$.*

We shall need the following lemmas which impose restrictions on the right-most composition factors of a polynomial whose monodromy group has a "diagonal kernel property" in the sense of Section 4.

Lemma 5.2. *Let $f = h \circ f_{r-1} \circ f_r \in k[X]$ be such that f_r, f_{r-1} are indecomposable of solvable monodromy, $q := \deg(f_r)$ is prime, and $f_{r-1} \circ f_r$ is either strongly-unique or has monodromy group D_4. Let $p := \deg(f_{r-1})$ and $K := \ker(\operatorname{Mon}_k(f) \to \operatorname{Mon}_k(h \circ f_{r-1}))$. If $(q, p) \neq (2, 4)$, then $|K|$ is divisible by q^{p-2}. If moreover $q \neq p$ are distinct primes, then $|K|$ is even divisible by q^p. In particular, if K is diagonal or $K \cong C_2 \times C_2$, then $(q, p) \in \{(2, 2), (3, 3), (2, 4)\}$.*

Proof. Set $G := \operatorname{Mon}_k(f)$, let $N := \ker(G \to \operatorname{Mon}_k(h)) \leq (\operatorname{Mon}_k(f_{r-1} \circ f_r))^{\deg(h)}$, and let N_0 be the normal subgroup of G generated by $I_\infty \cap N$, where $I_\infty \leq G$ is an inertia group at $t \mapsto \infty$. Write $\overline{N}_0$ for the image of N_0 under projection to a component. Note that $\overline{N}_0$ is a normal subgroup of $\operatorname{Mon}_k(f_{r-1} \circ f_r)$ containing a cyclic transitive subgroup, namely the projection of $I_\infty \cap N$. Let $K_2 = \ker(\operatorname{Mon}_k(f_{r-1} \circ f_r) \to \operatorname{Mon}_k(f_{r-1}))$.

We distinguish the following three cases:

1) p a prime different from q. Let $\overline{K \cap N_0} \leq \overline{N}_0$ be the image of $K \cap N_0$ on a component. Then $\overline{N}_0/\overline{K \cap N_0}$ is a quotient of $N_0/(K \cap N_0)$, which by Corollary 2.20, is a subdirect power of $\overline{N}_0/(K_2 \cap \overline{N}_0) = C_p$. On the other hand, since $\gcd(q,p) = 1$, Corollary 3.2(2) implies that $|\overline{N}_0|$ is divisible by q^p. This is only possible if $|\overline{K \cap N_0}|$, and a fortiori $|K|$, is also divisible by q^p. In particular, K cannot be diagonal, nor $C_2 \times C_2$ if $q = 2$, as $p \geq 3$.

2) $p = q > 3$. As above, $\overline{N}_0/\overline{K \cap N_0}$ is a quotient of a subdirect power of $C_p = C_q$, and hence must be abelian. On the other hand, by Corollary 3.2(1), $\ker(\overline{N}_0 \to C_p) = K_2 \cap \overline{N}_0$ contains $I_q(q)$, the unique codimension-1 submodule of the C_q-module $\mathbb{F}_q^q$. Since the only quotient module of $I_q(q)$ with trivial C_q-action is the one-dimensional one, it follows that the q-Sylow subgroup of $(K_2 \cap \overline{N}_0)/(\overline{K \cap N_0})$ is of order dividing q, and thus $|\overline{K \cap N_0}|$, and a fortiori $|K|$, is divisible by $\frac{1}{q} \cdot |I_q(q)| = q^{q-2}$. In particular, K cannot be diagonal since $q > 3$.

3) $p = 4$ and $q \neq 2$. Then, by Corollary 3.2(1), $\ker(\overline{N}_0 \to S_4)$ contains a submodule $V \cong C_q^3$. However, $\overline{N}_0/\overline{K \cap N_0}$ is again a quotient of a subdirect power of S_4. For $q \geq 5$, since q is coprime to $|S_4|$, this implies that $|K|$ is divisible by q^3. For $q = 3$, note that the above forces $\overline{N}_0/\overline{K \cap N_0}$ to have an abelian 3-Sylow group. Since the action of a 3-cycle in S_4 on a two-dimensional quotient of V would be nontrivial, this implies that the quotient $V/(\overline{K} \cap V)$ is at most one-dimensional. Therefore $|\overline{K \cap N_0}|$, and a fortiori $|K|$, is divisible by q^2. In total, $|K|$ is divisible by q^{p-2} for all $q \geq 3$, and K is not diagonal. □

We shall also need the following lemma for exceptional compositions of three factors.

Lemma 5.3. *Suppose $f = h \circ f_{r-2} \circ f_{r-1} \circ f_r$ for indecomposable $f_i \in k[X]$ with cyclic $\mathrm{Mon}_{\overline{k}}(f_r) = C_q$ and solvable $\mathrm{Mon}_k(f_{r-2} \circ f_{r-1})$. Set $p := \deg(f_{r-1})$ and $m := \deg(f_{r-2})$. Assume $f_{r-2} \circ f_{r-1}$ is right-unique, $f_{r-1} \circ f_r$ is either strongly-unique or has monodromy group $\mathrm{Mon}_k(f_{r-1} \circ f_r) = D_4$, and either: (1) $p = q$ or, (2) $q = 2, p = 4$, and $\mathrm{Mon}_k(f_{r-1} \circ f_r) \ncong \mathrm{GL}_2(3)$. If $K := \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(h \circ f_{r-2} \circ f_{r-1}))$ is diagonal or $K \cong C_2 \times C_2$, then $f_{r-2} \circ f_{r-1} \circ f_r$ is of degree 8 or 16.*

For the reader who wishes to skip the details of low-degree computation, we indicated throughout the proof when these were also verified using Magma.

Proof. Let N, K, K_3 be the kernels of the morphisms $\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(h)$, $\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(h \circ f_{r-2} \circ f_{r-1})$, and $\mathrm{Mon}_k(f_{r-2} \circ f_{r-1} \circ f_r) \to \mathrm{Mon}_k(f_{r-2} \circ f_{r-1})$, respectively. Let $N_0 \leq N$ be the normal subgroup of $\mathrm{Mon}_k(f)$ generated by $I_\infty \cap N$, where I_∞ is an inertia group at ∞. Let $\overline{N}_0, \overline{K}$ denote the images of N_0, K in $G_3 = \mathrm{Mon}_k(f_{r-2} \circ f_{r-1} \circ f_r)$, respectively, so that $\overline{N}_0$ contains a cyclic transitive subgroup as in Lemma 5.2. Note that $N_0/(K \cap N_0)$ is a subdirect power of $\overline{N}_0/(K_3 \cap \overline{N}_0)$ by Corollary 2.20.

(1) Assume $p = q$. We first prove the assertion in the case where $m \neq q$ is prime. Since the inertia subgroup over ∞ in $\mathrm{Mon}_k(f_{r-2}) \leq \mathrm{AGL}_1(m)$ is cyclic of order m and $\overline{K} \leq K_3$, the image of N_0 in $\mathrm{Mon}_k(f_{r-2})$ is also cyclic of order m. Thus, $\overline{N}_0/(K_3 \cap \overline{N}_0)$ has an elementary abelian q-Sylow subgroup. As $\overline{N}_0/\overline{K \cap N_0}$ is a quotient of a subdirect power of it, its q-Sylow is elementary abelian as well.

Let $I_q(q)$ and D denote the augmentation and diagonal submodules of $\mathbb{F}_q[C_q]$, respectively, with respect to the action of the q-cycle in $\mathrm{Mon}_k(f_{r-1}) \supseteq C_q$. Since $\overline{N}_0/(K_3 \cap \overline{N}_0)$ contains an (mq)-cycle, it contains the full socle C_q^m of $\mathrm{Mon}_k(f_{r-1})^m$ by Corollary 3.2(2). Since $f_{r-2} \circ f_{r-1}$ is strongly-unique (as $m \neq p$) and $f_{r-1} \circ f_r$ is either strongly-unique or has monodromy group D_4, Proposition 3.3(3) shows that the q-Sylow subgroup Q of $K_3 \cap \overline{N}_0$ contains an index-q subgroup of $I_q(q)^m$. If $q \geq 3$, we claim that the action of $C_q^m \leq \overline{N}_0/(K_3 \cap \overline{N}_0)$ on $Q/(\overline{K} \cap Q) \leq (K_3 \cap \overline{N}_0)/(\overline{K} \cap \overline{N}_0)$ is nontrivial, contradicting the fact that the q-Sylow subgroup of $\overline{N_0/K \cap N_0}$, and hence a fortiori the one of $\overline{N}_0/\overline{K} \cap \overline{N_0}$ is abelian. To see the claim, let $\sigma \in \overline{N}_0$ be a lift of the generator $\overline{\sigma}$ of some component C_q of C_q^m, and $\Delta \subset \{1, \dots, mq\}$ the support of $\overline{\sigma}$ (of size q). Since the projection of $Q \trianglelefteq \overline{N}_0$ to Δ must equal $I_q(q)$, there exists $x \in Q$ whose projection to Δ is nondiagonal. Then $[x, \sigma] \in Q$ is not supported outside of Δ, but is nontrivial in Δ, and thus $[x, \sigma]$ cannot lie in the diagonal $\overline{K}$, showing that σ acts nontrivially on $Q/(\overline{K} \cap Q)$.

If $q = 2$, then the subgroup $\overline{N}_0(2)^2$, generated by squares in the 2-Sylow subgroup $\overline{N}_0(2)$ of $\overline{N}_0$, contains C_2^m by Proposition 3.3(3), hence $\overline{N}_0(2)^2/(\overline{K} \cap \overline{N}_0(2)^2)$ is nontrivial as $m \geq 3$, contradicting the fact that the 2-Sylow subgroup of $\overline{N}_0/(\overline{K} \cap \overline{N}_0)$ is elementary abelian.

Assume now that $m = 4$ or $m = q$. Note that due to Lemma 5.2 and since we avoid degree 8 or 16 maps, we reduce to the case $q = 3$. Note that this case was also verified using Magma. Assume first that, additionally, $f_{r-2} \circ f_{r-1}$ is even strongly-unique. We may then invoke Proposition 3.3(3) (for $m = 3$) or 3.3(4) (for $m = 4$), which shows that $K_3 \cap \overline{N}_0$ contains a subgroup C_3^5. It thus follows [13] from Corollary 2.25 that the 3-Sylow group of $\overline{N}_0$ is of nilpotency class ≥ 5, and hence that the nilpotency class of its quotient by the diagonal subgroup $\overline{K}$ is ≥ 4. On the other hand, the 3-Sylow group of $\overline{N}_0/(K_3 \cap \overline{N}_0) \leq S_3 \wr S_4$ is of class at most 3, a contradiction.

Assume finally that $f_{r-2} \circ f_{r-1}$ is right-unique but not strongly-unique. By definition, this is only possible for $m = q$, and in this case, $\mathrm{Mon}_k(f_{r-2} \circ f_{r-1}) \leq \mathrm{AGL}_1(q^2)$, i.e., $f_{r-2} \circ f_{r-1}$ is linearly related over $\overline{k}$ to T_{q^2} or X^{q^2}. But then $\ker(\mathrm{Mon}_k(f_{r-2} \circ f_{r-1} \circ f_r) \to \mathrm{Mon}_k(f_{r-2} \circ f_{r-1}))$ contains the full group $C_q^{q^2}$ by [BKN26, Proposition 6.1 and Remark 6.2], and thus $K_3 \cap \overline{N}_0 \supseteq C_q^{q^2-1}$ by Corollary 2.24. This again yields an immediate contradiction to the fact that $N_0/(K \cap N_0)$ is a subdirect power of $\overline{N}_0/(K_3 \cap \overline{N}_0) = C_{q^2}$.

(2) Assume $q = 2, p = 4$, and $\mathrm{Mon}_k(f_{r-1} \circ f_r) \ncong \mathrm{GL}_2(3)$. First assume that m is an odd prime. As above, the projection of $\overline{N}_0$ to $\mathrm{Mon}_k(f_{r-2})$ is C_m. Since the image of the action of $\overline{N}_0/(K_3 \cap \overline{N}_0)$ in $\mathrm{Mon}_k(f_{r-1})$ is normal and contains a 4-cycle (generating an inertia group over ∞), this image must be the full group $\mathrm{Mon}_k(f_{r-1}) = S_4$. Hence a 2-Sylow subgroup P_2 of $\overline{N}_0/(K_3 \cap \overline{N}_0)$ has nilpotency class 2. Let $I_4(2) \leq C_2 \wr S_4$ denote the S_4-invariant subgroup of C_2^4 consisting of elements which sum to 0. Then $\overline{N}_0 \supseteq I_4(2)^m$ by Proposition 3.3(2). Since $[P_2, P_2] \leq \overline{N}_0/(K_3 \cap \overline{N}_0)$ projects to $[D_4, D_4] \neq \{1\}$ on each of the m coordinates, it is supported on all of these coordinates. Since moreover the action

[13] In particular, when $m = 4$, we need to use the restriction of the 3-Sylow subgroup to its orbit of length 27; hence the technical wording of Proposition 3.3(4).

of each component S_4 on $I_4(2)$ is faithful, the commutator (of the lifts to $\overline{N}_0$) of $[P_2, P_2]$ with $I_4(2)^m \leq K_3 \cap \overline{N}_0$ is of 2-rank at least $m \geq 3$. As $\overline{K}$ is of rank ≤ 2, we get that the 2-Sylow subgroup of $\overline{N}_0/\overline{K \cap N_0}$ has nilpotency class > 2. This contradicts the fact that $\overline{N_0}/\overline{K \cap N_0}$ is a quotient of a subdirect power of $\overline{N}_0/(K_3 \cap \overline{N}_0)$, since P_2 is of nilpotency class 2.

Asume finally that $m = 4$. Note that this case is also verified using Magma. Then Proposition 3.3(2) yields that $\overline{N}_0 \supseteq I_4(2)^4 \cong C_2^{12}$. It follows from Corollary 2.25 that the 2-Sylow subgroup of $\overline{N}_0$ is of nilpotency class at least 12, and thus that the 2-Sylow group of $\overline{N}_0/\overline{K \cap N_0}$ still has nilpotency class at least 10. However, the 2-Sylow group $C_2 \wr C_2 \wr C_2 \wr C_2$ of $S_4 \wr S_4$ has nilpotency class 8, again contradicting the fact that $\overline{N}_0/\overline{K \cap N_0}$ is a quotient of a subdirect power of $\overline{N}_0/(K_3 \cap \overline{N}_0) \leq S_4 \wr S_4$. □

Proof of Theorem 5.1. By possibly replacing f, g by left factors of theirs, we may assume that f, g is a minimally reducible pair. Hence $f(X) - t$ and $g(X) - t$ have the same Galois closure over $k(t)$ by Lemma 2.13 and $\deg(f) = \deg(g)$ by Corollary 2.15. Set $n := \deg(f)$ and write $f = f_1 \circ \cdots \circ f_r$ for indecomposable $f_i \in k[X]$. For $r = 1$, either n is prime or $n = 4$ by Proposition 2.1. The claim then follows from Lemma 2.3 when n is prime and since index-4 subgroups are conjugate in S_4 when $n = 4$.

Henceforth assume $r \geq 2$. By Proposition 2.17, f_r is right-unique, and moreover $f_{r-1} \circ f_r$ is either strongly-unique or $\mathrm{Mon}_k(f_{r-1} \circ f_r) = D_4$. Set $p_i := \deg(f_i)$ so that p_i is either prime or 4 by Proposition 2.1.

By Theorem 4.1, the kernel K of the projection $\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{r-1})$ is either diagonal, or has socle $C_2 \times C_2$. In the following, we claim that this implies $r \geq 3$ and that $f_{r-2} \circ f_{r-1} \circ f_r$ is either a composition of three quadratic maps, or $\deg(f_r) = 2$ and $\deg(f_{r-2} \circ f_{r-1}) = 8$. We argue for f but the same argument applies to g.

When $r = 2$, since K is diagonal or has socle $C_2 \times C_2$, since f_2 is right-unique, and since $f = f_1 \circ f_2$ is strongly unique or $\mathrm{Mon}_k(f) = D_4$, Theorem 3.1 implies that either ($p_1 = p_2 = 2$ and $\mathrm{Mon}_k(f) = D_4$) or ($p_2 = 2$, $p_1 = 4$ and $\mathrm{Mon}_k(f) = \mathrm{GL}_2(3)$). The former case implies that $(\mu \circ f \circ \eta_1, \mu \circ g \circ \eta_2) = (D_{4,\alpha}, -\frac{1}{4} D_{4,2\alpha})$ for $\mu, \eta_1, \eta_2 \in k[X]$ of degree 1 and $\alpha \in k$; see Example 2.16. The latter case cannot occur as a direct consideration[14] or Magma computation show.

Henceforth assume $r \geq 3$. Due to Proposition 2.17(1),(2) and Lemma 5.2, we either have $p_r = 4$ or $(p_r, p_{r-1}) \in \{(2,2), (3,3), (2,4)\}$.

Assume first that $\mathrm{Mon}_{\overline{k}}(f_r)$ is noncyclic. In this case, we are left to consider the cases $p_r = 4$, or ($\mathrm{Mon}_{\overline{k}}(f_r) = S_3$ and $p_{r-1} = 3$). Let $\overline{G} = \mathrm{Mon}_k(f_{r-1} \circ f_r)$ and $\overline{K} = \ker(\overline{G} \to \mathrm{Mon}_k(f_{r-1}))$. Since f_r is right-unique, it follows from Corollary 3.2(3) that $\overline{G}$ contains $\mathrm{soc}(\overline{K}) = V_4^{p_{r-1}}$ in case $p_r = 4$, (resp. $C_{p_r}^{p_{r-1}}$ otherwise), as a minimal normal subgroup. In particular, the image of $\mathrm{soc}(K)$ in $\mathrm{soc}(\overline{K})$ is therefore the full subgroup, and hence has rank ≥ 3, contradicting that the assumption that $\mathrm{soc}(K)$ is diagonal or $C_2 \times C_2$.

[14] E.g., any faithful transitive degree-8 action of $\mathrm{GL}_2(3)$ must have stabilizer of order 6 intersecting the center trivially; but all such subgroups project to conjugate subgroups $S_3 \leq S_4$, implying that a corresponding reducible pair (f, g) must have a pair of reducible left factors of degree 4.

Henceforth we assume $\mathrm{Mon}_{\overline{k}}(f_r) \cong C_{p_r}$ is cyclic. Recall that in this case we are reduced to considering $p_{r-1} = p_r \in \{2, 3\}$ or $(p_r, p_{r-1}) = (2, 4)$. If $f_{r-2} \circ f_{r-1}$ admits a Ritt move, then p_{r-2} and p_{r-1} are coprime by Corollary 2.10, hence so are p_{r-2} and p_r and we may apply the Ritt move to replace f_{r-1} by a factor of degree coprime to p_r. This case has already been treated above using Lemma 5.2. Hence we may assume $f_{r-2} \circ f_{r-1}$ is right-unique, and in particular that $f_{r-2} \circ f_{r-1} \circ f_r$ is of degree 8 or 16 if $\overline{G} = D_4$ (by Lemma 5.3). If $\overline{G} \neq D_4$, as noted above, $f_{r-1} \circ f_r$ is a strongly-unique decomposition. Thus, if $\overline{G} \ncong \mathrm{GL}_2(3)$, we may apply Lemma 5.3 to deduce that $f_{r-2} \circ f_{r-1} \circ f_r$ is again of degree 8 or 16.

Consider therefore finally the case $\overline{G} = \mathrm{GL}_2(3)$. Denote by $Q_8 \lhd \overline{G}$ the quaternion subgroup of $\overline{G}$, and let $M = \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{r-2})) \cap Q_8^{p_1 \cdots p_{r-2}} \lhd \mathrm{Mon}_k(f)$. Since $f_{r-2} \circ f_{r-1}$ is strongly-unique, it follows from Corollary 3.2(3) that $\mathrm{Mon}_k(f_{r-2} \circ f_{r-1})$ contains $V_4^{p_{r-2}}$ as a minimal normal subgroup, and hence the image of M in $\mathrm{Mon}_k(f_{r-2} \circ f_{r-1})$ equals $V_4^{p_{r-2}}$. Restricting the central extension $\pi : \mathrm{GL}_2(3) \to S_4$ to $\pi^{-1}(V_4) = Q_8 \to V_4$ one obtains a Frattini extension, forcing the image $\overline{M}$ of M in $G_3 := \mathrm{Mon}_k(f_{r-2} \circ f_{r-1} \circ f_r)$ to contain $Q_8^{p_{r-2}}$. Due to Corollary 2.20 (applied with $f_{r-2} \circ f_{r-1}$ in the role of f_2), M/K is a subdirect power of the image of M in $\mathrm{Mon}_k(f_{r-2} \circ f_{r-1})$, and hence a subdirect power of V_4. In particular, M/K, and a fortiori $\overline{M}/\overline{K}$, is elementary-abelian. But this enforces $\overline{K} = Z(Q_8)^{p_{r-2}}$, contradicting that K is diagonal or $C_2 \times C_2$ as soon as $p_{r-2} > 2$. This once again leaves only the degree-16 option $p_r = p_{r-2} = 2$, $p_{r-1} = 4$.

As the same argument applies to g, the right factors $f_{r-2} \circ f_{r-1} \circ f_r$ and $g_{s-2} \circ g_{s-1} \circ g_s$ of f and g, respectively, fulfill $\deg(f_r) = \deg(g_s) = 2$ and $\deg(f_{r-2} \circ f_{r-1}), \deg(g_{s-2} \circ g_{s-1}) \in \{4, 8\}$. The assertion therefore follows from the following Proposition 5.4. □

Proposition 5.4. *Suppose that $f, g \in k[X]$ are of the form $f = f_0 \circ u$, $g = g_0 \circ v$ such that $u = u_1 \circ u_2$ and $v = v_1 \circ v_2$ with $\deg(u_2) = \deg(v_2) = 2$ and each of u_1, v_1 of degree 4 or 8 with solvable monodromy. Then f, g are not minimally reducible.*

Lemma 5.5. *Suppose $f \in k[X]$ is of prime power degree, $\mathrm{Mon}_k(f)$ is solvable, and x a root of $f(X) - t \in k(t)[X]$. Let $L/k(t)$ be a field in which ∞ is unramified. Then the lattice of intermediate fields in $k(x)/k(t)$ is in one-to-one correspondence with that of $L(x)/L$ via the map $M \to ML$ given by compositum with L in the Galois closure of $L(x)/k(t)$.*

Proof. Suppose $\deg(f) = p^n$ for a prime p and integer $n \in \mathbb{N}$. Note, since $\mathrm{Mon}_k(f)$ is solvable, f is either a composition of degree-p polynomials, or $p = 2$ and degree-4 indecomposable polynomials also occur, by Proposition 2.1. The places of L lying over ∞ are totally ramified in $L(x)$ by Remark 2.8. Since $[L(x) : L] = p^n$ is a prime power, this implies the intermediate fields of $L(x)/L$ are totally ordered by Lemma 2.12.

If f is a composition of degree-p polynomials, the extension $k(x)/k(t)$ contains a maximal chain of degree-p extensions. Since these fields are linearly disjoint from $L/k(t)$, their compositum induces a maximal chain of degree-p extensions in $L(x)/L$. Since the intermediate fields in $L(x)/L$ are totally ordered the assertion follows.

Otherwise, $k(x)/k(t)$ has an intermediate degree-4 subextension $k(x')/k(t')$ with no intermediate fields. Letting Ω'_x, Ω' be the Galois closures of $k(x')/k(t')$, $L(t')/k(t)$, respectively, we have $\mathrm{Gal}(\Omega'_x/k(t')) = S_4$ by Proposition 2.1. Since ∞ is unramified in $\Omega'/k(t')$ by Remark 2.8, we see that $\mathrm{Gal}(\Omega'_x\Omega'/\Omega') = S_4$ as well by Lemma 2.7(2). It follows that the degree-4 extension $L(x')/L(t')$ has no nontrivial intermediate fields since such a field would yield a nontrivial intermediate field of $\Omega'(x')/\Omega'$. Thus, the same argument as for degree-p compositions yields that the composition of L with the maximal chain of intermediate fields in $k(x)/k(t)$ gives the maximal chain of intermediate fields of $L(x)/L$. □

Proof of Proposition 5.4. Assume on the contrary f, g is a minimally reducible pair, and let x, y be roots of $f(X) - t, g(X) - t \in k(t)[X]$, respectively. Set $u = u(x)$, $v = v(y)$, and let Ω_x, Ω_y and Ω' denote the Galois closures of $k(x)/k(u)$, $k(y)/k(v)$, and $k(u, v)/k(t)$, respectively. By the minimal reducibility assumption $k(x, v)$ and $k(u, y)$ are not linearly disjoint over $k(u, v)$, and hence admit intermediate extensions $k(u, v) \lneq F_1 \leq k(x, v)$ and $k(u, v) \lneq F_2 \leq k(y, u)$ which are not linearly disjoint and admit the same Galois closure by Lemma 2.13.

Assume first $n := \deg(u) = \deg(v)$, so that $k(u, v)/k(u)$ is unramified over ∞ by Remark 2.8(1). Then the extension $F_1/k(u, v)$ is defined over $k(u)$ by Lemma 5.5, that is, there exists $k(u) \lneq k(x') \leq k(x)$ which is linearly disjoint from $k(u, v)/k(u)$ such that $k(x', v) = F_1$. If F_1 is a proper subfield of $k(x, v)$, already the extensions $k(x'), k(y)$ are not linearly disjoint over $k(t)$ by the above claim, contradicting minimal reducibility. Hence we may assume $F_1 = k(x, v)$ and similarly $F_2 = k(u, y)$, so that these extensions of $k(u, v)$ have the same Galois closure Ω_c. Set $H := \mathrm{Gal}(\Omega_c/k(u, v))$.

Since $k(u, v)$ and $k(x)$ are linearly disjoint over $k(u)$ by minimal reducibility, $\Omega_x(v)$ coincides with the Galois closure Ω_c of $k(x, v)/k(u, v)$ and hence H can be viewed as a transitive subgroup of $\mathrm{Mon}_k(u) = \mathrm{Gal}(\Omega_x/k(u))$ via restriction. Similarly, H can be viewed as a transitive subgroup of $\mathrm{Mon}_k(v)$. Moreover, H contains a cyclic transitive subgroup (in both actions) due to ramification over ∞, as noted above. Let $H_x, H_y \leq H$ be the point stabilizers in the two actions, so that H_x acts intransitively on H/H_y. By running in Magma over transitive groups H (containing a cyclic transitive group) of degree 8 (resp., 16) in two actions, on H/H_x and H/H_y, we see that if H_x is intransitive on H/H_y, then there are overgroups $H_x \leq H'_x \leq H$ and $H_y \leq H'_y \leq H$ such that at least one of them is a proper subgroup of H, and H'_x is intransitive on H/H'_y, contradicting the minimal reducibility assumption once more.

Now assume u, v are of distinct degrees, and without loss of generality $\deg(u) = 16$, $\deg(v) = 8$. We may and will furthermore assume that u has an indecomposable left factor u_0 of monodromy group S_4, since in case $u_1 = u_0 \circ u'_1$ with $\deg(u_0) = 2$, we may simply reduce to the case $\deg(u) = \deg(v)$ via replacing u by $u'_1 \circ u_2$. Setting $H = \mathrm{Gal}(\Omega_x(v)/k(u, v))$ and $N := \mathrm{Gal}(\Omega_x\Omega'/\Omega')$, we identify H as a subgroup of $\mathrm{Mon}_k(u)$ and N as a subgroup of H, via restriction. Note that H is a transitive since $k(u, v)/k(u)$ and $k(x)/k(u)$ are linearly disjoint by minimal reducibility, Also note that $N \lhd \mathrm{Mon}_k(u)$, and that N contains the normal subgroup of $\mathrm{Mon}_k(u)$ generated by the inertia groups $I \leq N$ over ∞. One has $\#I = 8$ since I contains the square of a full cycle by Remark 2.8.

We first claim that there exists a unique proper maximal subfield $k(u,v) \lneq F_1 \lneq k(x,v)$, and it is defined over $k(u)$. We give a direct argument to show this, and note that the underlying group theoretic statement is also verified directly with Magma. Let $U < \mathrm{Mon}_k(u)$ denote a point stabilizer. Note that, since $\mathrm{Mon}_k(u_0) = S_4$ and (the order-8 cyclic group) I maps to the subgroup of S_4 generated by a double transposition, the 2-Sylow group N_2 of N is transitive and projects to $V_4 \lhd S_4$ under the map $\mathrm{Mon}_k(u) \to \mathrm{Mon}_k(u_0)$. Moreover, since all elements of $V_4 \setminus \{id\}$ are conjugate in S_4, the group N_2 has a quotient $C_2 \times C_2$ all of whose nonidentity elements lift to an order-8 element in N. In particular, any maximal subgroup M of the 2-group N_2 must contain at least one conjugate of a generator of I, i.e., an element of order 8. Letting $U \cap N_2 \subsetneq M \subsetneq N_2$ be the stabilizer of a maximal block Δ of N_2 in its action as a transitive subgroup of $\mathrm{Mon}_k(u)$, this implies that all stabilizers of blocks of N_2 which are contained in Δ must be totally ordered by inclusion, by Lemma 2.12 (as places over ∞ are totally ramified in the corresponding extension). Since intersections of blocks are again blocks, this implies that N_2 stabilizes a unique block system of each block length 2 and 4. In particular, since $N_2 \leq H \leq \mathrm{Mon}_k(u)$, every block of these groups is a block of N_2, and hence H and $\mathrm{Mon}_k(u)$ have unique minimal block systems. Since u has a quadratic right factor u_2, the size of such a minimal block of $\mathrm{Mon}_k(u)$ and H must equal $\deg(u_2) = 2$. In particular, there exists a unique minimal intermediate group $U \cap H \lneq U' \lneq H$ in H, and U' is the intersection with H of the minimal block stabilizer UU' in $\mathrm{Mon}_k(u)$ fixing a root of u_2. Thus, letting F_1 be the fixed field of U', the claim follows from the usual Galois correspondence.

It follows that if a proper subfield of $k(x,v)$ is not linearly disjoint from $k(u,y)$ over $k(u,v)$, then so is F_1. However, as $F_1/k(u,v)$ is defined over $k(u)$, this contradicts the minimal reducibility assumption. Thus, $k(x,v)/k(u,v)$ has the same Galois closure Ω_c as $F_2/k(u,v)$ for some subfield $F_2 \leq k(u,y)$ by Lemma 2.13. Letting $V = \mathrm{Gal}(\Omega_c/F_2)$, we obtain a faithful transitive action of H and hence of $N_2 \subseteq H$ on H/V. It is an action of degree dividing 8. But now let $\tilde{M} \subset N_2$ be the stabilizer of a maximal block in this action. This contradicts that $\tilde{M}$ contains an element of order 8 as shown above. Thus there exists no minimal reducible pair f, g as desired. □

Remark 5.6. While not strictly required for the proof of any of the theorems, it may be of interest for related applications to give a precise list of possible monodromy groups $G_3 := \mathrm{Mon}_{\overline{k}}(f_{r-2} \circ f_{r-1} \circ f_r)$ such that $\ker(\mathrm{Mon}_k(h \circ f_{r-2} \circ f_{r-1} \circ f_r) \to \mathrm{Mon}_k(h \circ f_{r-2} \circ f_{r-1}))$ can be diagonal or isomorphic to $C_2 \times C_2$ for some $h \in k[X] \setminus k$.

Lemma 5.3 and the proof of Theorem 5.1 show that all such examples fulfill

$$(\deg(f_r), \deg(f_{r-1}), \deg(f_{r-2})) \in \{(2,2,2), (2,2,4), (2,4,2)\}.$$

We then use Magma (in particular the database of transitive groups of degrees 8 and 16) to run over quotients $\overline{N}/\overline{K}$ of normal subgroups $\overline{N} \lhd G_3$ containing a full cycle by subgroups $\overline{K} \leq \overline{N}$ isomorphic to C_2 or $C_2 \times C_2$, and keep track of cases in which the nilpotency class of the q-Sylow subgroup of $\overline{N}/\overline{K}$ is at most as large as that of the q-Sylow of $\overline{N}/(K_3 \cap \overline{N})$, where $K_3 = \ker(G_3 \to \mathrm{Mon}_k(f_{r-2} \circ f_{r-1}))$. This gives a reasonably short list of possible groups G_3, of which some can furthermore be excluded on the ground of not possessing

a polynomial genus-0 system. This leaves only the monodromy groups G_3 of Id $8T\theta$ for $\theta \in \{6, 27, 28, 35\}$, and $16T\theta$ for $\theta \in \{773, 1499, 1651, 1832, 1866, 1871, 1872, 1886\}$. Thus, except for these groups, we obtain a contradiction to the fact that $\overline{N}/\overline{K}$ is a quotient of a subdirect power of $\overline{N}/(K_3 \cap \overline{N})$.

In particular, there are no such examples of odd degree.

We similarly obtain the following intermediate result on not necessarily polynomial reducible pairs with solvable monodromy group.

Theorem 5.7. *Let $f \in k[X] \setminus k$ be a polynomial of odd degree with solvable monodromy group, and let $g \in k(Y) \setminus k$ be a Siegel function of degree at least 2. Then $f(X) = g(Y)$ is reducible if and only if f and g have a nontrivial common left composition factor, that is, $f = h \circ f_1$ and $g = h \circ g_1$ for some $h, f_1 \in k[X]$ and $g_1 \in k(X)$ such that $\deg(h) > 1$.*

Proof. By possibly replacing f, g by left factors of theirs, we may assume it is a minimally reducible pair. Now write $f = f_1 \circ \cdots \circ f_r$ for indecomposable polynomials $f_i \in k[X]$. Since f is assumed to be solvable of odd degree, $p_i = \deg(f_i)$ is prime for all $i = 1, \dots, r$ by Proposition 2.1. Then, Theorem 4.1 implies that the socle of $K = \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{r-1}))$ is either C_{p_r} (with $p_r = \deg(f_r)$) or $C_2 \times C_2$.

Assume that $r \geq 2$. Pick roots x and y of $f(X) - t = 0$ and $g(Y) - t = 0$, respectively. By Lemma 2.13, the extensions $k(x)/k(t)$ and $k(y)/k(t)$ have a common Galois closure Ω. Since $\deg(f_{r-1} \circ f_r)$ is not divisible by 4, Proposition 2.17(1) implies $f_{r-1} \circ f_r$ is not linearly related to $X^{p_r p_{r-1}}$ or $T_{p_r p_{r-1}}$ over $\overline{k}$, and thus is strongly-unique by Ritt's theorems. Lemma 5.2 thus already forces $p_r = p_{r-1} = 3$, and this possibility is furthermore ruled out in the proof of Theorem 5.1, as in Remark 5.6.

Thus we get $r = 1$. In such case $\mathrm{Mon}_k(f) \leq \mathrm{AGL}_1(p_1)$ and hence $k(y)$ contains a root of $f(X) - t$ by Lemma 2.3, so that g factors through f as needed. □

6. Proofs of main results

6.1. **DLS over general fields.** Let k be a field of characteristic 0. Theorem 1.1 is the special case $k = \mathbb{C}$ of the following theorem. Recall that $D_{n,\alpha}$ denote the n-th Dickson polynomial with parameter $\alpha \in k$.

Theorem 6.1. *Let $f, g \in k[X]$ be polynomials of degree > 1. Then $f(X) - g(Y)$ is reducible in $k[X, Y]$ if and only if one of the following occurs for some polynomials $f_1, g_1 \in k[X]$:*

1. *f and g have a common left composition factor $h \in k[X]$ of degree at least 2, that is, $f = h \circ f_1$ and $g = h \circ g_1$;*
2. *$f = (\mu \circ h_1 \circ \lambda) \circ f_1$ and $g = (\mu \circ h_2 \circ \lambda) \circ g_1$, for some linear $\mu, \lambda \in \overline{k}[X]$, where (h_1, h_2) is one of the pairs of polynomials of degrees 7,11,13,15,21,31 given in* [CNC99, §5].
3. *$f = (\mu \circ D_{4,\alpha}) \circ f_1$ and $g = (\mu \circ (-\frac{1}{4} D_{4,2\alpha})) \circ g_1$, for some linear $\mu \in k[X]$ and $\alpha \in k$.*

Note that when $k = \overline{k}$ is algebraically closed, the case $\alpha = 0$ in (3) falls into Case (1), whereas all cases with $\alpha \neq 0$ can be expressed as $\{f, g\} = \{(\mu \circ T_4) \circ f_1, \mu \circ (-T_4) \circ g_1\}$.

Remark 6.2. For the converse direction of Theorem 6.1, it is straightforward to see that (1) implies the reducibility of $f(X) - g(Y) \in k[X, Y]$. For (3), reducibility follows from

(2.1). For (2), since $\mathrm{Mon}_k(\mu\circ h_i\circ\lambda)=\mathrm{Mon}_{\overline{k}}(\mu\circ h_i\circ\lambda)$, reducibility over k is equivalent to that over $\overline{k}$ since these are equivalent to the intransitivity in one action of the stabilizer in the other action. Thus, in this case the reducibility over k follows from the reducibility of $h_1(X)-h_2(Y)\in\overline{k}[X,Y]$, whose factorizations are given in [CNC99, Section 5].

For maps with nonsolvable monodromy, we take a simpler approach based on [KN24]. The key argument is given by the following lemma. We shall apply this argument to compare the Galois closures of maximal nonsolvable left factors of maps.

Lemma 6.3. *Let $f,g\in k(X)$ be a minimally reducible pair with nonsolvable $\mathrm{Mon}_k(f)$. Write $f=f_1\circ\cdots\circ f_r$, and $g=g_1\circ\cdots\circ g_s$ for indecomposable $f_i,g_j\in k(X)$. Set $\Gamma_i=\mathrm{Mon}_k(f_i)$ (resp., $\Gamma'_j=\mathrm{Mon}_k(g_j)$), $\hat{f}_i:=f_1\circ\cdots\circ f_i$. (resp., $\hat{g}_j=g_1\circ\cdots\circ g_j$), and let Ω_i (resp., Ω'_j) be the splitting field of $\hat{f}_i(X)-t$ (resp., $\hat{g}_j(X)-t$), with $\Omega_0:=\Omega'_0:=k(t)$. Now choose the indices $i\in\{1,\dots,r\}$ and $j\in\{1,\dots,s\}$ maximal such that $\mathrm{Gal}(\Omega_i/\Omega_{i-1})$ and $\mathrm{Gal}(\Omega'_j/\Omega'_{j-1})$ are nonsolvable. Assume that Γ_i has a unique nonabelian minimal normal subgroup $\mathrm{soc}(\Gamma_i)$ and that f_i is a right-unique factor of $\hat{f}_i$. Then the following hold:*

(1) $\Omega'_j\supseteq\Omega_i$ and $\mathrm{soc}(\mathrm{Gal}(\Omega_i/\Omega_{i-1}))\cong\mathrm{soc}(\Gamma_i)^m$ for some $m\geq 1$.

(2) If moreover $f\in k[X]$ is a polynomial, then $\mathrm{soc}(\mathrm{Gal}(\Omega_i/\Omega_{i-1}))$ maps isomorphically to a normal subgroup of a quotient of $\mathrm{Mon}_k(g_j)$.

Remark 6.4. 1) By Lemma 2.13, the minimal reducibility of f,g implies $f(X)-t$ and $g(X)-t$ have the same splitting field Ω over $k(t)$. Beyond this implication, the assumption of reducibility is unnecessary for Assertion (1) of Lemma 6.3.
2) We shall in fact see that j is the minimal index for which $\Omega'_j\supseteq\Omega_i$.
3) The assumption that f is a polynomial is only used to guarantee that $\mathrm{soc}(\Gamma_i)$ is simple and primitive, by Proposition 2.1.

Proof of Lemma 6.3. Let Ω be the splitting field of $f(X)-t$ and $g(X)-t$ over $k(t)$, as in Remark 6.4. Let $\hat{K}:=\mathrm{Gal}(\Omega_i/\Omega_{i-1})=\ker(\mathrm{Mon}_k(\hat{f}_i)\to\mathrm{Mon}_k(\hat{f}_{i-1}))$, $\hat{K}_g:=\mathrm{Gal}(\Omega'_j/\Omega'_{j-1})$, and $K:=\mathrm{soc}(\hat{K})$.
(1) Since $\hat{K}\neq 1$ and f_i is a right-unique factor of $\hat{f}_i$, it follows from [KNR24, Proposition 3.3] that K is the unique minimal normal subgroup of $\mathrm{Mon}_k(\widehat{f_i})$, and that $K\cong\mathrm{soc}(\Gamma_i)^m$ for some $m\geq 1$. Moreover, it is contained as a subdirect power in $\mathrm{soc}(\Gamma_i)^{d_i}$, where $d_i=\deg(\hat{f}_{i-1})$.

Assume on the contrary that Ω'_j does not contain Ω_i. Since K is the unique minimal normal subgroup of $\mathrm{Mon}_k(\hat{f}_i)$, it follows that $\Omega'_j\cap\Omega_i\subseteq\Omega_i^K$. As $\mathrm{soc}(\Gamma_i)$, and hence K, is nonsolvable, $\mathrm{Gal}(\Omega_i/\Omega'_j\cap\Omega_i)$ is also nonsolvable. On the other hand, this group is isomorphic to the quotient $\mathrm{Gal}(\Omega_i\Omega'_j/\Omega'_j)$ of $\mathrm{Gal}(\Omega/\Omega'_j)$, which is solvable, a contradiction. Therefore $\Omega'_j\supseteq\Omega_i$. We moreover note that Ω'_{j-1} does not contain Ω_i as in Remark 6.4. Indeed, since $\hat{K}_g$ is nonsolvable, $\mathrm{Gal}(\Omega/\Omega'_{j-1})$ is nonsolvable as well. As $\mathrm{Gal}(\Omega/\Omega_i)$ is solvable, it follows that Ω'_{j-1} cannot contain Ω_i.
(2) Identifying $U_i:=\mathrm{Gal}(\Omega_i(y_{j-1})/k(y_{j-1}))$ with a subgroup of $\mathrm{Mon}_k(\hat{f}_i)$ via restriction

below, we claim that K is contained in U_i as its unique minimal normal subgroup. For that, let x be a root of $f(X)-t$, let x_i (resp., y_j) be a root of $\widehat{f}_i(X)-t$ (resp., $\widehat{g}_j(X)-t$), and set $x_{i-1}=f_i(x_i)$ (resp., $y_{j-1}=g_j(y_j)$). Moreover, define

$$U=\mathrm{Gal}(\Omega/k(y_{j-1})) \text{ and } U_{i-1}:=\mathrm{Gal}(\Omega_{i-1}(y_{j-1})/k(y_{j-1})).$$

By minimal reducibility of f and g, the extensions $k(y_{j-1})/k(t)$ and $k(x)/k(t)$ are linearly disjoint. The same holds a fortiori for $k(y_{j-1})/k(t)$ with $k(x_i)/k(t)$ and with $k(x_{i-1})/k(t)$. Consequently, U, U_i and U_{i-1} are the Galois groups of the Galois closures of $k(y_{j-1},x)/k(y_{j-1})$, $k(y_{j-1},x_i)/k(y_{j-1})$, and $k(y_{j-1},x_{i-1})/k(y_{j-1})$, respectively, by Remark 2.9. Under restriction, U_i identifies with $\mathrm{Gal}(\Omega_i/k(y_{j-1})\cap\Omega_i)\le \mathrm{Mon}_k(\widehat{f}_i)=\mathrm{Gal}(\Omega_i/k(t))$. Note that via this identifcation $K\le U_i$ since $k(y_{j-1})\cap\Omega_i\subseteq\Omega'_{j-1}\cap\Omega_i\subseteq\Omega_i^K$, where the last inclusion follows from the minimal normality of K and since $\Omega_i\not\subseteq\Omega'_{j-1}$. Moreover, U_{i-1} restricts to a subgroup of $\mathrm{Mon}_k(\widehat{f}_{i-1})=\mathrm{Gal}(\Omega_{i-1}/k(t))$, and since $\Omega_{i-1}\subseteq\Omega_i^K$, we deduce that K in contained in $K_U:=\ker(U_i\to U_{i-1})$.

We now use [KN24] to show that $K=\mathrm{soc}(K_U)=U_i\cap\mathrm{soc}(\Gamma_i)^{d_i}$ is a minimal normal subgroup of U_i. Since $K\subseteq K_U$ and the image of K in each of the Γ_i-components is $\mathrm{soc}(\Gamma_i)$, the Galois group Γ_U of the Galois closure of $k(x_i,y_{j-1})/k(x_{i-1},y_{j-1})$ (which is also the image in Γ_i of a block stabilizer) contains the image of K_U in Γ_i, and hence contains $\mathrm{soc}(\Gamma_i)$. Since $\mathrm{soc}(\Gamma_i)$ is primitive and simple, Γ_U is primitive almost-simple. Thus, viewing U_i as a subgroup of $\Gamma_U\wr U_{i-1}$, Lemma 3.1 and Corollary 3.4 of [KN24] imply that $\mathrm{soc}(K_U)=U_i\cap\mathrm{soc}(\Gamma_i)^{d_i}$ is a minimal normal subgroup of U_i. Since $K\le U_i\cap\mathrm{soc}(\Gamma_i)^{d_i}$ is normal in U_i, we deduce that $K=\mathrm{soc}(K_U)$ is a minimal normal subgroup of U_i. Since K is the unique minimal normal subgroup of $\mathrm{Mon}_k(\hat{f}_i)$, its centralizer is trivial. Thus, there is no other minimal normal subgroup of U_i, proving the claim.

To deduce (2), consider the image of $\pi: U\to\Gamma'_j$, that is, the image of the action of U on the $k(y_{j-1})$-conjugates of y_j. Let $\tilde{K}:=\mathrm{Gal}(\Omega/\Omega_i^K(y_{j-1}))\le U$ be the preimage of $K\le U_i$ and $N:=\mathrm{Gal}(\Omega/\Omega_i(y_{j-1}))$, so that $N\lhd U$ is solvable and $\tilde{K}/N\cong K$. Since N is contained in the kernel of the map $U\to\Gamma'_j/\pi(N)$ and $U_i\cong U/N$, we obtain an induced map $\tilde{\pi}: U_i\to\Gamma'_j/\pi(N)$. We claim that $\tilde{\pi}(K)\neq 1$. Assuming the claim, since K is the unique minimal normal subgroup of U_i, we deduce that K maps isomorphically onto $\tilde{\pi}(K)\cong\pi(\tilde{K})/\pi(N)$. Thus, $\pi(\tilde{K})/\pi(N)$ is the desired normal subgroup of $\Gamma'_j/\pi(N)$, yielding (2).

To show the remaining claim $\tilde{\pi}(K)\neq 1$, assume on the contrary $\pi(\tilde{K})=\pi(N)$. Since N is solvable, so is $\pi(N)=\pi(\tilde{K})$. In particular, the image of the action of $\tilde{K}$ on conjugates of y_j is solvable and hence $\Omega_i\Omega'_{j-1}/\Omega_i^K\Omega'_{j-1}$ has a solvable Galois group. On the other hand since $\Omega'_{j-1}\cap\Omega_i\subseteq\Omega_i^K$, the Galois group of $\Omega_i\Omega'_{j-1}/\Omega_i^K\Omega'_{j-1}$ identifies with K via restriction and hence is nonsolvable, a contradiction. □

The assumptions of Lemma 6.3 can be guaranteed as follows.

Remark 6.5. 1) If f is a polynomial, then a nonsolvable monodromy group $\Gamma_i=\mathrm{Mon}_k(f_i)$ has to be almost-simple by Proposition 2.1. Moreover the right-uniqueness assumption on

f_i may be assumed to hold up to performing Ritt moves.
2) Similarly, if f is a Siegel function with nonsolvable monodromy group such that f does not factor through an indecomposable with *affine* nonsolvable monodromy, then $\Gamma_i = \mathrm{Mon}_k(f_i)$ has a unique nonabelian minimal normal subgroup by Proposition 2.4. The right-uniqueness assumption may be assumed to hold via performing Ritt moves, using the generalization [Pak09, Theorem 1.1] of Ritt's theorem to Siegel functions.

Lemma 6.3 has the following surprising consequence.

Corollary 6.6. *Assume that $f, g \in k[X]$ form a minimally reducible pair. Then there exists a decomposition $f = f_1 \circ h$ of f, where $f_1 \in k[X]$ is indecomposable and $\mathrm{Mon}_k(h)$ is solvable.*

Proof. We may assume that $\mathrm{Mon}_k(f)$ is nonsolvable. Write $f = f_1 \circ \cdots \circ f_r \in k[X]$ and $g = g_1 \circ \cdots \circ g_s$ with all f_i and $g_j \in k[X]$ indecomposable. Let $i \in \{1, \dots, r\}$ (resp., $j \in \{1, \dots, s\}$) be maximal such that $\mathrm{Mon}_k(f_i)$ (resp., $\mathrm{Mon}_k(g_j)$) is nonsolvable. Set $\widehat{f_i} = f_1 \circ \cdots \circ f_i$ and $\widehat{g}_j = g_1 \circ \cdots \circ g_j$. After performing Ritt moves if necessary, we may assume that f_i is a right-unique factor of $\widehat{f_i}$ as in Remark 6.5. It then follows from [KNR24, Corollary 4.4] that $\ker(\mathrm{Mon}_k(\hat{f}_i) \to \mathrm{Mon}_k(\hat{f}_{i-1}))$ has socle $K \cong \Gamma_i^{\deg(\hat{f}_{i-1})}$, where $\Gamma_i := \mathrm{soc}(\mathrm{Mon}_k(f_i))$ is a nonabelian simple group, cf. Proposition 2.1.

On the other hand, by Lemma 6.3, K maps isomorphically to a normal subgroup of a quotient of $\mathrm{Mon}_k(g_j)$. Since $\mathrm{Mon}_k(g_j)$ is nonsolvable and hence almost-simple by Proposition 2.1, it follows that $\deg(\hat{f}_{i-1}) = 1$, and hence that $i = 1$. □

Finally, we combine Corollary 6.6 with the classification of indecomposable pairs f_1, g_1 (and hence the CFSG) to deduce Theorem 6.1.

Proof of Theorem 6.1. By possibly replacing f and g by left factors of theirs, we may assume f, g form a minimally reducible pair and hence admit the same Galois closure by Lemma 2.13 and hence $\mathrm{Mon}_k(f) \cong \mathrm{Mon}_k(g)$ as abstract groups. If $\mathrm{Mon}_k(f)$ is solvable the conclusion follows from Theorem 5.1, henceforth assume it is nonsolvable. By Corollary 6.6, we then have decompositions $f = f_1 \circ h_1$, $g = g_1 \circ h_2$ for solvable $\mathrm{Mon}_k(h_1), \mathrm{Mon}_k(h_2)$, and indecomposable f_1, g_1 with $\mathrm{Mon}_k(f_1), \mathrm{Mon}_k(g_1)$ nonsolvable, and thus almost-simple by Proposition 2.1.

By a symmetric application of Lemma 6.3, the splitting field of $f_1(X) - t$ equals that of $g_1(X) - t$. Thus $\mathrm{Mon}_k(f_1) \cong \mathrm{Mon}_k(g_1)$ is an almost-simple group admitting a cyclic transitive subgroup in its action on the roots of $f_1(X) - t$, as well as in its action on the roots of $g_1(X) - t$. Thus, [Mü95, Theorem] shows that the actions on roots of $f_1(X) - t$ and of $g_1(X) - t$, respectively, are permutation-equivalent, but are not equivalent (since f_1, g_1 have no common left composition factor by minimal reducibility). In particular, every element fixing a point in one of the two actions also fixes a point in the other action. Thus, by Burnside's lemma, the stabilizer of a root of $g_1(X) - t$ acts intransitively on the roots of $f_1(X) - t$. Thus, $f_1(X) - g_1(Y) \in k[X, Y]$ is reducible, and by the minimal reducibility assumption, h_1, h_2 are of degree 1 and f, g are indecomposable.

Moreover for pairs f_1, g_1 as above, [Mü95] gives the full list of possible degrees $\deg(f_1)$ and monodromy groups $\mathrm{Mon}_k(f_1)$, namely, $\deg(f_1) = 7, 11, 13, 15, 21, 31$ and $\mathrm{Mon}_k(f_1) = \mathrm{PSL}_3(2), \mathrm{PSL}_2(11), \mathrm{PSL}_3(3), \mathrm{PSL}_4(2), \mathrm{P\Gamma L}_4(3)$, and $\mathrm{PSL}_5(2)$, respectively. The corresponding polynomials f_1, g_1 were shown to be linearly related over $\overline{k}$ to those in [CNC99, §5]. □

Remark 6.7. The CFSG was not used in the proof of Corollary 6.6 but only in the last step of Theorem 6.1, where the monodromy of the indecomposable factors f_1, g_1 was needed.

6.2. **Proof of Theorem 1.2.** By [KN24, Corollary 2.5], $\mathrm{Red}_f(\mathbb{Z})$ is the union of a finite set and value sets $g(\mathbb{Q}) \cap \mathbb{Z}$ of Siegel functions g over $\mathbb{Q}$ such that the fiber product of $f : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ and $g : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ is reducible. Equivalently, $\mathrm{Red}_f(\mathbb{Z})$ is the union of a finite set and value sets $\tilde{g}(\mathbb{Q}) \cap \mathbb{Z}$ of Siegel functions $\tilde{g}$ over $\mathbb{Q}$ such that $\tilde{f}$ and $\tilde{g}$ form a *minimally* reducible pair, for some left factor $\tilde{f}$ of f. The case of solvable $\mathrm{Mon}_{\mathbb{Q}}(\tilde{f})$ is immediate from Theorem 5.7. To deal with the nonsolvable case, we begin with the following generalization of Corollary 6.6. It requires the classification of indecomposable Siegel functions from [Mü13] and hence the CFSG.

Setup. Throughout the proof, we use the notation of Section 6.1. We write $f = f_1 \circ \cdots \circ f_r$ and $g = g_1 \circ \cdots \circ g_s$ for indecomposable $f_1, \dots, f_r \in k[X]$ and $g_1, \dots, g_s \in k(X)$ over a number field k. Write $\hat{g}_j = g_1 \circ \cdots \circ g_j$ for $j = 1, \dots, s$. Let $j \in \{1, \dots, s\}$ be maximal such that $\ker(\mathrm{Mon}_k(\widehat{g}_j) \to \mathrm{Mon}_k(\widehat{g}_{j-1}))$ is nonsolvable. Without loss of generality, we may assume that g_j is a right-unique factor of $\hat{g}_j$ via performing Ritt moves ([Pak09, Theorem 1.1]). In the part where the argument is specific to $\mathbb{Q}$, we shall assume $k = \mathbb{Q}$.

We next show $\mathrm{Mon}_k(f)$ contains only the single nonabelian composition factor $\mathrm{soc}(\mathrm{Mon}_k(f_1))$. In particular there is only a single index j as above.

Lemma 6.8. *Assume that a polynomial $f \in k[X]$ and a Siegel function $g \in k(X)$ form a minimally reducible pair. Then there exists a decomposition $f = f_1 \circ h$ with indecomposable $f_1 \in k[X]$ and some $h \in k[X]$ of solvable monodromy.*

Proof. We use the notation of the above Setup. The proof of Corollary 6.6 applies if g_j has an almost-simple monodromy group, or more generally when $\mathrm{Mon}_k(g_j)$ has only one nonabelian composition factor counting with multiplicity. But by [Mü13, Theorem 4.8], the only other case is $\mathrm{Mon}_k(g_j) = S_n \wr C_2$, in which case it suffices to rule out the possibility $\deg(\hat{f}_{i-1}) = 2$, i.e., $f = f_1 \circ f_2 \circ h$ where $\deg(f_1) = 2$ and $\mathrm{Mon}_k(f_2)$ is almost-simple. Further assume g_j is a right-unique factor of $\hat{g}_j$ as in the setup above. Thus we may apply Lemma 6.3(1) symmetrically in f, g to conclude that $\hat{g}_j(X) - t$ and $(f_1 \circ f_2)(X) - t$ have the same splitting field. Therefore, $\mathrm{Mon}_k(\widehat{g_j}) = \mathrm{Mon}_k(f_1 \circ f_2) \leq S_n \wr C_2$ for $n := \deg(f_2)$. Since $\mathrm{Mon}_k(g_j)$ is a subquotient of $\mathrm{Mon}(\hat{g}_j)$ and it is already isomorphic to $\mathrm{Mon}(\hat{g}_j) \cong S_n \wr C_2$, it follows that $\hat{g}_j = g_j$ and $j = 1$. We now compare inertia groups at $t \mapsto \infty$ for the maps g_1 and $f_1 \circ f_2$. Since their Galois closures coincide, these inertia groups must have the same order; the latter one is obviously of order $2n$, but the former one is generated by an element with exactly two orbits in the primitive product-type group $S_n \wr C_2 \leq S_{n^2}$. Since $n \geq 5$, we have $n^2 > 4n$, so that at least one of these two orbits is of length $> 2n$, contradicting that the order is $2n$. □

To conclude the proof of Theorem 1.2, it therefore remains to classify minimally reducible pairs $f \in \mathbb{Q}[X]$, $g \in \mathbb{Q}(X)$ a Siegel function over $\mathbb{Q}$, where $f = f_1 \circ h$ with $\mathrm{Mon}_{\mathbb{Q}}(f_1)$ almost-simple and $\mathrm{Mon}_{\mathbb{Q}}(h)$ solvable. We divide the remainder of the proof according to the shape of $\mathrm{Mon}_k(g_j)$. Firstly if $|\hat{g}_j^{-1}(\infty)| = 1$, since $f_1(X) - t$ and $\hat{g}_j(X) - t$ have the same splitting field (by Lemma 6.3(1)), the proof of Theorem 6.1 applies and yields (over arbitrary number fields k) that f, g must be indecomposable. On the other hand, $|\hat{g}_{j-1}^{-1}(\infty)| = 1$ holds by Lemma 2.5 and the nonsolvability of $\mathrm{Mon}_k(g_j)$. In total, we shall henceforth assume:

(6.1) $\mathrm{Mon}_k(f_1)$ is almost-simple; $\mathrm{Mon}_k(h)$ is solvable; $|\hat{g}_{j-1}^{-1}(\infty)| = 1$; and $|\hat{g}_j^{-1}(\infty)| = 2$.

We distinguish the cases of nonaffine and affine $\mathrm{Mon}_{\mathbb{Q}}(g_j)$. In the former case, we have a result over arbitrary number fields k:

Lemma 6.9. *Let $f = f_1 \circ \cdots \circ f_r \in k[X]$ and $g = g_1 \circ \cdots \circ g_s \in k(X)$ be a minimally reducible pair, where g is a Siegel function with $|g^{-1}(\infty)| = 2$. If $\mathrm{Mon}_k(f)$ is nonsolvable and g does not factor through an indecomposable with affine nonsolvable monodromy group, then one of the following holds:*

(1) f is indecomposable, $\mathrm{Mon}_k(f) \in \{A_5, S_5\}$, and $\deg(g) = 10$. More precisely, f is one of the polynomials in [DF99, (1.8)]*;*
(2) f is of composition length 2, and more precisely $\mathrm{Mon}_k(f)$ is one of the groups $C_2 \times \mathrm{PSL}_3(2), C_3 \times A_5, C_3 \rtimes S_5, C_2.P\Gamma L_2(9), C_2 \times M_{11}$ of Magma Id 14T17, 15T15, 15T21, 20T265,22T26, resp.

Moreover, in 2), g is not a Siegel function over $\mathbb{Q}$.

Proof. We use the Setup from the beginning of the section, and following the above discussion assume (6.1) holds. Since $\mathrm{Mon}_k(f)$ has only a single nonabelian composition factor, and since $\mathrm{Mon}_k(g_j)$ is assumed to be nonaffine, it follows that $\mathrm{Mon}_k(g_j)$ is almost-simple by Proposition 2.4. Moreover, $g_{j+1} \circ \cdots \circ g_s$ has cyclic monodromy group over $\overline{k}$ by Lemma 2.5. Thus, Proposition 2.17(1) implies that $g_{j+1} \circ \cdots \circ g_s$ is either i) trivial (and thus $s = j$), or ii) of prime degree (and thus $s = j + 1$), or iii) of degree 4 (and thus $s = j + 2$). Furthermore, since $f = f_1 \circ h$ and $\mathrm{Mon}_k(h)$ is solvable, a symmetric application of Lemma 6.3(1) implies that $f_1(X) - t$ and $\hat{g}_j(X) - t$ have the same splitting field Ω'.

Case i) therefore implies that $f = f_1$ is indecomposable. Here, it remains to determine the indecomposable polynomials whose monodromy group $G \leq S_n$ is almost-simple and admits another faithful transitive permutation action (not factoring through an action permutation-equivalent to the first one) in which a cyclic transitive subgroup of G is mapped to a cyclic group with exactly two orbits, and moreover a point stabilizer in one action is intransitive in the other action. Since the "two-orbit condition" in particular enforces the second action to be of degree $\leq 2n$, [DM96, Theorems 5.2.A and 5.2.B] show that $G \in \{A_n, S_n\}$ is impossible as soon as $n > 8$, whence the entire check reduces to the short finite list of cases by [Mü95, Theorem]. One directly verifies using Magma that the only possibilities for $(G, \tilde{G}, [a, b])$, where $\tilde{G}$ denotes the image in the second action and $[a, b]$ denotes the two orbit lengths, are $(A_5, A_5(10), [5, 5])$, and $(S_5, S_5(10), [5, 5])$, where

$A_5(10), S_5(10)$ denote the degree-10 actions of A_5, S_5, resp. Such polynomials f are shown in [DF99, Theorem 1.1] to lie in the family [DF99, (1.8)].

For Case ii), recall that $f(X)-t$ and $g(X)-t$ (resp., $f_1(X)-t$ and $\hat{g}_j(X)-t$) have the same splitting field Ω (resp., Ω'). Thus, since $\mathrm{Mon}_{\overline{k}}(g_s)$ is cyclic of prime order p by Lemma 2.5, and hence the ramification index of Ω/Ω' at ∞ is $\deg(f_2\circ\cdots\circ f_r)=\deg(g_s)$ by Remark 2.8 (Abhyankar's lemma). In particuar, $r=2$. Since $\mathrm{Mon}_k(f_2)\le \mathrm{AGL}_1(p)$ for a prime p, the group $K:=\mathrm{Gal}(\Omega/\Omega')$ is a subdirect power of a subgroup of $\mathrm{AGL}_1(p)$ containing C_p. Let y be a root of $g(X)-t$. By Proposition 4.3, y generates all of Ω over the fixed field of $\mathrm{soc}(K)$. But y must have a minimal polynomial of degree p already over Ω'. This implies the diagonality of $\mathrm{soc}(K)$, and hence of K via Remark 2.22. Note furthermore that $f=f_1\circ f_2$ must be right-unique due to Proposition 2.17(5). The list of groups $\mathrm{Mon}_k(f_1\circ f_2)$ with this diagonality property is classified in [BKN26, Theorem 1.2], see [BKN26, Table 1] for the finite list. Running with Magma on the entries of that list, we find the the groups giving rise to a minimally reducible pair f,g with $f\in k[X]$ and $g\in k(X)$ Siegel. This is the list given in Case 2) of the assertion. Since all the occurring Siegel functions have an inertia group at ∞ with two different orbit lengths, none of the functions g is Siegel over $\mathbb{Q}$.

For Case iii), note that over $\overline{k}$, one has $\mathrm{Mon}_{\overline{k}}(g_{s-1}\circ g_s)=C_4$ and hence (f,g) cannot be a minimally reducible pair over $\overline{k}$ by Proposition 2.17(2). Due to Lemma 2.13, a corresponding minimally reducible pair over $\overline{k}$ must involve proper left-factors $\tilde{f}$ of f and $\tilde{g}$ of g, so that $(\tilde{f},\tilde{g})$ fall into Case i) or ii), and so $\mathrm{Mon}_{\overline{k}}(\tilde{f})$ must either be as in Assertion (1) or one of the even-degree cases in Assertion (2). But since $A_5\le \mathrm{Mon}_{\overline{k}}(\tilde{f})\trianglelefteq \mathrm{Mon}_k(\tilde{f})\le S_5$ in (1), and $\mathrm{Mon}_{\overline{k}}(\tilde{f})=\mathrm{Mon}_k(\tilde{f})$ for all the even-degree cases in (2), cf. Table 1 of [BKN26], reducibility of $(\tilde{f},\tilde{g})$ over $\overline{k}$ implies reducibility even over k, contradicting the minimal reducibility of (f,g). □

Finally we consider cases where $\mathrm{Mon}(g_j)$ is affine. This relies more concretely on the classification of indecomposable Siegel functions over $\mathbb{Q}$ in [Mü13, Theorem 5.2].

Lemma 6.10. *There is no minimally reducible pair $f\in\mathbb{Q}[X]$, $g\in\mathbb{Q}(X)$, for which g is a Siegel function over $\mathbb{Q}$ factoring through an indecomposable function in $\mathbb{Q}(X)$ with a nonsolvable affine monodromy group.*

Proof. We use the setup from the beginning of the section and, as above, assume (6.1). In particular, $f=f_1\circ h$ for an indecomposable $f_1\in\mathbb{Q}[X]$ and $h\in\mathbb{Q}[X]$ with solvable monodromy and $\mathrm{Mon}_{\mathbb{Q}}(f)$ has only the single nonabelian composition factor $\mathrm{soc}(\mathrm{Mon}_{\mathbb{Q}}(f_1))$. As in the setup, since $\mathrm{Mon}_{\mathbb{Q}}(f)\cong\mathrm{Mon}_{\mathbb{Q}}(g)$ as abstract groups, there is only a single index j such that $\mathrm{Mon}_{\mathbb{Q}}(g_j)$ is nonsolvable.

Assume on the contrary that $\mathrm{Mon}_{\mathbb{Q}}(g_j)$ is affine. By [Mü13, Theorem 5.2], the only affine monodromy groups of indecomposable Siegel functions over $\mathbb{Q}$ are $\mathrm{AGL}_3(2)$ and $C_2^4\rtimes S_5(\le S_{16})$. The case $\mathrm{Mon}_{\mathbb{Q}}(g_j)=\mathrm{AGL}_3(2)$ does not occur since the simple composition factor $\mathrm{PSL}_3(2)$ of $\mathrm{AGL}_3(2)$ does not occur as a composition factor of the monodromy of a polynomial over $\mathbb{Q}$ by [Mü95]. (This can also be seen using Fried's branch cycle lemma, cf. [Fri73, Section 3].) Thus, we are in the second case, that is, $\mathrm{Mon}_{\mathbb{Q}}(g_j)=C_2^4\rtimes S_5$. Moreover,

$\mathrm{Mon}_{\mathbb{Q}}(f_1) = S_5$ or $\mathrm{PGL}_2(5)(\leq S_6)$, since these are the only faithful actions of the almost-simple group S_5 with a cyclic transitive subgroup. Since $K = \ker(\mathrm{Mon}_{\mathbb{Q}}(f) \to \mathrm{Mon}_{\mathbb{Q}}(f_1))$ is solvable, it has to be contained in the kernel of any S_5-quotient of $\mathrm{Mon}_{\mathbb{Q}}(f)$ (since S_5 has no nontrivial solvable normal subgroups). Hence the quotient $\mathrm{Mon}_{\mathbb{Q}}(f_1)$ is the unique (nonsolvable) almost-simple quotient of $\mathrm{Mon}_{\mathbb{Q}}(f)$. Note that the ramification index over $t \mapsto \infty$ in the Galois subextension corresponding to this quotient is either 5 or 6. Thus, every normal subgroup $N \trianglelefteq \mathrm{Mon}_{\mathbb{Q}}(f) = \mathrm{Mon}_{\mathbb{Q}}(g)$ similarly has a unique S_5-quotient, if any, and the ramification index over a place extending $t \mapsto \infty$ in the extension corresponding to this S_5-quotient must divide either 5 or 6 by Remark 2.8 (since its corresponding cover must be the pullback of the Galois closure of f_1). But $N = \ker(\mathrm{Mon}_{\mathbb{Q}}(g) \to \mathrm{Mon}_{\mathbb{Q}}(\widehat{g}_{j-1}))$ is such a normal subgroup, whose S_5-quotient has ramification index 4 (as is easily seen from the fact that the splitting field of $g_j(X) - t$ is ramified over $t \mapsto \infty$ with ramification index 8, see [Mü13, Theorem 5.2]). This contradiction shows that $\mathrm{Mon}_{\mathbb{Q}}(g_j)$ must be almost-simple. □

Proof of Theorem 1.2. Using the setup from the beginning of the section. By Lemma 6.8 we may assume (6.1) holds. The conclusion then follows from Lemma 6.9 if $\mathrm{Mon}(g_j)$ is nonaffine, and Lemma 6.10 if it is affine. □

Remark 6.11. (1) As seen, Theorem 5.7 and Lemma 6.9 also yield a solution to the Hilbert-Siegel problem over arbitrary number fields k under the assumption that $f \in k[X]$ does not factor through a solvable of degree 2 or 4, and the *additional* assumption that the corresponding Siegel function $g \in k(X)$ does not factor through a nonsolvable indecomposable with affine monodromy group. Since there is only a short finite list of such affine monodromy groups of Siegel functions, cf. [Mü13, Theorem 4.8], we have a complete solution to the problem for polynomials f which do not factor through an indecomposable $h \in k[X]$ such that $\mathrm{Mon}_k(h)$ has a nonsolvable composition factor occurring in that list (the largest degree exception being $\mathrm{Mon}_k(h) = \mathrm{PSL}_5(2) \leq S_{31}$).
(2) The case of even degree solvable polynomials, left open in Theorem 1.2, requires additional ideas. In particular, the diagonality assertion of Theorem 4.1 is no longer valid for minimally reducible pairs (f, g) with f a polynomial and g a Siegel function, in case $\deg(f_r) \in \{2, 4\}$, as the following paragraph shows.

By [Mü13, Section 5.3.2], there is a family of indecomposable degree-16 Siegel functions g over $\mathbb{Q}$ with monodromy group $\mathrm{Mon}_{\mathbb{Q}}(g) = S_4 \wr C_2$ in the product-type action, and such that the *imprimitive* wreath product action of the same monodromy group gives rise to a polynomial ramification type. Comparing point and block stabilizers in these two actions, one furthermore sees that the pairs (f, g) of polynomials f and Siegel functions g arising in this way are minimally reducible. But the polynomial f is then of the form $f = f_1 \circ f_2$ with $\mathrm{Mon}_k(f_1) = C_2$, $\mathrm{Mon}_k(f_2) = S_4$, and $\mathrm{soc}(\ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(f_1))) = \mathrm{soc}(S_4^2) = C_2^4$.

This is also an example where $\mathrm{Red}_f(\mathbb{Z})$ contains an infinite set $g(\mathbb{Q}) \cap \mathbb{Z}$ that is not contained in $f_1(\mathbb{Q})$ for the (unique) indecomposable left factor f_1 of f.

6.3. **Functional equations.** Let k be an algebraically closed field of characteristic 0.

Proof of Corollary 1.4. Let $F(X,Y) \in k[X,Y]$ be a right-reduced irreducible factor of $f(X)-g(Y)$ defining a genus-0 curve birational to $F(X,Y)=0$. Let $k(x,y)$ be its genus-0 function field, so that $F(x,y)=0$. Set $t=f(x)=g(y)$. Then $k(x)\cap k(y)$ is a rational function field by a theorem of Lüroth. Furthermore, we may write $k(x)\cap k(y)=k(s)$ where $s=f_1(x)=g_1(y)$ and $t=w_1(s)$ for some polynomials $f_1,g_1,w_1\in k[X]\setminus k$. Since the factor is assumed to be right-reduced, we get $k(s)=k(t)$, and hence $\deg(w_1)=1$. The reducibility of $f(X)-g(Y)\in k[X,Y]$ thus implies that of $f_1(X)-g_1(Y)\in k[X,Y]$. Theorem 6.1 then implies that one of the following holds:

(a) f_1 and g_1 have a common left factor $h\in k[X]$ with $\deg(h)>1$, or

(b) $f_1=w_2\circ h_1\circ f_2$ and $g_1=w_2\circ h_2\circ g_2$, where $\deg(w_2)=1$, and $\{h_1,h_2\}$ is either $\{T_4,-T_4\}$ or is one of the pairs of polynomials of degree $7,11,13,15,21,31$ in [CNC99, §5].

A direct computer check, using Magma for the possibilities of ramification in [Mü95, Theorem], shows that the only pairs $\{h_1,h_2\}$ in [CNC99] with a genus-0 factor are certain pairs of degree 7 or 13, cf. Remark 6.12 for a concrete description.

In the first case (a), we have $f_1=h\circ f_2$ and $g_1=h\circ g_2$, for $h,f_2,g_2\in k[X]\setminus k$. Since $k(x)\cap k(y)=k(s)$, it follows that $k(x_2)\cap k(y_2)=k(s)$, where $x_2=f_2(x)$ and $y_2=g_2(y)$. Since $h(x_2)=h(y_2)=s$, we obtain two distinct roots x_2 and y_2 of $h(X)-s\in k(s)[X]$, so that $h(X)-h(Y)\in k[X,Y]$ has a nondiagonal irreducible factor $H(X,Y)\in k[X,Y]$ whose corresponding curve $H(X,Y)=0$ is birational to a genus-0 curve $\mathcal{D}$. Since $k=\overline{k}$, it now follows from [AZ03, Theorem 1] that[15] there exist $w_2,h',u_1\in k[X]\setminus k$ such that $h=w_2\circ h'\circ u_1$ and h' is either

i) X^d for $d\geq 3$, or

ii) T_d for $d\geq 3$, or

iii) one of the polynomials P_i, $i=1,2,3$ appearing in the statement of the corollary.

Moreover, [AZ03] shows that $\deg(u_1)=1$ in cases ii) and iii), and that $k(h'(u_1(x_2)))=k(h'(u_1(y_2)))$. Since $k(x_2)\cap k(y_2)=k(s)$, it follows that $k(h'(u_1(x_2)))$ is of degree 1 over $k(s)$, and hence $\deg(w_2)=1$. For simplicity, in what follows for case (a) we replace h,f_2,g_2 by h', $u_1\circ f_2$ and $u_1\circ g_2$, respectively, and consequently x_2,y_2 by their new values $f_2(x),g_2(y)$, respectively. We modify H and $\mathcal{D}$ so that they still correspond to a nondiagonal factor of $h(X)-h(Y)$, and a curve birational to $H=0$, resp.

We next note that case i) does not occur: For, both x_2 and y_2 are roots of $X^d-s\in k(s)[X]$. Since $k=\overline{k}$ this implies that $k(x_2)=k(y_2)$ is of degree $d\geq 3$ over $k(s)$, contradicting $k(x_2)\cap k(y_2)=k(s)$.

For the remaining cases ii) and iii) of a), as well as the cases in b), it remains to determine the possibilities for the right factors f_2 and g_2. In case b), set $h=h_1$, and let $\mathcal{D}$ be a curve birational to $H(X,Y)=0$, for an irreducible factor $H(X,Y)$ of $h_1(X)-h_2(Y)\in k[X,Y]$. Since $\mathcal{D}$ is of genus 0 and $k=\overline{k}$, the function field $k(\mathcal{D})=k(z)$ is rational. Furthermore, $k(z)/k(x_2)$ is unramified over the place $x_2\mapsto\infty$ by Remark 2.8(1). Since $k(x,z)$ is contained in the genus-0 field $k(x,y)$, it is also of genus 0. Since $k(x)/k(x_2)$ is totally ramified over $x_2\mapsto\infty$, whereas $k(z)/k(x_2)$ is unramified over $x_2\mapsto\infty$, the

[15] In [AZ03], w_2 is denoted by A, and u_1 corresponds to S in (1) and M in (2)-(5).

fields $k(x)$ and $k(z)$ are linearly disjoint over $k(x_2)$ by Remark 2.8(2), and moreover every place of $k(z)$ lying over $x_2 \mapsto \infty$ is totally ramified in $k(x,z)/k(z)$ by Remark 2.8(2). If $m := [k(z) : k(x_2)] > 2$, then the Riemann–Hurwitz formula for the degree-$\deg(f_2)$ extension $k(x,z)/k(z)$ shows the genus $\tilde{g} = 0$ of $k(x,z)$ satisfies:

$$2(\tilde{g}-1) \geq -2\deg(f_2) + \sum_Q (\deg(f_2)-1) = (m-2)\deg(f_2) - m, \tag{6.2}$$

where Q runs over the places of $k(z)$ lying over $x_2 \mapsto \infty$. If $m > 2$ and $\deg(f_2) > 1$, (6.2) contradicts that $\tilde{g} = 0$ as above. Since $m > 2$ in case (a) iii) and in case (b), except for $\{h_1, h_2\} = \{T_4, -T_4\}$, it follows that $\deg(f_2) = 1$ in all those cases, and by symmetry $\deg(g_2) = 1$, leading to cases (2) and (3) of the assertion with $\mu := w_1 \circ w_2$, $\lambda_1 := f_2$ and $\lambda_2 = g_2$.

It remains to treat the cases $h = T_d$ for $d \geq 3$ in a), or $\{h_1, h_2\} = \{T_4, -T_4\}$ in b). In these cases we have $m = 2$, and there are exactly two places Q_1, Q_2 of $k(z)$ lying over $x_2 \mapsto \infty$. In particular, (6.2) is an equality, and hence $k(x,z)/k(z)$ is unramified away from Q_1, Q_2. Thus the *only* finite branch points of $k(x)/k(x_2)$ are the two branch points $x_2 \mapsto -2, 2$ of $k(z)/k(x_2)$, by Remark 2.8(3). Moreover, Abhyankar's lemma implies that the ramification index of every place in $f_2^{-1}(\pm 2)$ is at most 2. Since $x_2 \mapsto -2, 2$ are the only unramified places over two finite branch points s by [ZM08, Lemma 3.2.], it follows that $h \circ f_2$ has only two finite branch points and the $(h \circ f_2)$-preimages of these are all of ramification index ≤ 2. Such ramification forces that $h_1 \circ f_2 = \pm T_n \circ v_1$ for $n := \deg(f)$ and some $v_1 \in k[X]$ of degree 1, by [ZM08, Lemma 3.2.]. Similarly, $h_2 \circ g_2 = \pm T_m \circ v_2$ for $m := \deg(g)$ and $v_2 \in k[X]$ of degree 1.

We may therefore write $f = \mu \circ (\pm T_n) \circ \lambda_1$ and $g = \mu \circ (-T_m) \circ \lambda_2$ for linear $\mu, \lambda_1, \lambda_2 \in k[X]$, where $d := \gcd(m,n) \geq 3$. So far we allow any combination of plus and minus signs for f. But note that f, g cannot have a common left factor T_2, since it is linearly related to X^2 and thus would contradict minimality as for Case i) above. In case d is even this leaves only the possibility of different signs in f, g, as asserted in (1). In case d is odd, we may assume without loss of generality that n odd. Then, by possibly composing μ, λ_1, λ_2 with $X \mapsto \pm X$ and using the identity $T_n(-X) = -T_n(X)$, we obtain the combination of signs given in (1). □

Remark 6.12. (a) A computer check further reveals that in case (3) of Corollary 1.4, the degree-7 (resp., degree-13) polynomials h_1, h_2 have three branch points with branch cycles of orders $2,3,7$ or $2,4,7$ (resp., $2,3,13$). From this, it is possible to obtain concrete parameterizations, namely

$$h_1 = X(X+1)^3(X+a+3)^3, \text{ with } a^2+a+2=0, \tag{6.3}$$

$$h_1 = X^4(X-2)^2(X-a), \text{ with } a^2+a+2=0, \text{ and} \tag{6.4}$$

$$\begin{aligned} h_1 = X^3(X-27)(X^3 + (-16a^3 - 12a^2 - 29a + 51)X^2 + (16a^3 - 96a^2 - 25a - 618)X \\ + \frac{1}{3}(21872a^3 + 29148a^2 + 58408a - 53112))^3, \text{ with } a = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9 \end{aligned} \tag{6.5}$$

in the three respective cases. In all cases, h_2 is then obtained as $h_2(X) = \gamma/\overline{\gamma} \cdot \overline{h_1}(X)$, where γ denotes the unique finite nonzero branch point of h_1, and $\overline{z}$ denotes the complex conjugate of z.
(b) For the converse of Corollary 1.4 we show that (1)-(3) indeed have right-reduced irreducible factors defining curves of genus 0. For case (1) with $d := \gcd(m, n)$, the polynomials $T_d(X) \pm T_d(Y) \in \mathbb{C}[X, Y]$ admit[16] an irreducible factor $H(X, Y) = X^2 - 2XY\cos(\pi/d) + Y^2 - 4\sin^2(\pi/d)$ [AZ03, Prop. 2.2], so that $H(T_{n/d}(X), T_{m/d}(Y))$ is an irreducible factor of $T_n(X) \pm T_m(Y)$ defining a right-reduced genus-0 curve. Composing with linear polynomials one obtains the desired factor of $f(X) - g(Y)$. In case (2), the irreducible nondiagonal component of genus 0 is the unique one: $(f(X) - f(Y))/(X - Y)$. In case (3), the degrees of the irreducible factors defining a genus-0 curve are: 3 and 4 (i.e. two factors of genus 0) in (6.3); 3 in (6.4); and 4 in (6.5). Since the polynomials in (2) and (3) are indecomposable, the factors are automatically right-reduced.

Appendix A. Fried's (m, n)-problem

As a consequence of Theorem 6.1, we have the following answer to Fried's (m, n)-problem.

Corollary A.1. *Let $P, Q \in \mathbb{C}[X]$ be simply branched polynomials of degrees $m := \deg(Q) \geq 2$ and $n := \deg(P) \geq \max\{m, 3\}$ such that P and Q do not satisfy a relation $P = Q \circ \mu$ with $\mu \in \mathbb{C}[X]$ linear. If $n = 3$, then assume moreover that the sets of finite branch points of P and of Q are disjoint. Then $Q(f(X)) - P(g(Y))$ is irreducible for all $f, g \in \mathbb{C}[X] \setminus \mathbb{C}$.*

Note that the assumption $P \neq Q \circ \mu$ is required for $P(X) - Q(Y) \in k[X, Y]$ to be irreducible, and clearly holds if the branch loci of P and Q are disjoint.

Proof. Assume on the contrary that $Q(f(X)) - P(g(Y)) \in \mathbb{C}[X, Y]$ is reducible for some $f(X), g(X) \in \mathbb{C}[X] \setminus \mathbb{C}$. Let (h_Q, h_P) be a corresponding minimally reducible pair, so that in particular h_Q is a left-factor of $Q \circ f$ and h_P is a left-factor of $P \circ g$.

Note first that, as in Remark 2.11, a simply branched polynomial of degree $n \geq 4$ cannot be the left-factor of a Ritt move. Therefore, when $n \geq 4$, the polynomial h_P must admit (the simply branched, hence indecomposable) P as a left-factor. By Theorem 1.1, P is either a left factor of $Q \circ f$, or P is one of the exceptional polynomials in Theorem 1.1(2). The latter case cannot occur since the exceptional polynomials in Theorem 1.1(2) are not simply-branched. In the former case, the same reasoning shows that $P = Q \circ \mu$ for a linear $\mu \in \mathbb{C}[X]$, contradicting our assumptions.

Next, assume $n = 3$. Since P is simply branched of degree 3, it is linearly related to T_3 over $\mathbb{C}$. Since the only Ritt moves with T_3 as a left factor are $T_3 \circ (T_m \circ \ell) = T_m \circ (T_3 \circ \ell)$ or $(-T_2) \circ (T_3 \circ \ell) = T_3 \circ (-T_2 \circ \ell)$, for $m \geq 2$ and $\ell \in \mathbb{C}[X]$ of degree 1, by Ritt's second theorem, and since the branch loci of T_m and $-T_2$ are contained in that of T_3, it follows that any indecomposable left-factor of $P \circ g$ must have a branch point set which is contained in the one of P. On the other hand, every non-linear left factor of $Q \circ f$ must share at least one finite branch point with Q, as in Remark 2.11. Together with the assumption

[16] In fact any factor of it defines a genus-0 curve.

that the sets of finite branch points of P and Q are disjoint, these two observations yield that in every pair $(\tilde{h}_P, \tilde{h}_Q)$ of indecomposable left-factors of (h_P, h_Q), the branch point set of $\tilde{h}_P$ must be different from the one of $\tilde{h}_Q$. This contradicts the fact that, for all pairs in Theorem 1.1, these two branch point sets coincide. □

References

[AZ01] R. M. Avanzi and U. M. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation*, Acta Arith. **99** (2001), no. 3, 227–256.

[AZ03] ———, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$*, Compositio Math. **139** (2003), no. 3, 263–295.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I: The user language*, J. Symb. Comput. **24** (1997), no. 3-4, 235–265.

[BIJ+19] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. H. Silverman, and T. J. Tucker, *Current trends and open problems in arithmetic dynamics*, Bull. Amer. Math. Soc. (N.S.) **56** (2019), no. 4, 611–685.

[Bil99] Y. F. Bilu, *Quadratic factors of $f(x) - g(y)$*, Acta Arith. **90** (1999), no. 4, 341–355.

[BKN26] A. Behajaina, J. König, and D. Neftin, *Monodromy groups of polynomials of composition length 2*, 2026.

[BT00] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), no. 3, 261–288.

[BT12] B. Bukh and J. Tsimerman, *Sum-product estimates for rational functions*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 1, 1–26.

[Cas68] J. W. S. Cassels, *Factorization of polynomials in several variables*, Proc. 15th Scand. Congr. Oslo 1968, Lect. Notes Math. 118, 1-17 (1970), 1968.

[CCF+12] K. Chamberlin, E. Colbert, S.M. Frechette, P. Hefferman, R. Jones, and S. Orchard, *Newly reducible iterates in families of quadratic polynomials*, Involve, A Journal of Mathematics **5** (2012), 481–495.

[CDH+12] A. Carney, T. Do, J. Hallett, Q. Sun, B. Weiss, E. Wells, S. Xia, and M. E. Zieve, *On the functional equation f(u)=g(v) in complex polynomials f,g and meromorphic functions u,v, II: the reducible case*, Preprint, 2012.

[CNC99] P. Cassou-Noguès and J.-M. Couveignes, *Factorisations explicites de $g(y) - h(z)$*, Acta Arith. **87** (1999), no. 4, 291–317.

[Cox12] David A. Cox, *Galois theory*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2012. MR 2919975

[DF99] P. Dèbes and M. D. Fried, *Integral specialization of families of rational functions*, Pacific J. Math. **190** (1999), no. 1, 45–85.

[DHH+12] T. Do, J. Hallett, X. Huang, Y. Jiang, B. Weiss, E. Wells, and M. E. Zieve, *On the functional equation f(u)=g(v) in complex polynomials f,g and meromorphic functions u,v, I: the irreducible case*, Preprint, 2012.

[DLS61] H. Davenport, D. J. Lewis, and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quart. J. Math. Oxford Ser. (2) **12** (1961), 304–312.

[DM96] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, Springer New York, 1996.

[DR25] M. Derickx and J. Rawson, *Functions on curves with infinitely many split fibres*, Work in preparation, 2025.

[DS64] H. Davenport and A. Schinzel, *Two problems concerning polynomials*, J. Reine Angew. Math. **214/215** (1964), 386–391.

[DZ22] Zhiguo Ding and Michael E. Zieve, *Extensions of absolute values on two subfields*, J. Algebra **598** (2022), 105–119. MR 4379276

[Ehr58] A. Ehrenfeucht, *Kryterium absolutnej nierozkladalnósci wielomiaów*, Prace Mat. **2** (1958), 167–169.

[FG12] M. D. Fried and I. Gusić, *Schinzel's problem: imprimitive covers and the monodromy method*, Acta Arith. **155** (2012), no. 1, 27–40.

[FM69] M. D. Fried and R. E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.

[Fri70] M. D. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970), 41–55.

[Fri73] ———, *Fields of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois Journal of Mathematics **17** (1973), 128–146.

[Fri74] ———, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231.

[Fri86a] ———, *The Hilbert–Siegel problems and Group Theory solving cases of them*, Preprint, `https://www.math.uci.edu/~mfried/paplist-cov/Hilb-Sieg86.pdf`, 1986.

[Fri86b] ———, *Rigidity and applications of the classification of simple groups to monodromy Part II-applications of connectivity: Davenport and Hilbert–Siegel problems*, Preprint, 1986.

[Fri87] ———, *Irreducibility results for separated variables equations*, J. Pure Appl. Algebra **48** (1987), no. 1-2, 9–22.

[Fri12] ———, *Variables separated equations: strikingly different roles for the branch cycle lemma and the finite simple group classification*, Sci. China Math. **55** (2012), no. 1, 1–72.

[Fri23] ———, *Taming genus 0 (or 1) components on variables-separated equations*, Albanian J. Math. **17** (2023), no. 2, 19–80.

[GMS02] R. M. Guralnick, P. Müller, and J. Saxl, *The rational function analogue of a question of Schur and exceptionality of permutation representations*, Memoirs of the American Mathematical Society **162** (2002), 0–0.

[GS07] R. M. Guralnick and J. Shareshian, *Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points*, Mem. Amer. Math. Soc. **189** (2007), no. 886, vi+128, With an appendix by Guralnick and R. Stafford. MR 2343794

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR 463157

[HT23] L. Hajdu and R. Tijdeman, *The Diophantine equation $f(x) = g(y)$ for polynomials with simple rational roots*, J. Lond. Math. Soc. (2) **108** (2023), no. 1, 309–339.

[IJO+21] P. Illig, R. Jones, E. Orvis, Y. Segawa, and N. Spinale, *Newly reducible polynomial iterates*, International Journal of Number Theory **17** (2021), no. 06, 1405–1427.

[Kle79a] F. Klein, *Ueber die Transformation elfter Ordnung der elliptischen Functionen*, Mathematische Annalen **15** (1879), 533–555.

[Kle79b] ———, *Ueber die Transformation siebenter Ordnung der elliptischen Functionen*, Mathematische Annalen **14** (1879), 428–471.

[KMS07] M. Kulkarni, P. Müller, and B. Sury, *Quadratic factors of $f(X) - g(Y)$*, Indag. Math. (N.S.) **18** (2007), no. 2, 233–243.

[KN24] J. König and D. Neftin, *Reducible fibers of polynomial maps*, Int. Math. Res. Not. IMRN (2024), no. 6, 5373–5402.

[KNR24] J. König, D. Neftin, and S. Rosenberg, *Polynomial compositions with large monodromy groups and applications to arithmetic dynamics*, 2024, https://arxiv.org/abs/2401.17872.

[Mon24] T. Monderer, *Reducibility, specialization and related low genus phenomena*, Ph.D. thesis, Technion, Israel Institute of Technology, Haifa, Israel, 2024, Doctoral dissertation.

[MV96] Peter Müller and Helmut Völklein, *On a question of Davenport*, J. Number Theory **58** (1996), no. 1, 46–54. MR 1387720

[Mü95] P. Müller, *Primitive monodromy groups of polynomials*, Recent developments in the inverse Galois problem (Seattle, WA, 1993), Contemp. Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995, pp. 385–401.

[Mü98] ———, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc. **350** (1998), no. 5, 1823–1850.
[Mü99] ———, *Hilbert's irreducibility theorem for prime degree and general polynomials*, Israel J. Math. **109** (1999), 319–337.
[Mü02] ———, *Finiteness results for Hilbert's irreducibility theorem*, Ann. Inst. Fourier (Grenoble) **52** (2002), no. 4, 983–1015.
[Mü13] ———, *Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** (2013), no. 2, 369–438.
[NZ24] D. Neftin and M. Zieve, *Monodromy groups of indecomposable coverings of bounded genus*, 2024, arXiv:2403.17167.
[Ost25] A. Ostrov, *M.Sc. Thesis, Fibonacci numbers as special values of polynomials*, 2025.
[Pak09] F. Pakovich, *Prime and composite Laurent polynomials*, Bulletin des Sciences Mathématiques **133** (2009), no. 7, 693–732.
[Pak10] ———, *On the equation $P(f) = Q(g)$, where P, Q are polynomials and f, g are entire functions*, Amer. J. Math. **132** (2010), no. 6, 1591–1607.
[Pak18] ———, *On algebraic curves $A(x) - B(y) = 0$ of genus zero*, Math. Z. **288** (2018), no. 1-2, 299–310.
[Pak23a] ———, *On intersection of lemniscates of rational functions*, arXiv:2309.04983, Preprint, 2023.
[Pak23b] ———, *Tame rational functions: decompositions of iterates and orbit intersections*, J. Eur. Math. Soc. (JEMS) **25** (2023), no. 10, 3953–3978.
[Rur12] Rurik, *Criteria for irreducibility of polynomial*, Question on MathOverflow, 2012, User "Rurik" on MathOverflow. `https://mathoverflow.net/questions/105304/criteria-for-irreducibility-of-polynomial` (accessed 2026-03-04).
[Sch63] A. Schinzel, *Some unsolved problems on polynomials*, Neki nereseni problemi u matematici. Matematicka Biblioteka 25, 1963, pp. 63–70.
[Sch67] ———, *Reducibility of polynominals of the form $f(x) - g(y)$*, Colloq. Math. **18** (1967), 213–218.
[Sch00] ———, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000, With an appendix by Umberto Zannier.
[Sch07] ———, *Andrzej Schinzel selecta. Vol. I*, Heritage of European Mathematics, European Mathematical Society (EMS), Zürich, 2007, Diophantine problems and polynomials.
[Tao12] T. Tao, *When is $P(x) - Q(y)$ irreducible?*, `https://mathoverflow.net/q/105747`, 2012, MathOverflow post.
[Tao15] ———, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, Contrib. Discrete Math. **10** (2015), no. 1, 22–98.
[Tve68] H. Tverberg, *A study in irreducibility of polynomials*, Ph.D. thesis, University of Bergen, Bergen, Norway, 1968, Doctoral dissertation.
[Zie12] M. E. Zieve, *Criteria for irreducibility of polynomial*, `https://mathoverflow.net/questions/105304/criteria-for-irreducibility-of-polynomial/`, 2012, MathOverflow post.
[ZM08] M. E. Zieve and P. Müller, *On Ritt's polynomial decomposition theorems*, 2008, https://arxiv.org/pdf/0807.3578.

Univ. Lille, CNRS, UMR 8524, Laboratoire Paul Painlevé, F-59000 Lille, France
Email address: `angelot.behajaina@univ-lille.fr`

Department of Mathematics Education, Korea National University of Education, Cheongju, South Korea
Email address: `jkoenig@knue.ac.kr`

Department of Mathematics, Technion - Israel Institute of Technology, Haifa, Israel
Email address: `dneftin@technion.ac.il`