REDUCIBILITY OF SEPARATED POLYNOMIALS AND APPLICATIONS

ANGELOT BEHAJAINA, JOACHIM KÖNIG, AND DANNY NEFTIN

Abstract. We solve a problem of Davenport–Lewis–Schinzel, originating in the 50's, concerning the reducibility of separated polynomials, in the absence of indecomposable factors of degree ≤ 4. Consequences are derived to the finiteness problem for Hilbert's irreducibility theorem (a.k.a. Hilbert–Siegel problem), to stability in arithmetic dynamics, and to functional equations in rational functions.

1. Introduction

Reducibility of polynomials is a central topic of interest in number theory, cf. [Sch00]. In a prominent paper from 1963, Schinzel poses nine problems concerning reducibility of polynomials. The first three were described by Zannier [Sch07, Part E] as "substantial, involving several mathematical fields" due to the intimate relation to polynomial monodromy. The second problem was solved by Fried [Fri86], cf. [CNC99], 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 first problem by Davenport and Schinzel [DS64]. As we shall see below, the first problem, also known as the Davenport–Lewis–Schinzel (DLS) problem[1], arises naturally in several topics including the finiteness problem for Hilbert's irreducibility theorem (a.k.a. the Hilbert–Siegel problem), low degree points in fibers of polynomial maps, stability in arithmetic dynamics, functional equations, intersections of lemniscates [Pak23a], expanding polynomials [Tao12, Tao15], and sum-product estimates [BT12, Thm. 6, proof].

The DLS problem is deceptively easy to state:

"For which polynomials $f,g\in\mathbb{C}[x]\setminus\mathbb{C}$, is $f(x)-g(y)\in\mathbb{C}[x,y]$ reducible?"

A trivial source for reducible pairs arises when $f=g$, in which case $f(x)-f(y)$ has a diagonal factor $x-y$. Further examples $(f,g)=(T_4,-T_4)$ were given by Davenport, Lewis, and Schinzel [DLS61], where T_n is the degree-n Chebyshev polynomial satisfying $T_n(x+1/x)=x^n+1/x^n$. Soon after, examples where $\deg(f)=\deg(g)$ is either 7 or 11 were given by Birch. There has been an extensive work on the problem from the 50's to the 60's, see Cassels [Cas70]. Eventually, when f,g are indecomposable polynomials (i.e., cannot be written as a composition of two polynomials of degree >1), the cases where $f(x)-g(y)\in\mathbb{C}[x,y]$ is reducible were classified by Fried [Fri86], and in particular $\deg(f)=\deg(g)$ is $7,11,13,15,21$, or 31. The special indecomposable polynomials of these degrees were then explicitely written by Müller [M95], and Cassou-Noguès–Couveignes

[1]The problem is also named Schinzel's problem in some papers, e.g. [Fri12]. It is first explicitely stated in a paper of Davenport, Lewis and Schinzel [DLS61].

[CNC99]. Further studies concern quadratic factors of $f(x)-g(y)\in\mathbb{C}[x,y]$ by Bilu [Bil99], cf. [KMS07]; the cases $g=cf$, $c\in\mathbb{C}$ by Avanzi–Zannier [AZ03]; the case $g=\alpha\circ f$, for degree-1 $\alpha\in\mathbb{C}[x]$ by Fried and Gusić [Fri12, FG12]; the case where $f(x)=g(y)$ has a component of genus ≤ 1 by Zieve et al., cf. [Zie12]; and the case where f is a composition of polynomials with nonsolvable monodromy [KN24]. However, the problem remains open for decomposable polynomials.

In this paper, we develop and use results concerning solvable monodromy groups of decomposable polynomials in order to solve the DLS problem and consequently make significant advances on the above mentioned topics. For this working draft, we avoid composition factors of degree ≤ 4 for one of the polynomials:

Theorem 1.1. *Let $f,g\in\mathbb{C}[x]$ be polynomials of degree >1 such that f does not factor through a nonlinear polynomial of degree ≤ 4. Then $f(x)-g(y)$ is reducible in $\mathbb{C}[x,y]$ if and only if one of the following occurs for some polynomials $f_1,g_1\in\mathbb{C}[x]$:*

1. *f and g have a common 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 $g=\mu\circ h_2\circ g_1$, for some linear $\mu\in\mathbb{C}[x]$, where (h_1,h_2) is one of the pairs of polynomials of degrees 7,11,13,15,21,31 given in* [CNC99, §5].

In future versions, we shall remove the assumptions on factors of f. The new methods introduced deal with polynomials with solvable monodromy. For such poynomials Theorem 1.1 is a special case of Theorem 3.1. The general case, proved in §5.1, is based on the combination of these new methods, with the older methods [KN24] for nonsolvable monodromy. The theorem applies over arbitrary fields of characteristic 0.

We next discuss the consequences to the above-mentioned topics:

Reducible fibers and the Hilbert–Siegel problem. For a degree-d polynomial $f\in\mathbb{Q}[x]$, consider its fibers $f^{-1}(a)\subseteq\mathbb{C}$ over rational points $a\in\mathbb{Q}$, and more specifically, the degrees $[\mathbb{Q}(\alpha):\mathbb{Q}]$ of preimages $\alpha\in f^{-1}(a)$. For $a\in\overline{\mathbb{Q}}$, say that the fiber $f^{-1}(a)$ over a is irreducible [2] if the degree $[\mathbb{Q}(\alpha):\mathbb{Q}(a)]$ attains its maximal value d for (all) $\alpha\in f^{-1}(a)$.

Hilbert's Irreducibility Theorem (HIT) asserts the existence of infinitely many $a\in\mathbb{Z}$ such that $f^{-1}(a)$ is irreducible. The finiteness problem, a.k.a. the Hilbert–Siegel problem[3], asks to determine, up to a finite set, the set of integral exceptions for Hilbert's theorem:

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

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, when f_1 runs through left factors of f. For indecomposable polynomials $f\in\mathbb{Q}[x]$ of degree >5, the finiteness of $\mathrm{Red}_f(\mathbb{Z})\setminus f(\mathbb{Q})$ was shown by Fried [Fri74, Fri86], cf. [M99], and examples of degree-5 polynomials $f\in\mathbb{Q}[x]$ for which this set is infinite were constructed by Dèbes–Fried [DF99]. For compositions f

[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 reducible.

[3]The name first appeared in [Fri86], cf. [DF99].

of polynomials in $\mathbb{Q}[x]$ with nonsolvable monodromy and any indecomposable left factor f_1 of f, the set $\mathrm{Red}_f(\mathbb{Z}) \setminus f_1(\mathbb{Q})$ is also finite by [KN24].

The problem is closely related to the DLS problem: For, as in the proof of HIT, it 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 $f(x) = g(y)$ is reducible for a rational function $g \in \mathbb{Q}(x)$ whose value set $g(\mathbb{Q})$ contains infinitely many integers, a.k.a. a Siegel function. For polynomial $g \in \mathbb{Q}[x]$, this is equivalent to the reducibility of $f(x)-g(y) \in \mathbb{Q}[x,y]$, a rational version of the DLS problem.

Variants of the problem where $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ is a degree-d map from a (smooth projective) curve X of positive genus were also considered. In the general case, where the monodromy group is S_d, $\mathrm{Red}_f(\mathbb{Z})$ is in fact finite, see Müller [M99], and [M02] for other cases. The finiteness of the analogous set $\mathrm{Red}_f(\mathbb{Q})$ 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]. However, the original Hilbert–Siegel problem has remained open.

The above work on the DLS problem and solvable monodromy groups led us to the following theorem, bringing us close to the solution of the Hilbert–Siegel problem:

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 ≤ 6. Then $\mathrm{Red}_f(\mathbb{Z})$ 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.*

This is proved in Section 5.2 with an approach that applies over general number fields.

Stability in arithmetic dynamics. Stability of polynomials under iterates is a main topic in arithmetic dynamics, see [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, it is natural to ask whether for some $n \in \mathbb{N}$, there could be infinitely many $a \in \mathbb{Z}$ over which the fibers of $f^{\circ n}$ are reducible, but those of $f^{\circ n-1}$ aren't. In other words, when is $\mathrm{Red}_{f^n}(\mathbb{Z}) \setminus \mathrm{Red}_{f^{n-1}}(\mathbb{Z})$ infinite? As a direct consequence of Theorem 1.2, there are no such polynomials f admitting no indecomposable factor of degree ≤ 6:

Corollary 1.3. *Let $f \in \mathbb{Q}[x]$ be a polynomial of degree > 1 that does not factor through an indecomposable of degree ≤ 6. Then $\mathrm{Red}_{f^n}(\mathbb{Z}) \setminus \mathrm{Red}_f(\mathbb{Z})$ is finite.*

A natural arising open problem is to determine the exceptional polynomials f (with a factor of degree $2, 3$ or 4) for which $\mathrm{Red}_{f^n}(\mathbb{Z}) \setminus \mathrm{Red}_f(\mathbb{Z})$ is infinite for some $n \ge 2$ and for which n is this possible.

Functional equations. For polynomials $f, g \in \mathbb{C}[x]$, the solutions to the functional equation

$$f(X(z)) = g(Y(z)) \tag{1.1}$$

in polynomials $X, Y \in \mathbb{C}[z]$ are known by Ritt's theorems, cf. [ZM08]. Avanzi–Zannier [AZ01] raise the problem of determining the solutions in rational functions $X, Y \in \mathbb{C}(z)$.

As for the DLS problem, this problem is partially motivated (cf. [DLS61], or [AZ01, Pg. 1]) by the question: when is $f(\mathbb{Q}) \cap g(\mathbb{Q})$ (resp. $f(\mathbb{Z}) \cap g(\mathbb{Z})$) infinite for $f, g \in \mathbb{Q}[x]$? Or

equivalently, when does the curve $f(x) = g(y)$ admit infinitely many rational (resp. integral) points? The solution for integral points was given by Bilu–Tichy [BT00] and a solution for rational points was announced by Zieve et al. in 2012, cf. [Zie12, DHH$^+$12, CDH$^+$12] but have not yet appeared. By Faltings' (resp. Siegel's) theorem, such curves have a component of genus ≤ 1 (resp. 0). The existence of genus-0 component is equivalent to the solvability of (1.1) in $X, Y \in \mathbb{C}(z)$.

The problem naturally divides into two cases according to the reducibility of the curve $f(x) = g(y)$. Solutions in the irreducible case have appeared in various cases, see e.g. [Pak10, Pak18, HT23]. However, with the exception of cases where $f = cg$ for $c \in \mathcal{C}$ [AZ03], or cases where the degree of one of the polynomials is much larger than the other's [Pak23b, Thm. 1.3] or [Fri23], little has appeared in the literature on the reducible case.

Our solution to the DLS problem gives a simple approach to the reducible case. In particular, the following consequence of Theorem 1.1 and [AZ03] shows that when $f(x) = g(y)$ is reducible, f, g have to factor over $\mathbb{C}$, in a certain way, through x^n or T_n or few sporadic polynomials. Note that given $f, g \in \mathbb{C}[x]$ and $X, Y \in \mathbb{C}(z)$ satisfying (1.1), one obtains other solutions $(w \circ f)(X(z)) = (w \circ g)(Y(z))$ by composing with $w \in \mathbb{C}[z]$. To avoid these trivial extra solutions, call (f, g) a *minimal pair* admitting a solution $f(X(z)) = g(Y(z))$, $X, Y \in \mathbb{C}(z)\backslash\mathbb{C}$ if there is no $w \in \mathbb{C}[X]$ of degree > 1 such that $f = w \circ f_1$, $g = w \circ g_1$ such that (f_1, g_1) also has a solution $f_1(X_1(z)) = g_1(Y_1(z))$, for some $X_1, Y_1 \in \mathbb{C}(z) \setminus \mathbb{C}$.

Corollary 1.4. *Suppose $f, g \in \mathbb{C}[x]$ is a minimal pair admitting a solution $f(X(z)) = g(Y(z))$ for some $X, Y \in \mathbb{C}(z) \setminus \mathbb{C}$, and that $f(x) - g(y) \in \mathbb{C}[x, y]$ is reducible. Assume further that f does not factor through an indecomposable polynomial of degree ≤ 4. Then one of the following holds for some $\mu, u, v \in \mathbb{C}[x]$ with $\deg(\mu) = 1$:*

1. *$f = \mu \circ x^n \circ u$ and $g = \mu \circ x^n \circ v$ for $n \geq 2$;*
2. *$f = \mu \circ T_n \circ u$ and $g = \mu \circ T_n \circ v$ for $n \geq 2$;*
3. *$f = \mu \circ P_i \circ u$ and $g = \mu \circ P_i \circ v$, for $i \in \{1, 2, 3\}$, where $P_1(x) = x^a(x-1)^b$ for coprime a, b, and P_2, P_3 are the (degree 5 and 7) polynomials from* [AZ03, Def. 2.1].
4. *$f = \mu \circ h_1 \circ u$ and $g = \mu \circ h_2 \circ v$, where $\{h_1, h_2\}$ is among one of the pairs of degree-7 or degree-13 polynomials appearing in §5.1 or §5.3, resp., of* [CNC99].

The corollary is proved in Section 5.3 and further restrictions on the shapes of the involded decomposition are discussed after it.

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, and of Labex CEMPI (ANR-11-LABX-0007-01).

2. Basic setup and Preliminaries

Let k be a field of characteristic 0. In the whole paper, all groups actions are left actions.

2.1. **Monodromy groups.** A *map* $f : \mathcal{X} \to \mathcal{Y}$ defined 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 $[k(\mathcal{Y}) : k(\mathcal{X})]$.

Let $f : \mathcal{X} \to \mathcal{Y}$ be a map of degree d defined over k. The *monodromy group* $\mathrm{Mon}_k(f)$ 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 $f_1(X) - tf_2(X) \in k(t)[X]$.

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.

Let $f, g \in k(X) \setminus k$. We say that f and g are *linearly related over* k, and denote $f \sim_k g$, if there exist $\mu, \nu \in k(X)$ of[4] degree 1 such that $f = \mu \circ g \circ \nu$. Note that the degree of $f \in k(X) \setminus k$ is $\max\{\deg(f_1), \deg(f_2)\}$, where $f = f_1/f_2$ for coprime $f_1, f_2 \in k[X]$.

Note that every polynomial $f \in k[X] \setminus k$ with cyclic monodromy group is well known to be linearly related to X^n. We call such polynomials *cyclic*. Similarly, every polynomial $f \in k[X] \setminus k$ with dihedral monodromy group is linearly related over $\overline{k}$ to a 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 call such polynomials *dihedral*. Note that for both cyclic and dihedral polynomials f of degree n, the group $\mathrm{Mon}_k(f)$ contains a regular cyclic group 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, the holomorph of C_n.

Note that more generally, every indecomposable polynomial f of degree $p \geq 5$ with solvable monodromy group is of prime degree and is either cyclic or dihedral, so that $\mathrm{Mon}_k(f)$ embeds in $\mathrm{AGL}_1(p)$ and its action is equivalent to the action on $\mathbb{F}_p$. Finally, note:

Remark 2.1. For any prime p, every intransitive subgroup $U \leq \mathrm{AGL}_1(p)$ fixes a point[5]. For $p = 2$, the claim holds trivially. Now assume that p is odd. Then we can write $U = \langle U \cap \mathbb{F}_p, (a, b)\rangle$, for some $\sigma = (a, b) \in \mathbb{F}_p \rtimes \mathbb{F}_p^\times$. By the intransitivity of U, we have $U \cap \mathbb{F}_p = 0$. Since $U \neq 1$, it follows that $b \neq 1$. Therefore, U fixes $a/(1 - b) \in \mathbb{F}_p$.

Moreover, if n is a composite number and U is an intransitive subgroup of $\mathrm{AGL}_1(n)$, then there exists a divisor $d|n$ which is either prime or equal to 4, such that U projects to an intransitive subgroup of $\mathrm{AGL}_1(d)$. Indeed, this is the group-theoretical wording of what is commonly known as Capelli's lemma.

2.2. **Polynomial decompositions.** Recall that the monodromy group $\mathrm{Mon}_k(f)$ of a composition $f = g \circ h$ of two maps $g : \mathcal{Y} \to \mathbb{P}^1, h : \mathcal{X} \to \mathcal{Y}$ is a subgroup of $A \wr B := A^d \rtimes B$,

[4]called also a *linear fractional*.

[5]Here, $\mathrm{AGL}_1(p)$ can be more generally replaced by a Frobenius group.

where $A := \mathrm{Mon}_k(h)$; $B := \mathrm{Mon}_k(g)$; $d = \deg(g)$; and B acts on A^d by permuting the d copies. 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 $k(\mathcal{Y})/k(t)$, 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 closures of g^*, and f^*, resp., the block kernel coincides with $\mathrm{Gal}(\Omega/\Omega')$, while the block stabilizer coincides with $\mathrm{Gal}(\Omega/k(t,b))$, where $k(t,b)$ is the conjugate of $K(\mathcal{Y})$ corresponding to b.

For polynomial decompositions, Abhyankar's lemma implies the block kernel is nontrivial, see e.g. [KN24, Lemma 2.8]. To be more precise, we have:

Lemma 2.2. *Suppose $f = g \circ h \in k[X] \setminus k$ with $\deg(f), \deg(g) \geq 2$. Then the order of the block kernel $K = \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(g))$ is divisible by $\deg(h)$.*

Proof. Let x be a root of $f(X) = t$ and let $w = h(x)$. Denote by $\Omega/k(t)$ the Galois closure of $k(x)/k(t)$. Note that $\Omega^K/k(t)$ is the Galois closure of $k(w)/k(t)$. By Abhyankar's lemma and the ramification index at ∞, the extensions $\Omega^K/k(w)$ and $k(x)/k(w)$ are linearly disjoint. Therefore $\deg(h) = [k(x) : k(w)]|[\Omega : \Omega^K] = |K|$. □

Recall [ZM08, Theorem 2.1.]:

Theorem 2.3 (Ritt's first theorem)**.** *Let $f \in k[X]$ be a polynomial of degree ≥ 2. Consider two complete decompositions[6] $\mathcal{U}$ and $\mathcal{V}$ of f. Then there exists a finite sequence $\mathcal{S}$ of complete decompositions of f such that $\mathcal{U}, \mathcal{V} \in \mathcal{S}$ and every pair of consecutive decompositions in $\mathcal{S}$ are Ritt neighbors[7].*

The following result, which relates decompositions over k and decompositions over $\overline{k}$, is based on Ritt's first theorem, and follows from [FM69]:

Theorem 2.4 (Fried–MacRae)**.** *Suppose $f = f_1 \circ \cdots \circ f_r \in k[X] \setminus k$ for indecomposable polynomials $f_i \in \overline{k}[X]$ $(1 \leq i \leq r)$. Then there exist linear polynomials $\ell_1, \ldots, \ell_{r-1} \in \overline{k}[X]$ such that $g_1 = f_1 \circ \ell_1 \in k[X]$, $g_r = \ell_{r-1}^{-1} \circ f_r \in k[X]$ and $g_i = \ell_{i-1}^{-1} \circ f_i \circ \ell_i \in k[X]$ for all $2 \leq i \leq r-1$. In this case, we have $f = g_1 \circ \cdots \circ g_r$.*

2.3. **Reducibility.** Given $f, g \in k(X) \setminus k$, the curve $f(X) = g(Y)$ is birational to the fiber product of $\mathbb{P}^1 \#_{f,g} \mathbb{P}^1$ 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 $f(X) - t \in k(t)[X]$ and $g(Y) - t \in k(t)[Y]$, resp., are linearly disjoint over $k(t)$.

In particular, if the curve $f(X) = g(Y)$ is reducible, then $f \circ u(X) = g \circ v(Y)$ is reducible for every $u, v \in k(X) \setminus k$. Thus, the Davenport–Lewis–Schinzel problem reduces to classifying the pairs $f, g \in k(X) \setminus k$ that are minimally reducible:

[6] A *complete decomposition* of f is a decomposition $f = f_1 \circ \cdots \circ f_r$ for indecomposable polynomials $f_1, \ldots, f_r \in k[X]$.

[7] Complete decompositions $f = f_1 \circ \cdots \circ f_r$ and $f = \tilde{f}_1 \circ \cdots \circ \tilde{f}_r$ are *Ritt neighbors* if there exists $1 \leq i < r$ such that

- $f_j = \tilde{f}_j$ for $j \notin \{i, i+1\}$, and
- $f_i \circ f_{i+1} = \tilde{f}_i \circ \tilde{f}_{i+1}$.

Definition 2.5. We say that $f, g \in k(X) \setminus k$ is a *minimally reducible pair* if $f(X) = g(Y)$ is reducible and $f_1(X) = g_1(Y)$ is irreducible for every decomposition $f = f_1 \circ f_2$ and $g = g_1 \circ g_2$ such that $\deg(f_1) < \deg(f)$ or $\deg(g_1) < \deg(g)$.

Clearly every pair f, g for which $f(X) = g(Y)$ is reducible factors as $f = f_1 \circ f_2$, $g = g_1 \circ g_2$ for a minimally reducible pair f_1, g_1.

The following well known lemma shows that minimally reducible pairs have a common Galois closure:

Lemma 2.6. *Let $f, g \in k(X) \setminus k$ be a minimally reducible pair, and $k(x)$ and $k(y)$ the root fields of $f(X) - t$ and $g(X) - t \in k(t)[X]$, resp. Then $k(x)/k(t)$ and $k(y)/k(t)$ have the same Galois closure.*

Proof. Suppose on the contrary $k(y)$ is not contained in the Galois closure Ω of $k(x)/k(t)$. Since $k(x)$ and $k(y)$ are not linearly disjoint over $k(t)$, so are $k(x)$ and $k(y) \cap \Omega$ by [KN24, Lemma 2.11]. Since $k(y) \cap \Omega = k(y_1)$ is properly contained in $k(y)$, we may write $g = g_1 \circ g_2$ for $g_1, g_2 \in k(X) \setminus k$ with $\deg(g_1) < \deg(g)$ such that $t = g_1(y_1)$ and $y_1 = g_2(y)$. Thus, g_1, f is a reducible pair with $\deg(g_1) < \deg(g)$, contradicting the minimality of the pair f, g. □

2.4. **Wreath products of affine groups.** For polynomial maps $f, g \in k[X]$ of prime degrees p and q resp., with solvable monodromy groups, we have $\mathrm{Mon}_k(f \circ g) \leq A \wr B$, where $A \leq \mathrm{AGL}_1(q)$ and $B \leq \mathrm{AGL}_1(p)$ [8]. This section presents preliminary results on subgroups of $A \wr B$ for such A, B and firstly on normal subgroups of A^p:

Lemma 2.7. *Let $C_p \lneq H \leq \mathrm{AGL}_1(p)$ properly contain C_p, and $n \in \mathbb{N}$. Then every epimorphism $\psi : H^n \twoheadrightarrow H$ factors through the projection to one of the n coordinates.*

Proof. Since $\gcd(p, p-1) = 1$, we have $\psi(C_p^n) = C_p$. Viewing ψ as a surjective linear functional on $\mathbb{F}_p^n = \oplus_{i=1}^n \mathbb{F}_p e_i$, some direct summand $\mathbb{F}_p e_i$ is mapped onto $\mathbb{F}_p$. Let $\pi_i : H^n \to H$ denote the projection to the i-th coordinate. Since $\ker(\pi_i)$ and $\mathbb{F}_p e_i$ commute so are their images, and hence elements of $\ker(\pi_i)$ of order coprime to p have trivial ψ-images.

Now assume on the contrary that $\psi(\mathbb{F}_p e_j) = C_p$ for some $j \neq i$. Since every element in $\ker(\pi_j)$ of order coprime to p has trivial ψ-image, and since $\langle \ker(\pi_i), \ker(\pi_j) \rangle = H^n$, every element whose order is coprime to p has trivial ψ-image, contradicting the surjectivity of ψ. Thus $\psi(\mathbb{F}_p e_j) = 1$ for all $j \neq i$. Since in addition elements of $\ker(\pi_i)$ of order coprime to p have trivial ψ-image by the first paragraph, ψ factors through π_i. □

We describe normalizers and commutator subgroups of transitive subgroups of $G := \mathrm{AGL}_1(q) \wr \mathrm{AGL}_1(p)$ 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.

Proposition 2.8. *For primes p, q, let $\langle H, \sigma \rangle \leq \mathrm{AGL}_1(q) \wr C_p$ be a subgroup, where $H \leq C_q^p$ is σ-invariant: $H^\sigma = H$, and σ is a lift of C_p of order p or pq with $\sigma^p \in H$. Then 1) $[H : [H, \langle \sigma \rangle]] \mid q$, and 2) $[\mathcal{N}_{C_q^p}(\langle H, \sigma \rangle) : H] \mid q$.*

[8] More precisely, we can take $A = \mathrm{Mon}_k(g)$ and $B = \mathrm{Mon}_k(f)$.

If $I \leq H$ is a σ-invariant subgroup such that $\langle H, \sigma\rangle/I$ is abelian, then 3) $[H : I] \mid q$. In particular, if $\langle H, \sigma\rangle$ is abelian, then 4) $|\mathcal{N}_{C_q^p}(\langle H, \sigma\rangle)| \mid q^2$.

Proof. The conjugation by σ induces an automorphism $\overline{\sigma} \in \mathrm{Aut}(C_q^p)$ of order p, which endows C_q^p with an $\mathbb{F}_q[\overline{\sigma}]$-module structure. Note that $\mathbb{F}_q[\overline{\sigma}] \simeq \mathbb{F}_q[x]/(x^p - 1)$ via $x \mapsto \overline{\sigma}$, and that $C_q^p = \mathbb{F}_q[\overline{\sigma}]\mathbf{e}$ is a cyclic $\mathbb{F}_q[\overline{\sigma}]$-module generated by $\mathbf{e} := (1, 0, \ldots, 0)$. Thus, C_q^p is a quotient of the free module $\mathbb{F}_q[\overline{\sigma}]$ of rank 1. Since both have the same cardinality, it follows that $C_q^p \cong \mathbb{F}_q[\overline{\sigma}]$ as an $\mathbb{F}_q[\overline{\sigma}]$-module. Henceforth, we identify C_q^p with $\mathbb{F}_q[\overline{\sigma}]$ under this isomorphism. Therefore H is a submodule of the form $g\mathbb{F}_q[\overline{\sigma}]$, where $g \in \mathbb{F}_q[\overline{\sigma}]$ divides the characteristic polynomial $\overline{\sigma}^p - 1$.

To see 1), note that, in $\mathbb{F}_q[\overline{\sigma}]$, the element $[g, \sigma] = g\sigma g^{-1}\sigma^{-1} = g(\overline{\sigma} \cdot g^{-1}) \in H$ identifies with $g - \overline{\sigma}g = -(\overline{\sigma} - 1)g \in \mathbb{F}_q[\overline{\sigma}]$. Thus, $[H, \langle\sigma\rangle]$ identifies with $(\overline{\sigma} - 1)g\mathbb{F}_q[\overline{\sigma}]$. Since the latter is an $\mathbb{F}_q$-subspace of codimension at most 1 in $g\mathbb{F}_q[\overline{\sigma}]$, we obtain $[H : [H, \langle\sigma\rangle]] \mid q$.

To prove 2), we first claim that $\mathcal{N} = \mathcal{N}_{C_q^p}(\langle H, \sigma\rangle)$ is also invariant under σ. Indeed, let $u \in \mathcal{N}$. Then $u\sigma^{-1}u^{-1} = h\sigma^k$ for some $h \in H$ and k. Considering the projection on C_p, we get $k = -1 + pr$ for some $r \geq 0$. Hence, we have

$$\sigma u \sigma^{-1} u^{-1} = (\sigma h \sigma^{-1})\sigma^{pr} \in H\sigma^{pr} = H.$$

Since $H \leq \mathcal{N}$ (as $H^\sigma = H$), we obtain $\sigma u \sigma^{-1} \in Hu \subset \mathcal{N}$, proving the claim. It follows that $H \leq \mathcal{N} \leq C_p^q$ is an $\mathbb{F}_q[\overline{\sigma}]$-submodule, so that $\mathcal{N} = f\mathbb{F}_q[\overline{\sigma}]$ for some $f \mid g \in \mathbb{F}_q[\overline{\sigma}]$. Since $\mathcal{N}$ normalizes $\langle H, \sigma\rangle$, we have $[\mathcal{N}, \langle\sigma\rangle] \subseteq H$. As in the proof of (1), $[\mathcal{N}, \langle\sigma\rangle] = (\overline{\sigma} - 1)f\mathbb{F}_q[\overline{\sigma}]$, so that the inclusion $[\mathcal{N}, \langle\sigma\rangle] \subseteq H$ implies $g \mid (\overline{\sigma} - 1)f$. From $(\overline{\sigma} - 1)f\mathbb{F}_q[\overline{\sigma}] \leq H = g\mathbb{F}_q[\overline{\sigma}] \leq \mathcal{N} = f\mathbb{F}_q[\overline{\sigma}]$ and $[\mathbb{F}_q[\overline{\sigma}] : (\overline{\sigma} - 1)\mathbb{F}_q[\overline{\sigma}]] \mid q$, we deduce that $[\mathcal{N} : H] \mid q$.

To see 3), note that $[H, \langle\sigma\rangle] \leq I \leq H$, so that $[H : I] \mid [H : [H, \langle\sigma\rangle]]$ and the latter divides q by 1).

To see 4), pick $I = 0$, so that the combination of 2) and 3) gives:

$$|\mathcal{N}_{C_q^p}(\langle H, \sigma\rangle)| = [\mathcal{N}_{C_q^p}(\langle H, \sigma\rangle) : H] \cdot |H| \mid q^2.$$

□

Lemma 2.9. *Let $K \leq \mathrm{AGL}_1(p)^n$ such that each component projection contains C_p. Then $\mathrm{soc}(K) = K \cap C_p^n$.*

Proof. Since K is solvable, $\mathrm{soc}(K)$ 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 $\mathrm{AGL}_1(p)$, i.e., are contained in C_p, it follows that $H_q = 1$ for every $q \neq p$, so $\mathrm{soc}(K) \subseteq K \cap C_p^n$. For the converse inclusion, note that $K \cap C_p^n$ is a semisimple module under the action of $K/(K \cap C_p^n)$, meaning that the submodule $\mathrm{soc}(K)$ has a complement N, which is in particular normal in K. By the definition of the socle, this implies $N = \{1\}$. □

2.5. **A lemma on 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 $\varphi(\mathcal{X}) \cap O_k$ 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 $|\varphi^{-1}(\infty)| \leq 2$. 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 zero 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. The following lemma describes Siegel functions that factor through solvable polynomials.

Lemma 2.10. *Let $q \geq 3$ be a prime. Let $U \in \overline{k}[X]$ be of degree ≥ 2, let $V \in \{X^q, T_q\}$ and let $\ell \in \overline{k}(X)$ be a linear fractional. Assume that $U \circ \ell \circ V$ is a Siegel function.*

1. *If $V = X^q$, then $\ell = \frac{aX+b}{X}$ for some $a \in \overline{k}, b \in \overline{k}^\times$, or ℓ is a linear polynomial. In the former case, $(U \circ \ell \circ V)(1/X) = U \circ (bX + a) \circ V$.*
2. *If $V = T_q$ and $q \geq 5$, then ℓ is a linear polynomial.*

Proof. (1) Assume $V = X^q$. Since $q \geq 3$, we have $|V^{-1}(c)| \geq 3$ for all $c \in \overline{k}^\times$. Hence $\ell^{-1}(\infty) \in \{0, \infty\}$, which implies that $\ell(X) = \frac{aX+b}{X}$ for some $a \in \overline{k}, b \in \overline{k}^\times$, or that ℓ is a linear polynomial. In the former case, we have $\ell \circ V \circ (1/X) = a + bX^q = (bX + a) \circ V$, giving the second equality.

(2) Assume $V = T_q$. Since $q \geq 5$, we have $|V^{-1}(c)| \geq 3$ for all $c \in \overline{k}$. Hence $\ell^{-1}(\infty) = \infty$, so ℓ is a linear polynomial.

□

2.6. **Composition of two indecomposable solvable polynomials.** Our method for proving Theorem 1.1 relies on the 'largeness' of the monodromy groups of solvable polynomials:

Theorem 2.11. *Assume that $k = \overline{k}$. Suppose $h \in k[X] \setminus k$ (resp., $g \in k[X] \setminus k$) is linearly related over k to X^p or T_p (resp., T_q or X^q) for primes $p, q \geq 3$. Assume $g \circ h$ is not related over k to X^{pq} or T_{pq}. Then, the block kernel $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$ contains C_p^q. Moreover:*

1. *If h is linearly related over k to X^p, then $\Gamma = C_p^q$.*
2. *If h is linearly related over k to T_p, then either $\Gamma = D_p^q$ or*

$$\Gamma = \left\{(a_1, \ldots, a_q) \in D_p^q \mid a_1 \cdots a_q \in C_p\right\}.$$

The proof of the above theorem is given in Section 4.

3. Reducing the solvable case of Theorem 1.1 to length 2 compositions

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 will be discussed in Section 5.

Theorem 3.1. *Let k be a field of characteristic 0. Let $f \in k[X] \setminus k$ be a polynomial with solvable monodromy group such that $\deg(f)$ is coprime to 6, 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 $\deg(h) > 1$.*

3.1. **Diagonality of the kernel.** Recall that a subgroup D of a power B^r, $r \geq 1$, is a *diagonal* subgroup if each of its r projections to B is injective. We start with the following key theorem showing that the block kernel is diagonal for minimally reducible pairs:

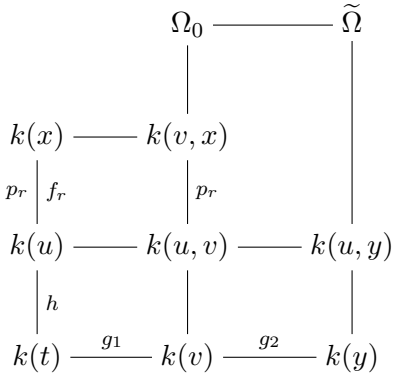
Theorem 3.2. *Suppose that an odd degree polynomial $f \in k[X]$ and a Siegel function $g \in k(X)$ form a minimally reducible pair, and that $f = h \circ f_r$ for indecomposable $f_r \in k[X]$ of degree p_r with solvable monodromy $\mathrm{Mon}_k(f_r)$. Then the kernel $K := \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(h))$ is a diagonal subgroup of $\mathrm{Mon}_k(f_r)^{\deg(h)}$ with $|\mathrm{soc}(K)| = p_r$.*

We shall need the following lemma:

Lemma 3.3. *Suppose that $f \in k[X]$ and $g = \gamma_1/\gamma_2 \in K(X)$ form a minimally reducible pair for coprime $\gamma_1, \gamma_2 \in k[X]$. 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 $p_r := \deg(f_r) \neq 4$. Then the fiber product $\mathbb{P}^1 \#_{g,h} \mathbb{P}^1 \to \mathbb{P}^1$ of g and h factors through f, so that $p_r \mid \deg(g_2)$.*

Equivalently, letting x, y be the roots of $f(X) - t$ and $\gamma_1(X) - t\gamma_2(X) \in k(t)[X]$, resp., and $u = f_r(x)$, 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 $v = g_2(y)$. Recall that 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 $\Omega_0/k(u,v)$ (resp., $\widetilde{\Omega}/k(u,v)$) 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 may identify $\mathrm{Gal}(\Omega_0/k(u,v))$ with a subgroup of $\mathrm{Mon}_k(f_r)$. Since f_r is indecomposable of degree $\neq 4$ with solvable monodromy, as in Section 2, these subgroups identify with subgroups of $\mathrm{AGL}_1(p_r)$, where $p_r = \deg(f_r)$ is prime. 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 $k(v,x) \subseteq \widetilde{\Omega}$ and hence $\Omega_0 \subset \widetilde{\Omega}$. Since the image of $\mathrm{Gal}(\widetilde{\Omega}/k(u,y))$ in $\mathrm{Gal}(\Omega_0/k(u,v)) \leq \mathrm{AGL}_1(p_r)$ is intransitive, Remark 2.1 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 $k(v,x_0) \subseteq k(u,y)$. 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. Moreover, since $x_0 \in k(u,y)$, the degree $p_r = [k(x_0,v) : k(u,v)]$ divides $[k(u,y) : k(u,v)] = [k(y) : k(v)] = \deg(g_2)$.



□

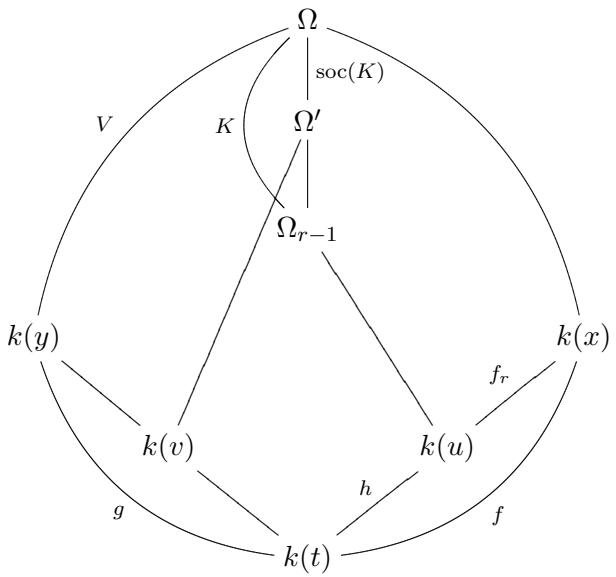
In the setup of Theorem 3.2, we get:

Corollary 3.4. *Let Ω be the common Galois closure (obtained by Lemma 2.6) of $f(X)-t$ and $G(X) := \gamma_1(X) - t\gamma_2(X) \in k(t)[X]$, where $g = \gamma_1/\gamma_2$ for coprime $\gamma_1, \gamma_2 \in k[X]$. Then $\Omega^{\mathrm{soc}(K)}(y) = \Omega$ for a root y of $G(X)$.*

Note that group theoretically, the equality $\Omega^{\mathrm{soc}(K)}(y) = \Omega$ means that $V := \mathrm{Gal}(\Omega/k(y))$ and $\mathrm{soc}(K)$ generate a subgroup isomorphic to a semidirect product $\mathrm{soc}(K) \rtimes V$.

Proof. As noted in Section 2, since f_r are indecomposable of degree $p_r \neq 4$ and solvable monodromy group, p_r is prime and $\Gamma_r = \mathrm{Mon}_k(f_r)$ embeds into $\mathrm{AGL}_1(p_r)$. Letting $G_{r-1} := \mathrm{Mon}_k(h)$, we may identify $\mathrm{Mon}_k(f)$ as a subgroup of $\mathrm{AGL}_1(p_r) \wr G_{r-1}$. Moreover, letting Ω_{r-1} be the splitting field of $h(X)-t$, we see that $K = \mathrm{Gal}(\Omega/\Omega_{r-1})$, and that $p_r \mid |K|$ by Lemma 2.2. Since the projections of $K \leq \Gamma_r^{\deg(h)}$ to each of the coordinates are isomorphic [KN24, Remark 3.2], this implies they all contain C_{p_r}. Since $\mathrm{soc}(\Gamma_r) = \mathrm{soc}(\mathrm{AGL}_1(p_r)) = C_{p_r}$, by Lemma 2.9, it follows that $\mathrm{soc}(K) = K \cap C_{p_r}^{\deg(h)}$. Set $\Omega' = \Omega^{\mathrm{soc}(K)}$.

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



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

On the other hand, since $k(y)/k(t)$ and $k(u)/k(t)$ are linearly disjoint, $h(X) - t$ 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 3.3, 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 $k(y,u)$. Thus $k(v,x_0^\sigma) \subset k(u^\sigma, y) \subset \Omega'(y)$, for every $\sigma \in V = \mathrm{Gal}(\Omega/k(y))$. Combining this with the transitivity of $V = \mathrm{Gal}(\Omega/k(y))$, we see that $\Omega'(y)$ contains all $k(t)$-conjugates of x, that is, $\Omega'(y) = \Omega$. □

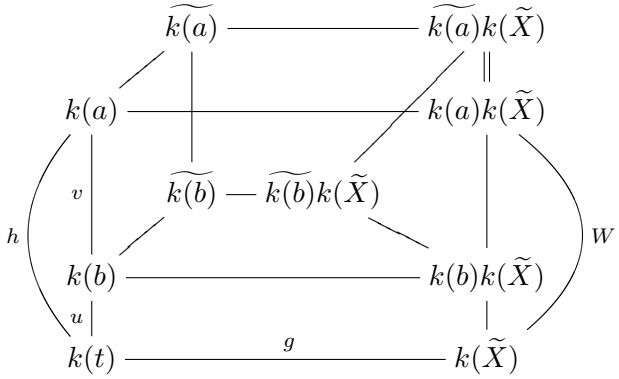
To conclude Theorem 3.2, we need the following proposition and lemma:

Proposition 3.5. *Let p be a prime and let $h = u \circ v : \mathbb{P}^1 \to \mathbb{P}^1$ be a composition of two degree-p maps with solvable monodromy. Suppose that there exists a Galois map $g : \widetilde{X} \to \mathbb{P}^1$ whose fiber product $\mathbb{P}^1 \#_{h,g} \widetilde{X}$ with h is irreducible, and that the pullback h_g of h along g has abelian monodromy group. Then the kernel K of the projection $\mathrm{Mon}_k(h) \to \mathrm{Mon}_k(u)$ has a socle of cardinality at most p^2.*

Lemma 3.6. *Let L/K and M/K be linearly disjoint extensions such that ML/L and L/K are Galois. Then ML/K is Galois.*

Proof. First note that, by linear disjointness, any $\sigma \in \mathrm{Gal}(L/K)$ extends to $\widetilde{\sigma} \in \mathrm{Aut}(ML/M) \leq \mathrm{Aut}(ML/K)$. Now we are going to prove that $(ML)^{\mathrm{Aut}(ML/K)} = K$, that is ML/K is Galois. For that, let $a \in (ML)^{\mathrm{Aut}(ML/K)}$. Since ML/L is Galois, we have $a \in (ML)^{\mathrm{Gal}(ML/L)} = L$. Moreover, for any $\sigma \in \mathrm{Gal}(L/K)$, we have $\sigma(a) = \widetilde{\sigma}(a) = a$. As L/K is Galois, we obtain $a \in L^{\mathrm{Gal}(L/K)} = K$. Consequently $(ML)^{\mathrm{Aut}(ML/K)} = K$. □

Proof of Proposition 3.5. Let a be such that $h(a) = t$, that is, a root of $h_1(X) - th_2(X) \in k(t)[X]$, where $h = h_1/h_2$ for coprime $h_1, h_2 \in k[X]$. Set $b := v(a)$ and denote by $\widetilde{k(a)}/k(t)$ (resp., $\widetilde{k(b)}/k(t)$) the Galois closure of $k(a)/k(t)$ (resp., $k(b)/k(t)$) and by $k(\widetilde{X})$ the function field of $\widetilde{X}$. By assumption, $k(a)/k(t)$ and $k(\widetilde{X})/k(t)$ are linearly disjoint. Since $k(a) \cdot k(\widetilde{X})/k(\widetilde{X})$ is the function field extension corresponding to h_g, and since $\mathrm{Mon}_k(h_g)$ is abelian, the extension is Galois and its group $W = \mathrm{Gal}(k(a)k(\widetilde{X})/k(\widetilde{X})) \simeq \mathrm{Mon}_k(h_g)$ is abelian. Moreover, $k(a)k(\widetilde{X})/k(t)$ is Galois by Lemma 3.6. Since it is Galois and contains $k(a)$, it also contains $\widetilde{k(a)}$ so that $\widetilde{k(a)}k(\widetilde{X}) = k(a)k(\widetilde{X})$.



Since u, v have degree p and solvable monodromy groups, as in Section 2, we identify both $\mathrm{Mon}_k(u)$ and $\mathrm{Mon}_k(v)$ as permutation subgroups of $\mathrm{AGL}_1(p)$, so that $\mathrm{Gal}(\widetilde{k(a)}/k(t)) \leq$

$\mathrm{AGL}_1(p) \wr \mathrm{AGL}_1(p)$. Since $[k(b)k(\widetilde{X}) : k(\widetilde{X})] = p$, the projection of the p-elementary abelian group $W \leq \mathrm{AGL}_1(p) \wr \mathrm{AGL}_1(p)$ to $\mathrm{AGL}_1(p)$ contains C_p. Since $H = W \cap \mathrm{AGL}_1(p)^p \leq C_p^p$ is the kernel of this projection and since $p^2 = [k(a)k(\widetilde{X}) : k(\widetilde{X})] = |W|$, we get $|H| = p$. Since $W \lhd \mathrm{Gal}(k(a)k(\widetilde{X})/k(t))$, the subgroup $\mathrm{soc}(K)$ also normalizes W in $\mathrm{Mon}_k(h)$. Hence, $|\mathrm{soc}(K)| \mid p^2$ by Proposition 2.8.[9] □

Lemma 3.7. *Let $f, g \in k(X) \setminus k$ be a minimally reducible pair such that $f = f_1 \circ f_2$ for $f_2 \in k(X)$ whose degree n is an odd composite number. Then f_2 is not linearly related to T_n or to X^n over $\overline{k}$.*

Proof. Suppose on the contrary that f_2 is linearly related over $\overline{k}$ to T_n or X^n, so that $\mathrm{Mon}_k(f_1) \leq \mathrm{AGL}_1(n)$. Suppose that x, y are such that $f(x) = t$ and $g(y) = t$, that is, x, y are roots of $p_1(X) - tp_2(X), q_1(X) - tq_2(X) \in k(t)[X]$ resp., where $f = p_1/p_2$, $g = q_1/q_2$ for coprime $p_1, p_2 \in k[X]$ and $q_1, q_2 \in k[X]$, resp. Let $u = f_2(x)$, and Ω' the Galois closure of $k(x)/k(u)$. Since $k(y,u)/k(u)$ and $k(x)/k(u)$ are not linearly disjoint, $L = k(y,u) \cap \Omega'$ is not linearly disjoint from $k(x)$ over $k(u)$. [10]

Since n is composite, Remark 2.1 and the Galois correspondence imply there exists an intermediate field $k(u) \subsetneq L_0 \subsetneq k(x)$ such that $L/k(u)$ and hence $k(y,u)/k(u)$ are not linearly disjoint from $L_0/k(u)$, contradicting the minimal reducibility of f and g. □

Proof of Theorem 3.2. Retain the notation from the proof of Corollary 3.4. By definition of $k(v)$, we have $[k(y) : k(v)] = |\mathrm{soc}(K)| = p_r^\ell$ for some $\ell \geq 1$. By assumption p_r is odd. Assume on the contrary that $\ell \geq 2$. Write $v = v(y)$ for $v \in k[y]$ (resp., $v \in k(y)$ Siegel) and consider a decomposition $v = v_1 \circ \cdots \circ v_m$, for indecomposable $v_i \in k[X]$ (resp., functions $v_i \in k(X)$ linearly related over $\overline{k}$ to Siegel functions), $i = 1, \ldots, m$. We claim that $m = \ell$ and each v_i $(1 \leq i \leq r)$ is linearly related over $\overline{k}$ to X^{p_r} or T_{p_r}. If g is polynomial, this follows from Ritt's first decomposition theorem. If g is a Siegel function, then v is linearly related to over $\overline{k}$ to a polynomial; indeed, letting $g = h \circ v$ for some $h \in k(X) \setminus k$ and $\lambda \in g^{-1}(\infty)$, note that, since $|v^{-1}(\lambda)| \leq 2$, $\deg(v)$ is odd, and the ramification at ∞ for g is odd, it follows that $|v^{-1}(\lambda)| = 1$. Therefore, for every $1 \leq i \leq m$, we have $\deg(v_i) = p_r$ and v_i is linearly related over $\overline{k}$ to X^{p_r} or T_{p_r}, so $m = \ell$.

By Lemma 2.10, $v_{m-1} \circ v_m$ is linearly related over $\overline{k}$ to $U \circ \theta \circ V$, where θ is a linear polynomial and $U, V \in \{X^{p_r}, T_{p_r}\}$. Let $K' = \ker(\mathrm{Mon}_k(U \circ \theta \circ V) \to \mathrm{Mon}_k(U))$. By Proposition 3.5, $|\mathrm{soc}(K')| \leq p_r^2$. Hence, by Theorem 2.11, $U \circ \theta \circ V$ is linearly related over $\overline{k}$ to $T_{p_r^2}$ or $X^{p_r^2}$. Therefore $v_{m-1} \circ v_m$ is linearly related to $X^{p_r^2}$ or $T_{p_r^2}$ over $\overline{k}$, which contradicts Lemma 3.7. Thus $\ell = 1$, and $\mathrm{soc}(K)$ is diagonal. □

3.2. **Relating the kernel to the two-step kernel.** Theorem 3.2 is a contrast to Theorem 2.11 for compositions of two polynomials. The following relates the two relevant kernels:

[9] Note that $W = \langle H, \sigma \rangle$ for some σ such that $H^\sigma = H$, and that the projection of σ generates C_p.

[10] Indeed, if N/K and M/K are non-linearly disjoint finite separable extensions, then neither are N/K and $\widetilde{N} \cap M/K$, where $\widetilde{N}/K$ denotes the Galois closure of N/K.

Proposition 3.8. *Suppose $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in k[X]$ of prime degrees p_{r-1} and p_r, resp., and solvable monodromy. Let $G = \mathrm{Mon}_k(f)$, let $K = \ker(G \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{r-1}))$, let $\overline{G} = \mathrm{Mon}_k(f_{r-1} \circ f_r)$ and let $\overline{G}_{p_r} = \overline{G} \cap C_{p_r}^{p_{r-1}}$. Then $[\overline{G}_{p_r} : \overline{\mathrm{soc}(K)}] \mid p_r^2$, where $\overline{\mathrm{soc}(K)}$ denotes the image of $\mathrm{soc}(K)$ in $\overline{G}$.*

Proof. Let $\mathcal{X}$ be the set of roots of $f(X) - t$ in its splitting field Ω. Fix $x \in \mathcal{X}$, and let $y := f_r(x)$ and $z := f_{r-1}(y)$. Then $G = \mathrm{Gal}(\Omega/k(t))$ also acts on the sets $\mathcal{Y}, \mathcal{Z}$ of conjugates of y and z, resp. The kernels K, N of these actions on $\mathcal{Y}$ and $\mathcal{Z}$, resp., are normal subgroups of G which act on the block $\mathcal{X}_z = (f_{r-1} \circ f_r)^{-1}(z)$. Thus, the images $\overline{K}, \overline{N}$ of these actions are normal subgroups of $\overline{G} \leq \mathrm{AGL}_1(p_r) \wr \mathrm{AGL}_1(p_{r-1})$. Since $\mathrm{soc}(K) = K \cap C_{p_r}^{\deg(f_1 \circ \cdots \circ f_{r-1})}$ (by Lemma 2.9), the image $\overline{\mathrm{soc}(K)}$ of its action on $\mathcal{X}_z$ is contained in $\overline{N}_{p_r} := \overline{N} \cap C_{p_r}^{p_{r-1}}$.

We first claim that $[\overline{G}_{p_r} : \overline{N}_{p_r}] \mid p_r$. Since f_{r-1} is a polynomial, ∞ is totally ramified in $k(y)/k(z)$, but is completely split in the extension of $k(z)$ fixed by $\overline{N}$ as in Lemma 2.2. Hence this fixed field and $k(y)$ are linearly disjoint over $k(z)$, so that $\overline{N}$ acts transitively on the block $f_{r-1}^{-1}(z)$. Thus the image of $\overline{N}$ in $\mathrm{Mon}_k(f_{r-1})$ contains an element σ' of order p_{r-1}. Let $\sigma \in N$ be a lift of this element of order[11] a power of p_{r-1} and $\overline{\sigma}$ its image in $\overline{N}$. Observe next that $\overline{G}_{p_r} \leq \mathcal{N}_{C_{p_r}^{p_{r-1}}}(\langle \overline{N}_{p_r}, \overline{\sigma} \rangle)$: indeed for $a \in \overline{G}_{p_r}$, since $\overline{N} \lhd \overline{G}$, we have $a\overline{\sigma}a^{-1} \in \overline{N}$, so $a\overline{\sigma}a^{-1}\overline{\sigma}^{-1} \in \overline{N} \cap C_{p_r}^{p_{r-1}} = \overline{N}_{p_r}$ and $a\overline{\sigma}a^{-1} \in \langle \overline{N}_{p_r}, \overline{\sigma} \rangle$. Hence, by Proposition 2.8, we get

$$[\overline{G}_{p_r} : \overline{N}_{p_r}] \mid [\mathcal{N}_{C_{p_r}^{p_{r-1}}}(\langle \overline{N}_{p_r}, \overline{\sigma} \rangle) : \overline{N}_{p_r}] \mid p_r, \text{ as claimed.}$$

Finally, we claim that $\langle \overline{\sigma}, \overline{N}_{p_r} \rangle / \overline{\mathrm{soc}(K)}$ is abelian, so that $[\overline{N}_{p_r} : \overline{\mathrm{soc}(K)}] \mid p_r$ by Proposition 2.8, and in total we have $[\overline{G}_{p_r} : \overline{\mathrm{soc}(K)}] \mid p_r^2$ as needed. Since $\mathrm{Mon}_k(f_{r-1}) \leq \mathrm{AGL}_1(p_{r-1})$, the action of N/K on $\mathcal{Y}$ factors through $\mathrm{AGL}_1(p_{r-1})^{\mathcal{Z}}$. Consider the projection $\pi : N/K \to \overline{N}/\overline{K}$ (where the latter acts on $f_{r-1}^{-1}(z)$ not necessarily faithfully), and the preimage of $\overline{N}_{p_r}\overline{K}/\overline{K} = \overline{N}_{p_r}/\overline{\mathrm{soc}(K)}$[12] under π. Let $W \leq N/K$ denote a p_r-Sylow subgroup of this preimage, so that $\pi(W) = \overline{N}_{p_r}/\overline{\mathrm{soc}(K)}$.

Assume first that $p_r \neq p_{r-1}$. Since $C_{p_{r-1}}$ is normal in $\mathrm{AGL}_1(p_{r-1})$, the commutator $[\sigma, w] \in N/K \leq \mathrm{AGL}_1(p_{r-1})^{\mathcal{Z}}$ is an element of order dividing p_{r-1} for every $w \in W$, and hence $\pi([\langle \sigma \rangle, W]) = [\langle \overline{\sigma} \rangle, \overline{N}_{p_r}]$ is a trivial subgroup of $\overline{N}_{p_r}/\overline{\mathrm{soc}(K)}$, so that $\langle \overline{\sigma}, \overline{N}_{p_r} \rangle / \overline{\mathrm{soc}(K)}$ is abelian, as claimed. Henceforth assume that $p_{r-1} = p_r = p$. In this case $\langle \sigma, W \rangle$ is contained in the p-Sylow subgroup of $\mathrm{AGL}_1(p)^{\mathcal{Z}}$ and hence is abelian. Thus $\pi(\langle \sigma, W \rangle) = \langle \overline{\sigma}, \overline{N}_p \rangle / \overline{\mathrm{soc}(K)}$ is abelian as well, proving the claim.

□

3.3. **Proof of Theorem 3.1.** In the rest of the section, we prove Theorem 3.1 assuming Theorem 2.11 whose proof will be provided in Section 4.

Proof of Theorem 3.1. Let $f \in k[X]$ and $g \in k(X)$ be a Siegel function as in Theorem 3.1. We may assume that the pair f, g is minimally reducible.

[11] Such a lift can be of order p_{r-1} or p_{r-1}^2.

[12] Note that since $K/\mathrm{soc}(K)$ is of order coprime to p_r, clearly $\overline{K} \cap \overline{N}_{p_r} = \overline{K} \cap C_{p_r}^{p_{r-1}} = \overline{\mathrm{soc}(K)}$.

Now write $f = f_1 \circ \cdots \circ f_r$ for indecomposable polynomials $f_i \in k[X]$ with $p_i = \deg(f_i) \geq 5$ a prime. Pick roots x and y of $f(X) - t = 0$ and $g(Y) - t = 0$, respectively. By Lemma 2.6, the extensions $k(x)/k(t)$ and $k(y)/k(t)$ have a common Galois closure Ω.

Assume on the contrary that $r \geq 2$. Letting $K = \ker(\mathrm{Mon}_k(f) \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{r-1}))$, we claim that $p_r^3 \mid |\mathrm{soc}(K)|$. Since by assumption $p_r \neq 2$, Lemma 3.7 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 $\overline{k}$. Theorem 2.11 implies that the geometric monodromy group $\mathrm{Mon}_{\overline{k}}(f_{r-1} \circ f_r) \leq \mathrm{AGL}_1(p_r) \wr \mathrm{AGL}_1(p_{r-1})$ contains $C_{p_r}^{p_{r-1}}$ and hence so does $\overline{G} = \mathrm{Mon}_k(f_{r-1} \circ f_r) \leq \mathrm{AGL}_1(p_r) \wr \mathrm{AGL}_1(p_{r-1})$. Therefore, by Proposition 3.8, we get $p_r^{p_{r-1}-2} \mid |\mathrm{soc}(K)|$, and so $p_r^3 \mid |\mathrm{soc}(K)|$ since $p_r \geq 5$, proving the claim. This contradicts Theorem 3.2 which gives $|\mathrm{soc}(K)| = p_r$.

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 Remark 2.1, so that g factors through f as needed. □

4. Proof of Theorem 2.11

In this section, our aim is to prove Theorem 2.11. In §4.1, we begin by establishing some necessary elementary results in linear algebra. In §4.2, we proceed with the proof of Theorem 2.11.

4.1. Linear algebra lemmas.

Let $p, q \geq 2$ be prime numbers. Consider an $\mathbb{F}_p$-vector space

$$W = \mathbb{F}_p \cdot u_0 \oplus \cdots \oplus \mathbb{F}_p \cdot u_{q-1}$$

of dimension q.

Lemma 4.1. *Let $A = \{a_i \mid i \in \mathbb{F}_q\}$ be a set of size q. Let $i_0 \in \mathbb{F}_q^*$ and let $\emptyset \neq S \subset \mathbb{F}_q$ be such that, in the multiset*

$$K = \{a_s, a_{s+i_0} \mid s \in S\},$$

each element appears exactly twice. Then $S = \mathbb{F}_q$.

Proof. Observe that, for any $s \in S$, since a_{s+i_0} appears exactly twice in K, we have $s + i_0 \in S$. Fix $s_0 \in S$. By the observation above, $s_0, s_0 + i_0, s_0 + 2i_0, \ldots, s_0 + (q-1)i_0 \in S$. Since $\mathbb{F}_q = \{s_0, s_0 + i_0, \ldots, s_0 + (q-1)i_0\}$, we get $S = \mathbb{F}_q$. □

Lemma 4.2. *Assume $p, q \geq 3$. Let $i_0 \in \mathbb{F}_q^*$ and let $\emptyset \neq S \subset \mathbb{F}_q$. Then*

$$\sum_{s \in S} \lambda_s \left(u_s + u_{s+i_0}\right) \neq 0,$$

for all $(\lambda_s)_{s \in S} \subset \mathbb{F}_p^*$.

Proof. Assume on the contrary that

$$\sum_{s \in S} \lambda_s \left(u_s + u_{s+i_0}\right) = 0, \tag{4.1}$$

for some $(\lambda_s)_{s \in S} \subset \mathbb{F}_p^*$. Consider the multiset $K = \{u_s, u_{s+i_0} \mid s \in S\}$. From (4.1) and the fact that $\{u_0, \ldots, u_{q-1}\}$ is an $\mathbb{F}_p$-basis of W, each element in K appears exactly twice. By Lemma 4.1, we get $S = \mathbb{F}_q$. Using again (4.1), we deduce that $\lambda_k = -\lambda_{k-i_0}$, for all

$k \in S = \mathbb{F}_q$. Hence $\lambda_0 = (-1)^q \lambda_{0-q\cdot i_0} = (-1)^q \lambda_0 = -\lambda_0$, so $2\lambda_0 = 0$. Since p is odd, we get $\lambda_0 = 0$, a contradiction. □

Lemma 4.3. *Let $i_0 \in \mathbb{F}_q^*$ and let $\emptyset \neq S \subset \mathbb{F}_q$ be such that*

$$\sum_{s\in S} \lambda_s \left(u_s + (p-1)u_{s+i_0}\right) = 0, \tag{4.2}$$

for some $(\lambda_s)_{s\in S} \subset \mathbb{F}_p^*$. Then $S = \mathbb{F}_q$.

Proof. Consider the multiset $K = \{u_s, u_{s+i_0} \mid s \in S\}$. From (4.2) and the fact that $\{u_0, \dots, u_{q-1}\}$ is an $\mathbb{F}_p$-basis of W, each element in K appears exactly twice. By Lemma 4.1, we obtain $S = \mathbb{F}_q$. □

Lemma 4.4. *Assume $p = 2$ and $q \geq 3$. Let $i_0, j_0 \in \mathbb{F}_q$ be such that $j_0 \neq 0$ and $i_0 \neq j_0$. Let $\emptyset \neq S \subset \mathbb{F}_q$ be such that*

$$\sum_{s\in S} \lambda_s \left(u_s + u_{s+i_0} + u_{s+j_0} + u_{s+i_0-j_0}\right) = 0, \tag{4.3}$$

for some $(\lambda_s)_{s\in S} = \mathbf{1}$. Then $S = \mathbb{F}_q$.

Proof. For any $k \in \mathbb{F}_q$, let $w_k = u_k + u_{k+i_0-j_0}$. Then we can rewrite (4.3) as

$$\sum_{s\in S} \lambda_s \left(w_s + w_{s+j_0}\right) = 0. \tag{4.4}$$

Note that

$$w_0 + \cdots + w_{q-1} = 0. \tag{4.5}$$

Moreover, by Lemma 4.3, any $q-1$ vectors from $\{w_0, \dots, w_{q-1}\}$ are $\mathbb{F}_2$-linearly independent.

Assume on the contrary that there exists $s_0 \in S$ such that w_{s_0} or $w_{s_0+j_0}$ appears exactly once in (4.4). Without loss of generality we may suppose that w_{s_0} does. Then we get

$$w_{s_0} = \sum_{s\in S\setminus\{s_0\}} (w_s + w_{s+j_0}) + w_{s_0+j_0}. \tag{4.6}$$

Note that, in the RHS of (4.6), each vector appears at most twice, and that the writing

$$w_{s_0} = \sum_{i\in\mathbb{F}_q\setminus\{s_0\}} w_i$$

is unique in $\oplus_{i\in\mathbb{F}_q\setminus\{s_0\}}\mathbb{F}_2 \cdot w_i$. Hence, we conclude that, in (4.6), each vector appears exactly once (since $\mathbb{F}_p = \mathbb{F}_2$). This implies that $2(|S| - 1) + 1 = q - 1$, and so q is even, a contradiction. Consequently, each vector in (4.4) appears exactly twice. Applying Lemma 4.1 to the multiset $K = \{w_s, w_{s+j_0} \mid s \in S\}$, we obtain that $S = \mathbb{F}_q$. □

Lemma 4.5. *Assume $p = 2$ and $q \geq 3$. Let v be a vector independent with $u_0, \dots, u_{q-1}$ over $\mathbb{F}_2$. Let $i_0 \in \mathbb{F}_q^*$. Then $u_0 + u_{i_0} + v, \dots, u_{q-1} + u_{q-1+i_0} + v$ are linearly independent over $\mathbb{F}_2$.*

Proof. Assume on the contrary there exists $\emptyset \neq S \subset \mathbb{F}_q$ and $(\lambda_s)_{s\in S} = \mathbf{1}$ such that

$$\sum_{s\in S} \lambda_s(u_s + u_{s+i_0} + v) = 0.$$

Then

$$\sum_{s\in S} \lambda_s(u_s + u_{s+i_0}) = 0$$

and $|S|v = 0$. By Lemma 4.3, we have $S = \mathbb{F}_q$. Since q is odd, we get $v = 0$ a contradiction.

Consequently $u_0 + u_{i_0} + v, \dots, u_{q-1} + u_{q-1+i_0} + v$ are linearly independent over $\mathbb{F}_2$. □

4.2. **Proof of Theorem 2.11.** Let k be an algebraically closed field of characteristic 0. Suppose $h \in k[X] \setminus k$ (resp., $g \in k[X] \setminus k$) is linearly related to X^p or T_p (resp., T_q orX^q) for primes $p, q \geq 2$. Denote by $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$ the block kernel. To prove Theorem 2.11, without loss of generality, we may assume that $g \in \{X^q, T_q\}$ and that $h \in \{\ell \circ X^p, \ell \circ T_p\}$ for some $\ell = aX + b \in k[X] \setminus k$ with $a \in k^*$ and $b \in k$.

Fix a compatible system of primitive roots of unity $(\zeta_m)_{m\geq 1} \subset k$. For any group H and $n \geq 1$, denote by $\mathrm{diag}(H^n)$ the diagonal subgroup of H^n.

4.2.1. *Assume $g = X^q$ and $h = \ell \circ X^p$.* Without loss of generality, we may assume $a = 1$.

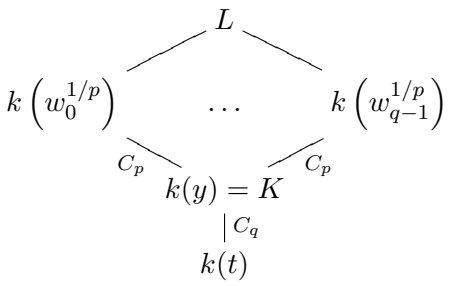
Proposition 4.6. *We have:*

$$\Gamma = \begin{cases} \mathrm{diag}(C_p^q) & \text{if } b = 0, \\ C_p^q & \text{otherwise.} \end{cases}$$

Proof. Let $K = k(y)$ where $y = t^{1/q}$. Then the splitting field of $f(X) - t$ over $k(t)$ is $L = k(t)\left(w_j^{1/p} \mid j \in \mathbb{F}_q\right)$, where $w_j = \zeta_q^j y - b$ $(j \in \mathbb{F}_q)$. Viewing $\mathscr{C} = K^\times/(K^\times)^p$ as an $\mathbb{F}_p$-vector space and letting $\mathcal{O} = \langle w_0, \dots, w_{q-1}\rangle_{\mathbb{F}_p} \leq \mathscr{C}$, by Kummer theory, we have $\dim_{\mathbb{F}_p}(\Gamma) = \dim_{\mathbb{F}_p}(\mathcal{O})$.

Assume first that $b = 0$. Then $w_0 = \cdots = w_{q-1} = y$ in $\mathscr{C}$, which implies $\mathcal{O} = \langle y\rangle_{\mathbb{F}_p}$, and so $\dim_{\mathbb{F}_p}(\Gamma) = \dim_{\mathbb{F}_p}(\mathcal{O}) = 1$. In addition, we have $\Gamma = \mathrm{diag}(C_p^q)$.

Assume next that $b \neq 0$. Since $w_0, \dots, w_{q-1}$ are $\mathbb{F}_p$-linearly independent in $\mathscr{C}$, we have $\dim_{\mathbb{F}_p}(\Gamma) = \dim_{\mathbb{F}_p}(\mathcal{O}) = q$, and so $\Gamma = C_p^q$.



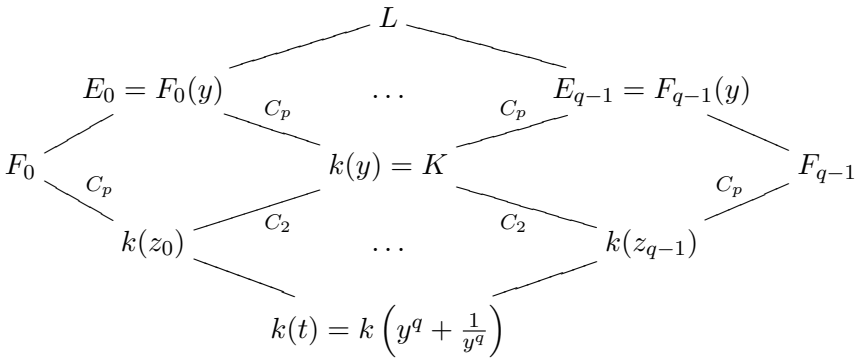
□

4.2.2. *Assume $g = T_q$ and $h = \ell \circ X^p$.* Since the case $g = T_2$ is covered by §4.2.1, we can assume that $q \geq 3$. Furthermore, without loss of generality, we may also suppose $a = 1$.

Proposition 4.7. *We have*

$$\Gamma = \begin{cases} \mathrm{diag}(C_2^q) & \text{if } p = 2 \text{ and } b = \pm 2, \\ C_p^q & \text{otherwise.} \end{cases}$$

Proof. Let $K = k(y)$ where $y \in \overline{k(t)}$ satisfies $t = y^q + \frac{1}{y^q}$. Then the splitting field of $T_q(X) - t$ over $k(t)$ is $k(y)$, and its roots are $z_i = \zeta_q^i y + \frac{1}{\zeta_q^i y}$ $(i \in \mathbb{F}_q)$. Moreover, the splitting field of $X^p - \ell^{-1}(z_i)$ $(i \in \mathbb{F}_q)$ over $k(z_i)$ is $F_i = k\left((z_i - b)^{1/p}\right)$. Hence, letting $E_i = F_i(y)$ $(i \in \mathbb{F}_q)$, the splitting field of $f(X) - t$ over $k(t)$ is $L = E_0 \cdots E_{q-1}$. Below, we view $\mathscr{C} = K^\times/(K^\times)^p$ as an $\mathbb{F}_p$-vector space.



For $i \in \mathbb{F}_q$, letting

$$u_i = y - \zeta_q^{-i}\left(\frac{b + \sqrt{b^2-4}}{2}\right), v_i = y - \zeta_q^{-i}\left(\frac{b - \sqrt{b^2-4}}{2}\right) \text{ and } w_i = u_i v_i y^{p-1},$$

we have $z_i - b = w_i$ in $\mathcal{C}$, and so $E_i = K\left(w_i^{1/p}\right)$. Consider $\mathcal{S}_1 = \{u_i \mid i \in \mathbb{F}_q\}$ and $\mathcal{S}_2 = \{v_i \mid i \in \mathbb{F}_q\}$. We distinguish three cases:

Case 1: Suppose $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$. Then $u_0, \ldots, u_{q-1}, v_0, \ldots, v_{q-1}, y^{p-1}$ are $\mathbb{F}_p$-linearly independent in $\mathscr{C}$, and so are $w_0, \ldots, w_{q-1}$. Hence, we get $\Gamma = C_p^q$.

Case 2: Suppose $p \geq 3$ and $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \emptyset$. Assume first $b = \pm 2$. Then $w_i = u_i^2 y^{p-1}$ for all $i \in \mathbb{F}_q$. Since $u_0^2, \ldots, u_{q-1}^2, y^{p-1}$ are $\mathbb{F}_p$-linearly independent in $\mathscr{C}$, so are $w_0, \ldots, w_{q-1}$, which implies $\Gamma = C_p^q$. Assume now $b \neq \pm 2$. Then, there exists $i_0 \in \mathbb{F}_q^*$, such that $v_i = u_{i+i_0}$, for all $i \in \mathbb{F}_q$. By Lemma 4.2, $u_0 v_0, \ldots, u_{q-1} v_{q-1}, y^{p-1}$ are $\mathbb{F}_p$-linearly independent in $\mathscr{C}$, so are $w_0, \ldots, w_{q-1}$. Consequently we get $\Gamma = C_p^q$.

Case 3: Suppose $p = 2$ and $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \emptyset$. Assume first $b = \pm 2$. Then $w_i = y$ in $\mathcal{C}$ for all $i \in \mathbb{F}_q$, so $\Gamma = \mathrm{diag}(C_2^q)$. [13] Assume now $b \neq \pm 2$. Then, there exists $i_0 \in \mathbb{F}_q^*$, such that $v_i = u_{i+i_0}$, for all $i \in \mathbb{F}_q$. By Lemma 4.5, $u_0v_0y, \dots, u_{q-1}v_{q-1}y$ are $\mathbb{F}_2$-linearly independent in $\mathscr{C}$, so are $w_0, \dots, w_{q-1}$. Consequently we get $\Gamma = C_2^q$. □

4.2.3. *Assume $g = X^q$ and $h = \ell \circ T_p$.* Since the case $h = \ell \circ T_2$ is covered by §4.2.1, we may suppose $p \geq 3$. For $n \geq 2$ and $H \leq \mathrm{AGL}_1(p)$, let

$$\mathcal{L}_{H,n} = \{(a_k)_{k=1}^n \in H^n \mid a_1 \cdots a_n \in C_p\},$$

Without loss of generality, we may assume that $a = 1$.

Proposition 4.8. *We have*

$$\Gamma = \begin{cases} \mathrm{diag}(D_p^q) & \text{if } q = 2 \text{ and } b = 0, \\ \mathcal{L}_{D_p,q} & \text{if } b = \frac{1+\zeta_q^{i_0}}{-1+\zeta_q^{i_0}} \text{ for some } i_0 \in \mathbb{F}_q^*, \\ \Gamma = D_p^q & \text{otherwise.} \end{cases}$$

Denoting by $D_p^n \times_{C_2} D_p$ the fiber product along the canonical epimorphisms $D_p^n \twoheadrightarrow D_p^n/\mathcal{L}_{D_p,n} = C_2$ and $D_p \twoheadrightarrow D_p/C_p = C_2$, we shall use:

Lemma 4.9. $\mathcal{L}_{D_p,n+1} \cong D_p^n \times_{C_2} D_p$.

Proof. This follows from $\mathcal{L}_{D_p,n+1} = ((D_p^n \setminus \mathcal{L}_{D_p,n}) \times (D_p \setminus C_p)) \cup (\mathcal{L}_{D_p,n} \times C_p)$. □

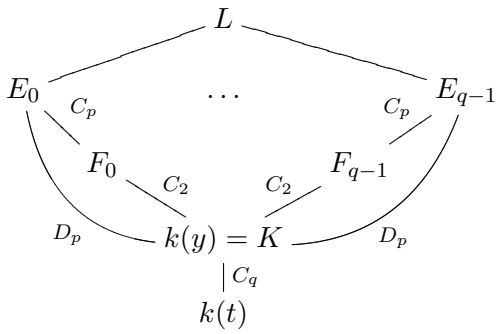
Proof of Proposition 4.8. Let $K = k(y)$ where $y = t^{1/q}$. For $j \in \mathbb{F}_q$, letting $u_j = y + (-b+2)\zeta_q^{-j}$, $v_j = y + (-b-2)\zeta_q^{-j}$ and $w_j = u_jv_j$, the field $F_j = K(\sqrt{w_j})$ is the unique quadratic subextension of the splitting field E_j of $T_p - \ell^{-1}(\zeta_q^j y)$ over K. Moreover the splitting field of $f(X) - t$ over $k(t)$ is $L = E_0 \dots E_{q-1}$. We view $\mathscr{C} = K^\times/(K^\times)^2$ as an $\mathbb{F}_2$-vector space. Consider $\mathcal{S}_1 = \{(-b+2)\zeta_q^{-j} \mid j \in \mathbb{F}_q\}$ and $\mathcal{S}_2 = \{(-b-2)\zeta_q^{-j} \mid j \in \mathbb{F}_q\}$. Unless $q = 2$ and $b = 0$, in which case $\Gamma = \mathrm{diag}(D_p^2)$, the extensions $E_0/K, \dots, E_{q-1}/K$ are pairwise distinct. We may assume now that $(q, b) \neq (2, 0)$ We distinguish two cases:

-Case 1: Suppose that $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$. Then $u_0, \dots, u_{q-1}, v_0, \dots, v_{q-1}$ are $\mathbb{F}_p$-linearly independent in $\mathscr{C}$, and so are $w_0, \dots, w_{q-1}$. This implies that $F_0/K, \dots, F_{q-1}/K$ are linearly disjoint. Hence $E_0/K, \dots, E_{q-1}/K$ are also linearly disjoint. Consequently, we obtain $\Gamma = D_p^q$.

-Case 2: Suppose that $\mathcal{S}_1 \cap \mathcal{S}_2 \neq \emptyset$. Note that $-b-2 \neq -b+2$, so $u_j \neq v_j$ in $\mathscr{C}$, for all $j \in \mathbb{F}_q$. Then, there exists $i_0 \in \mathbb{F}_q^*$ such that $(-b-2)\zeta_q^{-j} = (-b+2)\zeta_q^{-(j+i_0)}$, that is, $b = 2(1+\zeta_q^{i_0})(1-\zeta_q^{i_0})^{-1}$. Hence $v_j = u_{j+i_0}$ for all $j \in \mathbb{F}_q$. Since $u_0, \dots, u_{q-1}$ are $\mathbb{F}_2$-linearly independent in $\mathscr{C}$, by Lemma 4.3, $w_0, \dots, w_{q-2}$ are also $\mathbb{F}_2$-linearly independent. This implies that $F_0/K, \dots, F_{q-2}/K$ are linearly disjoint, and so are $E_0/K, \dots, E_{q-2}/K$. Since

[13] Here, we have $\mathrm{Mon}_k(g \circ h) = D_{2q}$. Indeed, since $X^2 - 2 = T_2(X)$, we have $g \circ h = T_{2q}$ when $b = -2$, and $g \circ h = -T_{2q}(\sqrt{-1}x)$ when $b = 2$.

$E_0/K, \dots, E_{q-1}/K$ are pairwise distinct and $w_0 \cdots w_{q-1} = 1$ in $\mathscr{C}$, combining Lemma 2.7 with Lemma 4.9, we deduce that $\Gamma = \mathcal{L}_{p,q}$.



□

4.2.4. *Assume $g = T_q$ and $h = \ell \circ T_p$.* Since the cases $g = T_2$ or $h = \ell \circ T_2$ are covered by the previous parts, we may suppose $p, q \geq 3$. Recall that $\ell = ax + b$ with $a \in k^*$ and $b \in k$.

Proposition 4.10. *We have*

$$\Gamma = \begin{cases} \mathrm{diag}(C_p^q) & \text{if } (a,b) = (\pm 1, 0), \\ \mathcal{L}_{D_p,q} \text{ or } \Gamma = D_p^q & \text{otherwise.} \end{cases}$$

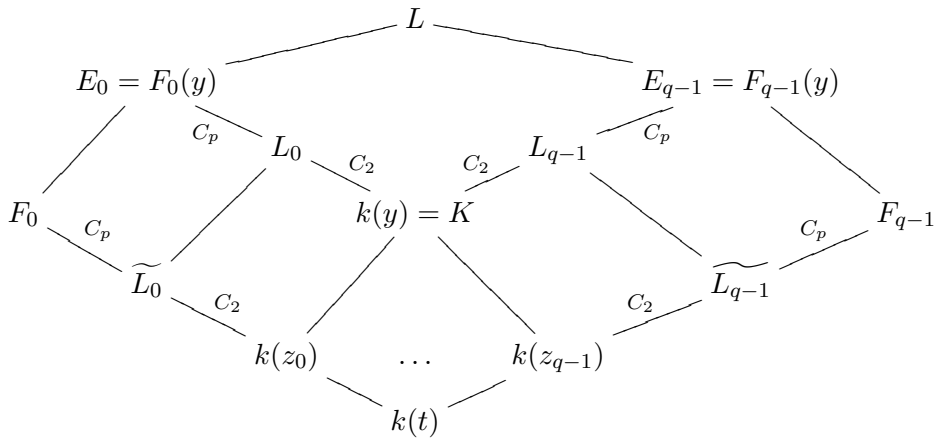
Proof. Assume first that $(a,b) = (\pm 1, 0)$. In this case, f is linearly related to T_{pq}, so $\Gamma = \mathrm{diag}(C_p^q)$.

Assume now that $(a,b) \neq (\pm 1, 0)$. Let $K = k(y)$ where $y \in \overline{k(t)}$ satisfies $t = y^q + \frac{1}{y^q}$. Then the splitting field of $T_q(X) - t = 0$ over $k(t)$ is $k(y)$, and its roots are $z_i = \zeta_q^i y + \frac{1}{\zeta_q^i y}$ ($i \in \mathbb{F}_q$). For all $i \in \mathbb{F}_q$, let F_i be the splitting field of $T_p(X) - \ell^{-1}(z_i)$ over $k(z_i)$. Note that, for all $i \in \mathbb{F}_q$, the extensions $k(y)/k(z_i)$ and $\widetilde{L}_i/k(z_i)$ are linearly disjoint, where

$$\widetilde{L}_i = k(z_i)\left(\sqrt{(z_i - b + 2a)(z_i - b - 2a)}\right)$$

is the unique quadratic subextension of $F_i/k(z_i)$; as a consequence, $E_i = F_i(y)/k(y)$ is dihedral, and so has a unique quadratic subextension $L_i/k(y)$. Moreover, the splitting

field of $f(X)-t$ over $k(t)$ is $L=E_0\cdots E_{q-1}$.



For $i\in\mathbb{F}_q$, let

$$u_i=y-\zeta_q^{-i}\left(\frac{b-2a+\sqrt{(-b+2a)^2-4}}{2}\right),\ v_i=y-\zeta_q^{-i}\left(\frac{b-2a-\sqrt{(-b+2a)^2-4}}{2}\right),$$

$$z_i=y-\zeta_q^{-i}\left(\frac{b+2a+\sqrt{(-b-2a)^2-4}}{2}\right)\text{ and }t_i=y-\zeta_q^{-i}\left(\frac{b+2a-\sqrt{(-b-2a)^2-4}}{2}\right).$$

By letting

$$w_i=\left(\zeta_q^{2i}y^2+(-b+2a)\zeta_q^iy+1\right)\left(\zeta_q^{2i}y^2+(-b-2a)\zeta_q^iy+1\right)(i\in\mathbb{F}_q),$$

we have

$$L_i=k(y)(\sqrt{w_i}). \tag{4.7}$$

With $A=-b-2a$ and $B=-b+2a$, we have

$$w_i=\left(\zeta_q^{2i}y^2+B\zeta_q^iy+1\right)\left(\zeta_q^{2i}y^2+A\zeta_q^iy+1\right),$$

for all $i\in\mathbb{F}_q$. We view $\mathscr{C}=K^\times/(K^\times)^2$ as an $\mathbb{F}_2$-vector space. Clearly, for every $i\in\mathbb{F}_q$, we have $w_i=u_iv_iz_it_i$ in $\mathscr{C}$. Consider

$$\mathcal{S}_1=\{u_i\mid i\in\mathbb{F}_q\},\mathcal{S}_2=\{v_i\mid i\in\mathbb{F}_q\},\mathcal{S}_3=\{z_i\mid i\in\mathbb{F}_q\}\text{ and }\mathcal{S}_4=\{t_i\mid i\in\mathbb{F}_q\}.$$

We distinguish four cases:

Case 1: There exists $k\in\{1,2,3,4\}$ such that $\mathcal{S}_k\notin\{\mathcal{S}_i\mid i\neq k\}$. In this case, since the vectors in $\mathcal{S}_k$ are $\mathbb{F}_2$-linearly independent in $\mathscr{C}$, so are $w_0,\ldots,w_{q-1}$. Hence we obtain $\Gamma=D_p^q$.

Case 2: $\mathcal{S}_1=\mathcal{S}_2$ and $\mathcal{S}_3=\mathcal{S}_4$ but $\mathcal{S}_1\neq\mathcal{S}_3$. Note that $u_0\neq v_0$ or $z_0\neq t_0$, for otherwise $w_0=1$ in $\mathcal{C}$, a contradiction. Without loss of generality, we may assume $z_0\neq t_0$. Then there exists $i_0\in\mathbb{F}_q^*$ such that $t_j=z_{j+i_0}$, for all $j\in\mathbb{F}_q$. On the one hand, $\langle u_iv_i\mid i\in\mathbb{F}_q\rangle_{\mathbb{F}_p}\cap\langle z_it_i\mid i\in\mathbb{F}_q\rangle_{\mathbb{F}_p}=1$. On the other hand, by Lemma 4.3, $z_0t_0,\ldots,z_{q-2}t_{q-2}$ are

$\mathbb{F}_2$-linearly independent in $\mathscr{C}$. Therefore $w_0, \dots, w_{q-2}$ are also $\mathbb{F}_2$-linearly independent in $\mathscr{C}$. Since $w_0 \cdots w_{q-1} = 1$ in $\mathscr{C}$, we have $\Gamma = \mathcal{L}_{D_p,q}$.

Case 3: $\mathcal{S}_1 = \mathcal{S}_3$ and $\mathcal{S}_2 = \mathcal{S}_4$ but $\mathcal{S}_1 \neq \mathcal{S}_2$. Note that $u_0 \neq z_0$ or $v_0 \neq t_0$. Without loss of generality, we may assume $u_0 \neq z_0$. Then there exists $i_0 \in \mathbb{F}_q^*$ such that $z_j = u_{j+i_0}$, for all $j \in \mathbb{F}_q$. In this case, $\langle u_i z_i \mid i \in \mathbb{F}_q \rangle_{\mathbb{F}_p} \cap \langle v_i t_i \mid i \in \mathbb{F}_q \rangle_{\mathbb{F}_p} = 1$. By Lemma 4.3, $u_0 z_0, \dots, u_{q-2} z_{q-2}$ are $\mathbb{F}_2$-linearly independent in $\mathscr{C}$, so are $w_0, \dots, w_{q-2}$. Since $w_0 \cdots w_{q-1} = 1$ in $\mathscr{C}$, we have $\Gamma = \mathcal{L}_{D_p,q}$.

Case 4: $\mathcal{S}_1 = \mathcal{S}_4$ and $\mathcal{S}_2 = \mathcal{S}_3$ but $\mathcal{S}_1 \neq \mathcal{S}_2$. By the same reasoning as in Case 3, we also have $\Gamma = \mathcal{L}_{D_p,q}$.

Case 5: $\mathcal{S}_1 = \mathcal{S}_2 = \mathcal{S}_3 = \mathcal{S}_4$. In this case, there exist $i_0, j_0 \in \mathbb{F}_q$ such that $v_k = u_{k+i_0}$, $z_k = u_{k+j_0}$ and $t_k = u_{k+i_0-j_0}$[14] for all $k \in \mathbb{F}_q$. But we have $i_0 \neq j_0$ and $j_0 \neq 0$, for otherwise $w_0 = u_0^2 u_{i_0}^2 = 1$ in $\mathscr{C}$, a contradiction. By Lemma 4.4, $w_0, \dots, w_{q-2}$ are $\mathbb{F}_2$-linearly independent. Since $w_0 \cdots w_{q-1} = 1$ in $\mathscr{C}$, we obtain $\Gamma = \mathcal{L}_{D_p,q}$. □

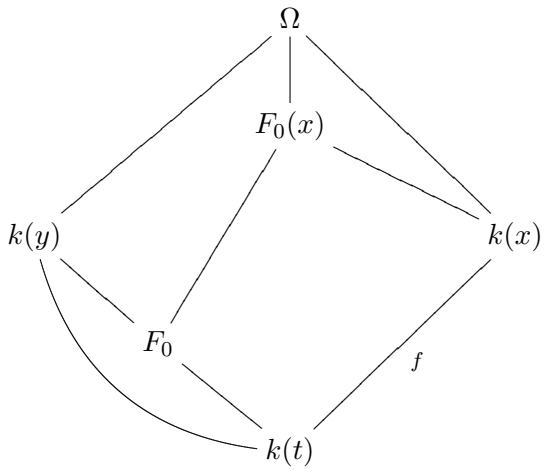
5. Proofs of main results

5.1. **Proof of Theorem 1.1.** Let f and g be as in Theorem 1.1. By Theorem 3.1, we may assume that $\mathrm{Mon}_k(f)$ is nonsolvable. Write $f = f_1 \circ \cdots \circ f_r$ ($r \geq 1$) and $g = g_1 \circ \cdots \circ g_s$ ($s \geq 1$) for indecomposable polynomials $f_i, g_j \in k[X]$, $i = 1, \dots, r$, $j = 1, \dots, s$. Let $k(x_i)$, $i = 0, \dots, r$ be the corresponding tower of fields such that $x_r = x$, $x_0 = t$ and $f_i(x_i) = x_{i-1}$ for all $1 \leq i \leq r$. Similarly, define $k(y_j)$, $i = 0, \dots, s$, so that $y_s = y$, $y_0 = t$ and $g_i(y_i) = y_{i-1}$ for all $1 \leq i \leq s$. For $i = 1, \dots, r$, let $R_i = f_1 \circ \cdots \circ f_i$.

By Fried's argument, we can also assume that (f, g) is minimally reducible. Let $h \in k[X]$ be a minimal nonsolvable left factor of g. Without loss of generality, we can suppose that $h = g_1 \circ \cdots \circ g_u$ for some $1 \leq u \leq s$. Note that $g_1, \dots, g_{u-1}$ are solvable polynomial maps while g_u is nonsolvable. By minimal irreducibility, $k(x)$ and $F_0 := k(y_{u-1})$ are linearly

[14]The expression for $t_k = u_{k+i_0-j_0}$ follows from $v_k = u_{k+i_0}, z_k = u_{k+j_0}$, and the fact that the constant terms of both $u_k v_k$ and $z_k t_k$, as a polynomial in y, are equal to ζ_q^{-2k}.

disjoint over $k(t)$.



Hence, since Ω is the Galois closure of $k(x)/k(t)$, by [KN24, Lemma 2.12], it is also the Galois closure of $F_0(x)/F_0$. In particular, $\Gamma_u = \mathrm{Mon}_k(g_u)$ is quotient of $U_r := \mathrm{Gal}(\Omega/F_0)$. As g_u is nonsolvable, Γ_u is a nonabelian almost simple group.

For $i = 1, \dots, r$, let $\Omega_i/k(t)$ be the Galois closure of $k(x_i)/k(t)$ and let $U_i = \mathrm{Gal}(\Omega_i F_0/F_0)$. Let $m \geq 1$ be minimal such that Γ_u is a quotient of U_i. Since Γ_u has a unique minimal normal subgroup and it is nonabelian, $\mathrm{Mon}_k(f_m)$ has to be nonsolvable. Indeed, otherwise $\Omega_m F_0/\Omega_{m-1}F_0$ is a solvable extension and the kernel K'_m of the natural projection $U_m \to U_{m-1}$ has to be in the kernel of the projection $\pi : U_m \to \Gamma_u$, contradicting the minimality of m.

This moreover shows that in every decomposition $R_m = h_1 \circ \cdots \circ h_m$ for indecomposables h_i, the group $\mathrm{Mon}_k(h_m)$ is nonsolvable. By the Ritt theorems [ZM08], this implies f_m is *right unique*, that is, for every decomposition $f = u \circ v$ with $\deg(v) \geq 2$, one has $v = v' \circ f_m$ for some $v' \in k[X]$. Thus, letting K_m be the kernel of the projection $G := \mathrm{Mon}_k(R_m) \to \mathrm{Mon}_k(f_1 \circ \cdots \circ f_{m-1})$, by [KNR24, Proposition 3.3.], the socle $\mathrm{soc}(K_m)$ is a unique minimal normal subgroup of G. In particular, its centralizer in G is trivial.

Since the Galois closure of $F_0/k(t)$ is solvable, $U_r = \mathrm{Gal}(\Omega/F_0)$ contains $\mathrm{soc}(K_m)$ (which is a power of a nonabelian simple group). As in addition $K'_m = K_m \cap U_m$, we deduce $\mathrm{soc}(K_m) = \mathrm{soc}(K'_m)$. Since the centralizer of $\mathrm{soc}(K_m)$ in G is trivial, it follows that so is the centralizer of $\mathrm{soc}(K'_m)$ in U_m. Since $\mathrm{soc}(K'_m)$ is minimal normal in U_m by [KN24, Cor. 3.4][15], and its centralizer is trivial, its a unique minimal normal subgroup of U_m. It follows that $\mathrm{soc}(K'_m)$ is mapped isomorphically to a minimal normal subgroup of Γ_u and hence is simple. Thus $\mathrm{soc}(K_m) = \mathrm{soc}(K'_m)$ is simple and hence diagonal[16] in $\mathrm{Mon}_k(f_m)^d$, $d = \deg(f_1 \circ \cdots \circ f_{m-1})$. Hence, since $\mathrm{soc}(\mathrm{Mon}_k(f_m))^d \subset \mathrm{soc}(K_m)$ by [KNR24, Corollory 4.4.], we have $d = 1$, and so $m = 1$.

[15]When applying [KN24, Corollary 3.4], one has to choose U as the image of the action of a block stabilizer in the action of U_m.

[16]that is, the projection into each factor of $\mathrm{Mon}_k(f_m)^d$ is injective.

It follows that U_1 is almost simple (so that $U_1 = \mathrm{Mon}_k(g_u)$) and $k(y_u)$ is the fixed field of some $V \le U_1 \le G = \mathrm{Mon}_k(f_1)$. In particular, we see that Ω_1^V is a common subfield of Ω_1 and $k(y_u)$ and hence is of the form $k(z)$ with $h(z) = t, h'(y_u) = z$ and $g_1 \circ \cdots \circ g_u = h \circ h'$ for some polynomials $h, h' \in k[X]$. As the core of V in U_1 is trivial so is its core in G, so that Ω_1 is the common Galois closure of f_1 and h.

By applying [M95], it follows that the stabilizers G_1 and V of f_1 and h, resp., are either conjugate or permutation equivalent, that is, $G/G_1 \cong G/V$ as G-sets. In the former case V is clearly intransitive. In the latter case, every element of V has a fixed point in its action on G/G_1. Thus, in this case as well V is intransitive on G/G_1 by Burnside's lemma. It follows that in both cases $f_1(X) - h(Y) \in k[X, Y]$ is reducible. By [KN24], either $f_1 = h \circ \mu$ for a linear $\mu \in k[X]$ in which case both f and g factor through f_1, or (f_1, h) is among the exceptional pairs classified by Fried.

5.2. **Proof of Theorem 1.2.** We assume f does not factor through an indecomposable polynomial of degree ≤ 6. 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 such that the fiber product of g and f is reducible. Here we classify all g satisfying these properties and $G = \mathrm{Mon}_{\mathbb{Q}}(g) = \mathrm{Mon}_{\mathbb{Q}}(f)$ is nonsolvable, showing they have to be left factors of f. Throughout, assume on the contrary $f \in \mathbb{Q}(x)$ and $g \in \mathbb{Q}(x)$ is a minimal pair, consisting of a polyonmial and a Siegel function, such that $\mathrm{Red}_f(\mathbb{Z})$ contains $g(\mathbb{Q}) \cap \mathbb{Z}$ but f and g do not have a common left factor. The minimality here amounts to the following assertion: For every decomposition $f = h \circ h_2 \in \mathbb{Q}[x]$ with $\deg(h_2) > 1$, the set $\mathrm{Red}_h(\mathbb{Z}) \setminus \bigcup_{h=u\circ v} u(\mathbb{Q})$ is finite. This implies that (f, g) is a minimally reducible pair (but now with g a Siegel function), and hence f and g have a common Galois closure by Lemma 2.6.

Assume $g_1 \circ \cdots \circ g_t \in \mathbb{Q}(y)$ for $t \le s$ is a minimal nonsolvable subcover[17] of g. Thus $g_1, \dots, g_{t-1}$ are linearly related over $\overline{\mathbb{Q}}$ to Siegel functions with solvable monodromy while g_t has nonsolvable monodromy. In particular by our minimality assumption, $\mathbb{Q}(x)$ and $F_0 := \mathbb{Q}(y_{t-1})$ are linearly disjoint over $\mathbb{Q}(t)$. Since these are linearly disjoint and Ω is the Galois closure of $\mathbb{Q}(x)/\mathbb{Q}(t)$, it is also the Galois closure of $F_0(x)/F_0$ by [KN24, Lemma 2.12]. In particular, the monodromy group Γ_t of g_t is quotient of $U_r := \mathrm{Gal}(\Omega/F_0)$ (the Galois closure of $F_0(x)/F_0$). Recall that by [M95, Lemma 4.7(c)] the maps g_i are also indecomposable over $\mathbb{C}$.

Suppose[18] r is minimal for which $\Gamma := \Gamma_t$ is a quotient of U_r. Since Γ has a unique minimal normal subgroup and it is nonabelian, $\mathrm{Mon}_{\mathbb{Q}}(f_r)$ has to be nonabelian. Indeed, otherwise $F_0(x_r)/F_0(x_{r-1})$ is a solvable extension and the kernel K_r' of the natural projection $U_r \to U_{r-1}$ has to be in the kernel of the projection $\pi : U_r \to \Gamma$, contradicting the minimality of r. This moreover shows that in every decomposition $f = h_1 \circ \cdots \circ h_r$, $\mathrm{Mon}_{\mathbb{Q}}(h_r)$ is nonsolvable. By the Ritt theorems [ZM08] this implies f_r is *right unique*, that is, for every decomposition $f = u \circ v$ with $\deg(v) > 1$, one has $v = v' \circ f_r$ for some

[17] One might need to replace the decomposition $g = g_1 \circ \cdots \circ g_s$ to get such a subcover. In this step, one loses the reducibility of the curve $f(x) = g(y)$.

[18] To do so, one might need to replace f by a subcover of it. Then U_r can still be identified with a subgroup of G via restriction.

$v' \in \mathbb{Q}[x]$. Thus, letting K_r be the kernel of the projection $G \to \mathrm{Mon}_{\mathbb{Q}}(f_1 \circ \cdots \circ f_{r-1})$, its socle $\mathrm{soc}(K_r)$ is a unique minimal normal subgroup of G by [KNR24, Proposition 3.3.]. In particular, its centralizer in G is trivial.

Since $\mathrm{soc}(K_r)$ is a power of a nonabelian simple group (since it is a nonabelian minimal normal subgroup), its projection to the solvable group $G/\mathrm{core}_G(U_r)$ is trivial, so that $\mathrm{soc}(K_r) \subseteq U_r$. Since its centralizer in G is trivial, so is its centralizer in U_r, so that it is the unique minimal normal subgroup of U_r. It follows that $\mathrm{soc}(K_r)$ is mapped isomorphically into Γ.

By the monodromy classification of indecomposable Siegel functions [MI3, Thm. 4.8], either (A) Γ is almost simple, or (B) it is of product type $A_k^2 \leq \Gamma \leq S_m \wr S_2$, $m \geq 5$, or (C) it is in an explicit list of small degree affine groups. We claim that only case (A) occurs. Since Γ is nonsolvable and G contains only composition factors of polynomials of degree > 6, in case (C) its nonabelian composition factor is one of $A_7, \mathrm{SL}_k(2)$, $k = 4, 5$ by [MI3]. Moreover by [MI3, Theorem 5.2], $SL_3(2)$ is the only composition factor of a Siegel function over $\mathbb{Q}$ among the list for (C). However, by the monodromy classification of indecomposable polynomials over $\mathbb{Q}$, $SL_3(2)$ does not appear as a composition factor of $\mathrm{Mon}_{\mathbb{Q}}(f_i)$ and hence is not a composition factor of G, so that (C) does not occur. In case (B), since $\mathrm{soc}(K_r)$ is mapped isomorphically to Γ, $\mathrm{soc}(K_r) \cong A_k^2$. On the other hand by [KN24, Proposition 2.1], $\mathrm{soc}(K_r) \cong A_k^P \leq A_k^{[d'_{r-1}]}$, where $m := \deg(f_1 \circ \cdots \circ f_{r-1})$, $[m]$ is the corresponding set of blocks, and P is a partition of $[m]$. Since $\mathrm{soc}(K_r) \cong A_k^2$, P consists of two blocks. The stabilizer G_P of the action of G on P contains the stabilizer of $\mathbb{Q}(x)$ but on the other hand is of index 2 in G. This yields a subfield $\Omega^{G_P} \subseteq \mathbb{Q}(x)$ of degree 2 over $\mathbb{Q}(t)$, yielding a contradiction to the assumptions that f does not factor through a degree 2 polynomial.

Henceforth, we may assume case (A). Since the minimal normal subgroup $\mathrm{soc}(K_r)$ is mapped isomorphically into the almost simple group Γ, it is simple. Thus $\mathrm{soc}(K_r)$ is diagonal in $\mathrm{Mon}_{\mathbb{Q}}(f_r)^m$. If $m > 1$, this contradicts [KNR24, Theorem 3.1] or [Ros22, Main Thm.]. Thus $m = 1$ and hence $r = 1$. It follows that U_r is almost simple and $\mathbb{Q}(y_t)$ is the fixed field of some subgroup $V \leq U_r$. In particular, letting Ω_1 be the Galois closure of $\mathbb{Q}(x_1)/\mathbb{Q}(t)$, we see that Ω_1^V is a common subfield of Ω_1 and $\mathbb{Q}(y_t)$ and hence is of the form $\mathbb{Q}(z)$ with $h(z) = t$ and $g_1 \circ \cdots \circ g_t = h \circ h'$ for some $h, h' \in \mathbb{Q}(x)$ where h is a Siegel function over $\mathbb{Q}$. As the core of V in U_r is trivial so is its core in G, so that Ω_1 is the common Galois closure of f_1 and h.

As in the proof of [KN24, Theorem 1.1], crossing the lists in [M95, MI3] over $\mathbb{Q}$ yields that either h factors through f_1 or $\mathrm{Mon}_{\mathbb{Q}}(f_1) \cong S_5$ in the natural action. The latter case contradicts our assumption that $\deg(f_1) > 6$. In the former case, the minimal reducibility assumption implies f and h coincide with f_1 up to composition with linear fractionals, as desired.

Finally, in the solvable case, we deduce Theorem 1.2 from:

Proposition 5.1. *Suppose $f = f_1 \circ \cdots \circ f_r$ for indecomposable $f_i \in \mathbb{Q}[X]$, $i = 1, \dots, r$ of degree ≥ 7 with solvable $\mathrm{Mon}_{\mathbb{Q}}(f_i)$. Then*

$$\mathrm{Red}_f(\mathbb{Z}) = \cup_h (h(\mathbb{Q}) \cap \mathbb{Z}) \cup \textit{finite set},$$

where $h \in \mathbb{Q}[X]$ runs through all left nontrivial factors of f.

Proof. By [KN24, Corollary 2.5],

$$\mathrm{Red}_f(\mathbb{Z}) = \left(\bigcup_h (h(\mathbb{Q}) \cap \mathbb{Z}) \right) \cup \text{finite set},$$

where $h \in \mathbb{Q}(Y)$ runs through all Siegel functions such that $f(X) = h(Y)$ is reducible. By Theorem 3.1, one can restrict those h to nontrivial left polynomial factors of f. □

5.3. **Application to 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 an irreducible factor of $f(x) - g(y)$ and $k(x, y)$ its corresponding genus-0 function field. Set $t = f(x) = g(y)$. Let $k(s) = k(x) \cap k(y)$. Furthermore, by possibly replacing s, we may assume $t = w_1(s)$ for $w_1 \in k[x]$, and $s = f_1(x) = g_1(y)$ for $f_1, g_1 \in k[x]$. By our assumption of minimality for f, g, we get $k(s) = k(t)$, so that $\deg(w_1) = 1$. Since $f_1(X) - g_1(Y) \in k[X, Y]$ is reducible by assumption, §5.1 (which gives Theorem 1.1 over arbitrary fields k of characteristic 0) implies that either (a) f_1 and g_1 have a common left factor $h \in k[x]$ of $\deg(h) > 1$, or (b) that $f_1 = w_2 \circ h_1 \circ u$ and $g_1 = w_2 \circ h_2 \circ v$, where $\deg(w_2) = 1$, and $\{h_1, h_2\}$ is one of the pairs of polynomials of degree $7, 11, 13, 15, 21$, or 31 in [CNC99].

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 $k(x_2) \cap k(y_2) = k(s)$ for $x_2 = f_2(x)$ 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 of genus 0. It now follows from [AZ03, Thm. 1] that there exist $w_2, h_2 \in k[x]$ such that $f = w_2 \circ h_2$, where already $h_2(x_2) = h_2(y_2)$. Moreover, either $h_2 = x^n \circ u_1$, or $T_n \circ u_1$ (with $\deg(u_1) = 1$) for some $n \geq 2$, or $h = w_2 \circ P_i \circ u_1$, $i = 1, 2, 3$ (with $\deg(u_1) = 1$). Since we assumed $k(x_2) \cap k(y_2) = k(s)$, it follows that $k(h_2(x_2)) = k(h_2(y_2))$ is of degree 1 over $k(s)$, and hence $\deg(w_2) = 1$. By setting $\mu = w_1 \circ w_2$, $u = u_1 \circ f_2$, and $v = u_1 \circ g_2$, it follows that (f, g) is in cases (2)-(4).

In the second case (b), setting $x_2 = u(x)$ and $y_2 = v(x)$, the function field $k(x_2, y_2)$ is of genus 0 as a subfield of $k(x, y)$. A direct computer check, using Magma and the list of ramification types in [M95], shows that the only pairs $\{h_1, h_2\}$ in [CNC99] with a genus 0 factor are certain pairs of degree 7 or 13. By setting $\mu = w_1 \circ w_2$, we get that (f, g) is in case (5). □

Remark 5.2. The computer check further reveals that in case (5), the degree-7 (degree-13) polynomials h_1, h_2 have three branch points with branch cycles of orders $2, 3, 7$ or $2, 4, 7$ (resp. $2, 3, 13$).

References

[AZ01] Roberto M. Avanzi and Umberto M. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation*, Acta Arith. **99** (2001), no. 3, 227–256. MR 1845348

[AZ03] ———, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$*, Compositio Math. **139** (2003), no. 3, 263–295. MR 2041613

[BIJ+19] Robert Benedetto, Patrick Ingram, Rafe Jones, Michelle Manes, Joseph H. Silverman, and Thomas J. Tucker, *Current trends and open problems in arithmetic dynamics*, Bull. Amer. Math. Soc. (N.S.) **56** (2019), no. 4, 611–685. MR 4007163

[Bil99] Yuri F. Bilu, *Quadratic factors of $f(x)-g(y)$*, Acta Arith. **90** (1999), no. 4, 341–355. MR 1723674

[BT00] Yuri F. Bilu and Robert F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), no. 3, 261–288. MR 1793164

[BT12] Boris Bukh and Jacob Tsimerman, *Sum-product estimates for rational functions*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 1, 1–26. MR 2876962

[Cas70] J. W. S. Cassels, *Factorization of polynomials in several variables*, Proc. 15th Scand. Congr. Oslo 1968, Lect. Notes Math. 118, 1-17 (1970)., 1970.

[CDH+12] Alex Carney, Thao Do, Jared Hallett, Qingyun Sun, Ben Weiss, Elliott Wells, Susan Xia, and Michael 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] Pierrette Cassou-Noguès and Jean-Marc Couveignes, *Factorisations explicites de $g(y) - h(z)$*, Acta Arith. **87** (1999), no. 4, 291–317. MR 1671641

[DF99] Pierre Dèbes and Michael D. Fried, *Integral specialization of families of rational functions*, Pacific J. Math. **190** (1999), no. 1, 45–85. MR 1722766

[DHH+12] Thao Do, Jared Hallett, Xiangyi Huang, Yuwei Jiang, Ben Weiss, Elliot Wells, and Michael 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. MR 137703

[DR25] Maarten Derickx and James 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. MR 162789

[FG12] Michael D. Fried and Ivica Gusić, *Schinzel's problem: imprimitive covers and the monodromy method*, Acta Arith. **155** (2012), no. 1, 27–40. MR 2982425

[FM69] Michael D. Fried and R. E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171. MR 238815

[Fri74] Michael Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231. MR 349624

[Fri86] Michael Fried, *Rigidity and applications of the classification of simple groups to monodromy Part ii-applications of connectivity: Davenport and Hilbert–Siegel problems*, Preprint, 1986.

[Fri12] Michael D. Fried, *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. MR 2873803

[Fri23] ———, *Taming genus 0 (or 1) components on variables-separated equations*, Albanian J. Math. **17** (2023), no. 2, 19–80. MR 4613608

[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. MR 4611831

[KMS07] Manisha Kulkarni, Peter Müller, and B. Sury, *Quadratic factors of $f(X) - g(Y)$*, Indag. Math. (N.S.) **18** (2007), no. 2, 233–243. MR 2352678

[KN24] Joachim König and Danny Neftin, *Reducible fibers of polynomial maps*, Int. Math. Res. Not. IMRN (2024), no. 6, 5373–5402. MR 4721056

[KNR24] Joachim König, Danny Neftin, and Shai Rosenberg, *Polynomial compositions with large monodromy groups and applications to arithmetic dynamics*, 2024.

[M95] Peter 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. MR 1352284

[M99] ———, *Hilbert's irreducibility theorem for prime degree and general polynomials*, Israel J. Math. **109** (1999), 319–337. MR 1679603

[M02] ———, *Finiteness results for Hilbert's irreducibility theorem*, Ann. Inst. Fourier (Grenoble) **52** (2002), no. 4, 983–1015. MR 1926669

[MI3] ———, *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. MR 3114008

[Pak10] F. Pakovich, *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. MR 2766178

[Pak18] Fedor Pakovich, *On algebraic curves $A(x) - B(y) = 0$ of genus zero*, Math. Z. **288** (2018), no. 1-2, 299–310. MR 3774414

[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. MR 4634687

[Ros22] Shai Rosenberg, *Ph.d. thesis, technion - iit*, 2022.

[Sch00] A. Schinzel, *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. MR 1770638

[Sch07] Andrzej Schinzel, *Andrzej Schinzel selecta. Vol. I*, Heritage of European Mathematics, European Mathematical Society (EMS), Zürich, 2007, Diophantine problems and polynomials. MR 2383194

[Tao12] Terry Tao, *When is $P(x) - Q(y)$ irreducible?*, `https://mathoverflow.net/q/105747`, 2012, MathOverflow post.

[Tao15] Terence Tao, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, Contrib. Discrete Math. **10** (2015), no. 1, 22–98. MR 3386249

[Zie12] Michael E. Zieve, *Criteria for irreducibility of polynomial*, `https://mathoverflow.net/questions/105304/criteria-for-irreducibility-of-polynomial/`, 2012, MathOverflow post.

[ZM08] Michael E. Zieve and Peter Müller, *On Ritt's polynomial decomposition theorems*, 2008.

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