MONODROMY GROUPS OF POLYNOMIALS OF COMPOSITION LENGTH 2

ANGELOT BEHAJAINA, JOACHIM KÖNIG, AND DANNY NEFTIN

ABSTRACT. We study the monodromy groups of compositions of two indecomposable polynomials. In particular, we show that such monodromy groups either fulfill a certain "largeness" property, or are in an explicit list of exceptions. Such largeness results are crucial for dealing with compositions of more than two polynomials, and consequently are expected to have a wide range of applications to problems concerning the arithmetic of polynomials. Concretely, our main result is a key ingredient in the solution of a long-standing open problem due to Davenport, Lewis and Schinzel, achieved in the companion paper [BKN26].

1. INTRODUCTION

Let k be a field of characteristic 0. The *(arithmetic) monodromy group* of $f \in k[X]\backslash k$ over k, denoted by $\mathrm{Mon}_k(f)$ (or simply $\mathrm{Mon}(f)$ when there is no risk of confusion), is the Galois group of $f(X)-t$ over $k(t)$, viewed as a permutation group acting on the generic fiber $f^{-1}(t) \subset \overline{k(t)}$. The *geometric monodromy group* of f is the normal subgroup $\mathrm{Mon}_{\overline{k}}(f) \trianglelefteqslant \mathrm{Mon}_k(f)$.

The classification of monodromy groups of indecomposable polynomials over $\mathbb{C}$ and $\mathbb{Q}$, along with their possible ramification types, was carried out by Müller in [Mül95]. The next step is to address the following:

Problem 1.1. Classify the monodromy groups of polynomials of length 2 over $\mathbb{C}$ and over $\mathbb{Q}$.

Recall that the *(composition) length* of $f \in k[X]\backslash k$ is the number of factors in a decomposition of f as a composition of indecomposable polynomials.[1]

We say that $f, g \in k[X]$ are *linearly equivalent* (over $\overline{k}$) and write $f \sim g$, if there exist linear polynomials $\mu, \nu \in \overline{k}[X]$ such that $g = \mu \circ f \circ \nu$. Of course, linearly equivalent polynomials have the same geometric monodromy group. Note that an upper bound for the monodromy group of a composition $f = g \circ h$ is given by (the imprimitive wreath product) $\mathrm{Mon}(h) \wr \mathrm{Mon}(g) = \mathrm{Mon}(h)^{\deg(g)} \rtimes \mathrm{Mon}(g)$. In case of equality, one in particular has that $\ker(\mathrm{Mon}(g \circ h) \to \mathrm{Mon}(g)) = \mathrm{Mon}(h)^{\deg(g)}$ is maximal possible. It turns out that, for many applications (see, e.g., [KNR24] for applications in arithmetic dynamics), a slight weakening of this property is sufficient: namely, for $g, h \in k[X]$ of degree > 1 with h indecomposable, we say that $g \circ h$ has a *large kernel*, if either

$$\mathrm{soc}(\mathrm{Mon}_k(h))^{\deg(g)} \leqslant \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g)),$$ [2]

or

$$\mathrm{soc}(\mathrm{Mon}_k(h)) \text{ is cyclic and } \mathrm{soc}(\mathrm{Mon}_k(h))^{\deg(g)-1} \leqslant \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g)).$$

[1] By Ritt's theory (see [ZM08]), this number is independent of the chosen decomposition.

[2] For a group G, the *socle* $\mathrm{soc}(G)$ denotes the subgroup generated by all minimal normal subgroups of G. Note that for an indecomposable h, the socle $\mathrm{soc}(\mathrm{Mon}_k(h))$ is always either a simple group or equal to $V_4 \lhd S_4$.

Recall finally that the *Chebyshev polynomial* $T_n \in \mathbb{Z}[X]$ of degree $n \geqslant 1$ is uniquely determined by the identity $T_n(X+1/X) = X^n + 1/X^n$. Chebyshev polynomials and monomials X^n are at the other end of "large kernel", fulfilling $\mathrm{Mon}_{\overline{k}}(T_n) = D_n$ $(n \geqslant 3)$ and $\mathrm{Mon}_{\overline{k}}(X^n) = C_n$, and thus $\ker(\mathrm{Mon}_{\overline{k}}(T_n \circ T_m) \to \mathrm{Mon}_{\overline{k}}(T_n)) = \ker(\mathrm{Mon}_{\overline{k}}(X^n \circ X^m) \to \mathrm{Mon}_{\overline{k}}(X^n)) = C_m$. A more diverse source for violation of the large kernel property (cf. Proposition 3.13) are pairs f, g admitting *Ritt move*; see Section 2 for a definition.

Our main result states in a precise way that, for length-2 polynomials, the above examples are "almost" the only ones violating the large kernel property. Namely,

Theorem 1.2. *Let $g, h \in k[X]$ be indecomposable polynomials of degree > 1. Then $g \circ h$ has a large kernel unless one of the following cases holds:*

1. *Over $\overline{k}$, one has $g \circ h \sim T_{p^2}$ or $g \circ h \sim X^{p^2}$ for some prime p;*
2. *$g \circ h$ has a Ritt move;*
3. *$\mathrm{Mon}(g \circ h)$ is one of the groups in Table 1. In particular, one of the following holds:*
   - *a. $h \sim X^2$ and $\mathrm{Mon}_{\overline{k}}(g) \in \{S_4, PGL_2(5), PSL_3(2), PGL_2(7), P\Gamma L_2(9), M_{11}, PSL_3(3), PSL_4(2), P\Gamma L_3(4), M_{23}, \mathrm{PSL}_5(2)\}$;*
   - *b. $h \sim X^3$ and $\mathrm{Mon}_{\overline{k}}(g) \in \{A_5, PGL_2(7), PSL_2(11), PSL_3(3)\}$;*
   - *c. $h \sim T_3$ and $\mathrm{Mon}_{\overline{k}}(g) = PSL_3(3)$.*

In particular, if $\mathrm{Mon}(g), \mathrm{Mon}(h)$ are both solvable, then $g \circ h$ either has large kernel or is linearly equivalent to a monomial or a Chebyshev polynomial, or one of only two other cases holds:

- *$\mathrm{Mon}_{\overline{k}}(g \circ h) = C_3 \times S_4 \leqslant S_{12}$, with a Ritt move;*
- *$\mathrm{Mon}_{\overline{k}}(g \circ h) = GL_2(3) \leqslant S_8$, without a Ritt move.*

The techniques used to prove this theorem are diverse and include permutation group theory, representation theory and linear algebra, as well as some topological ideas related to braid group action and configuration spaces of Galois covers. Some parts are also based on computer calculations in Magma [BCP97], mainly using the database of transitive groups. Code for the nontrivial Magma verifications is contained in an ancillary file.

Applications of Theorem 1.2 go far beyond the consideration of only compositions of *two* indecomposables. We demonstrate this with sample results on composition of arbitrarily many indecomposables in Section 6. In [BKN26], the authors apply (the restriction to solvable groups of) the theorem to solve a long-standing open problem due to Davenport, Lewis and Schinzel [DLS61] on the reducibility behavior of $f(X) - g(Y)$, with *arbitrary* polynomials f, g. Further applications are expected in the field of arithmetic dynamics, notably the study of dynamical Galois groups, i.e., the groups $G_{f,\alpha} := \varprojlim_n \mathrm{Gal}(f^n(X) - \alpha/k)$, where f^n denotes the n-th iterate of the polynomial $f \in k[X]$ (and $\alpha \in k$). To illustrate this, we give a sample application in Section 6.2. More comprehensive applications will be developed in follow-up work.

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

2. Beyond Theorem 1.2

In this section, we provide detailed refinements of Theorem 1.2. The theorem will be a direct consequence of the combination of Theorems 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 and 2.7 below, each of which deals with particular classes of monodromy groups $\mathrm{Mon}(g), \mathrm{Mon}(h)$. Note that, due to the definition of the "large kernel" property, we may work at the level of geometric monodromy groups in order to prove Theorem 1.2. We therefore may and will assume for the rest of this section that $k = \overline{k}$ is an algebraically closed field of characteristic 0.

2.1. **Solvable case.** This part is devoted to the refinements of the solvable case of Theorem 1.2. Note that Theorems 2.1, 2.2, 2.3 and 2.4 are essentially statements about configurations of branch points in a composition of two polynomials, as will become evident in the proofs. We additionally give explicit polynomials corresponding to each special case, whenever these are easy to compute from the respective branch point configurations; in some cases, however, such a parameterization would be too inconvenient to produce.

For a group H and integer $n \geqslant 1$, let $\mathrm{diag}(H^n) = \{(h, \dots, h) \mid h \in H\}$. We shall call a polynomial f an AGL_1-polynomial if its monodromy group is a transitive subgroup of $\mathrm{AGL}_1(p)$ for a prime p. The *ramification type* of f is a multiset of tuples $E_f(P)$, where P runs over branch points of f, and $E_f(P)$ consists of the ramification indices $e_f(Q/P)$ where Q runs over preimages in $f^{-1}(P)$. Following [ZM08], say that $\alpha \in k$ is a *special point* of a f if it is unramified but lies over a branch point.

Theorem 2.1 (Composition of AGL_1-polynomials)**.** *Let g and h be AGL_1-polynomials of prime degrees q and p, respectively. Let $\Gamma = \ker(\mathrm{Mon}(g \circ h) \to \mathrm{Mon}(g))$.*

1. *Suppose $h \sim X^p$. Then $\Gamma = C_p^q$, unless one of the following holds:*
   - **a.** *$g \circ h \sim X^{pq}$ – in which case $\Gamma = \mathrm{diag}(C_p^q)$.*
   - **b.** *$p = 2$ and $g \circ h \sim T_{2q}$ – in which case $\Gamma = \mathrm{diag}(C_2^q)$.*
2. *Suppose $h \sim T_p$ for $p \geqslant 3$. Then $\Gamma = D_p^q$ or $\Gamma = \{(a_k)_{k=1}^q \in D_p^q \mid a_1 \cdots a_q \in C_p\}$, unless $g \circ h \sim T_{pq}$ – in which case*

$$\Gamma = \begin{cases} \mathrm{diag}(C_p^q) & \text{if } q \neq 2, \\ \mathrm{diag}(D_p^2) & \text{if } q = 2. \end{cases}$$

For the next statements, recall that there are two types of polynomials with monodromy group S_4: the *special type*, of ramification type $([3.1], [2.1^2], [4])$, and the *generic type*, of ramification type $([2.1^2], [2.1^2], [2.1^2], [4])$; see Proposition 3.1.

Theorem 2.2 (Composition of an S_4-polynomial and an AGL_1-polynomial)**.** *Let $g \in k[X]$ be a polynomial with monodromy group S_4, and let h be an AGL_1-polynomial of prime degree p. Let $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$. Then the following hold:*

1. *If $g \circ h \sim (X^3+1)^3 X^3 = X^3(X-1) \circ (X^3+1)$, then $\mathrm{Mon}(g \circ h) = S_4 \times C_3$.*
2. *If $g \circ h \sim X^3(X-1) \circ (X^2+b)$, where b is a root of $X^2 + \frac{1}{2}X + \frac{3}{16}$, then $\mathrm{Mon}(g \circ h) = GL_2(3) (= C_2.S_4)$.*
3. *In all other cases, $\Gamma \cap C_p^4$ has dimension at least 3. Moreover, one has $\Gamma \supseteq C_p^4$ unless:*
   - **a.** *$g \circ h \sim (X^2 + \frac{3}{4})^3 (X^2 - \frac{1}{4}) = X^3(X-1) \circ (X^2 + \frac{3}{4})$.*
   - **b.** *g is special, $h \sim T_p$, and -2 and 2 are both the preimages of the finite branch point of cycle type $[3,1]$ (in other words, $g \circ h \sim (X-2)^3(X+2) \circ T_p$).*
   - **c.** *$h \sim T_p$, and 2 and -2 are both the special points of g lying over the same finite branch point of cycle type $[2,1^2]$ (in other words, $g \circ h \sim (X-a)^2(X^2-4) \circ T_p$ for some $a \notin \{-2, 0, 2\}$).*

Theorem 2.3 (Composition of an AGL_1-polynomial and an S_4-polynomial)**.** *Let g be an AGL_1-polynomial of prime degree p, and let $h \in k[X]$ be a polynomial with monodromy group S_4. Let $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$. Then the following hold:*

1. *If $g \circ h \sim (X^3+1)^3 X^3 = X^3 \circ ((X^3+1)X)$, then $\mathrm{Mon}(g \circ h) = S_4 \times C_3$.*
2. *In all other cases, Γ contains V_4^p. Moreover, $\Gamma = S_4^p$ unless one of the following holds:*
   - a. *$g \sim X^p$, h is special, and the finite branch point of h of cycle type $[2,1^2]$ equals 0 (in other words, $g \circ h \sim (X^3(X-4)+27)^p$). In this case, one has $\Gamma \supseteq A_4^p$.*
   - b. *$g \sim T_p$, h is special, and the branch point of h of cycle type $[2,1^2]$ is one of the two special points ± 2 of g (in other words, $g \circ h \sim T_p \circ (aX \pm 2) \circ (X^3(X-4)+27)$ for some $a \neq 0$). In this case, $\Gamma/(\Gamma \cap V_4^p)$ contains $\mathrm{Aug}(C_3^p)$.*
   - c. *$g \sim X^p$ ($p \geqslant 5$), h is generic, and the three finite branch points of h map to the same point under g. In this case, one has $\Gamma \supseteq A_4^p$.*
   - d. *$g \sim T_p$, h is generic, and the three finite branch points of h are all ramified points of g lying over the same branch point (i.e., either 2 or -2). In this case, one has $\Gamma \supseteq A_4^p$.*
   - e. *$g \sim T_3$, h is generic and the three branch points of h all map to the same non-branch point $\gamma \neq \pm 2$ under T_3. Here $\Gamma/(\Gamma \cap V_4^3)$ contains $\mathrm{Aug}(C_3^3)$.*
   - f. *$g \sim X^2$, h is generic, and the three finite branch points u, v, w of h fulfill $u = 0$ and $v^2 = w^2$ (in other words, $g \circ h \sim (X^2(X^2 + (\omega+3)X + \frac{9}{8}\omega + \frac{27}{8}))^2$, where $\omega = \pm\sqrt{3}$). In this case, one has $\Gamma \supseteq A_4^2$.*

Theorem 2.4 (Composition of two S_4-polynomials)**.** *Let $g, h \in k[X]$ be S_4-polynomials. Let $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$. Then Γ contains $V_4^4 \rtimes C_3^2$. Moreover, Γ contains A_4^4 unless:*

1. *Both g and h are special, and the branch points of h of cycle types $[3,1]$ and $[2,1^2]$ are special points lying over the branch points of g of cycle types $[3,1]$ and $[2,1^2]$ respectively (i.e., $f \circ g \sim X(X+4)^3 \circ \alpha X(X+4)^3$, where α is a root of $X^2 - \frac{10}{27}X + \frac{1}{27}$).*
2. *g is special, h is generic, and the three branch points of h of cycle type $[2,1^2]$ are precisely the two points over the branch point of g of cycle type $[3,1]$, together with one more special point over the branch point of g of cycle type $[2,1^2]$.*
3. *Both g and h are generic, and the three branch points of h of cycle type $[2,1^2]$ are special points lying over pairwise distinct branch points of g of cycle type $[2,1^2]$.*

2.2. **Nonsolvable case.** This part is devoted to the refinements of the nonsolvable case of Theorem 1.2. Note that if the monodromy group of an indecomposable polynomial is nonsolvable, then this group is known by [Mül95] to be either an alternating or symmetric group, or contained in an explicitly known finite list; cf. Proposition 3.1.

Theorem 2.5 (Composition of an arbitrary indecomposable and a nonsolvable)**.** *Let $g \in k[X]$ be an indecomposable polynomial, and let $h \in k[X]$ be a nonsolvable polynomial. Let $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$. Then the following hold:*

1. *If there is a Ritt move for $g \circ h$, then necessarily $g \sim X^p$, and moreover $\mathrm{Mon}(g \circ h) \cong C_p \times \mathrm{Mon}(h)$.*
2. *In all other cases, $\Gamma \supseteq \mathrm{soc}(\mathrm{Mon}_k(h))^{\deg(g)}$.*

Theorem 2.6 (Composition of a nonsolvable with an AGL_1-polynomial)**.** *Let $g \in k[X]$ be a nonsolvable polynomial, and let h be an AGL_1-polynomial of prime degree p. Consider the block kernel $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$. Then the following hold:*

1. *If there is a Ritt move for $g \circ h$, then necessarily $h \sim X^p$, and moreover $\mathrm{Mon}(g \circ h) \cong C_p \times \mathrm{Mon}(g)$.*

2. *In all other cases,* $\mathrm{Mon}(g \circ h)$ *is either one of the nonsolvable groups in Table 1, or* Γ *contains a subgroup* $C_p^{\deg(g)-1}$.

Theorem 2.7 (Composition of a nonsolvable with an S_4-polynomial)**.** *Let* $g \in k[X]$ *be a nonsolvable polynomial, and let* $h \in k[X]$ *be an* S_4*-polynomial. Consider the block kernel* $\Gamma = \ker(\mathrm{Mon}_k(g \circ h) \to \mathrm{Mon}_k(g))$. *Then* Γ *contains* $V_4^{\deg(g)}$. *Moreover,* Γ *contains a subgroup* $C_3^{\deg(g)-1}$, *unless one of the following holds:*

- $\mathrm{Mon}(g) = PSL_3(3) \leqslant S_{13}$, *with the* 3*-Sylow group of* Γ *of order* 3^6 *or* 3^{10}.
- $\mathrm{Mon}(g) = PSL_2(11) \leqslant S_{11}$, *with the* 3*-Sylow group of* Γ *of order* 3^5.

3. Preliminaries

In this section, we establish preliminary results needed for the sequel.

3.1. **Setup.** Given two permutation groups $U \leqslant \mathrm{Sym}(m)$ and $V \leqslant \mathrm{Sym}(n)$, the *wreath product* $U \wr V$ is the semidirect product $U^n \rtimes V$, where V permutes the n copies of U. For any $n \geqslant 2$ and $m \geqslant 2$, the *augmentation subgroup* of C_m^n is

$$\mathrm{Aug}(C_m^n) = \{(a_1, \ldots, a_n) \in C_m^n \mid a_1 \cdots a_n = 1\}.$$

For a group G, an integer d and an element $x = (x_1, \ldots, x_d) \in G^d$, let $\mathrm{supp}(x) := \{i \in \{1, \ldots, d\} \mid x_i \neq 1\}$ denote the *support* of x.

Given groups G_1, G_2, H, and morphisms $\phi_1 : G_1 \to H, \phi_2 : G_2 \to H$, the *fiber product* of G_1 and G_2 over H is the subgroup of $G_1 \times G_2$ given by

$$G_1 \times_H G_2 := \{(g_1, g_2) \in G_1 \times G_2 \mid \phi_1(g_1) = \phi_2(g_2)\}.$$

The *affine general linear group of degree* 1 *over a field* F, denoted by $AGL_1(F)$, is the semidirect product $F \rtimes F^\times$, where $F^\times$ acts by multiplication on F; this group acts naturally on F, where F acts on itself by translation. An indecomposable polynomial $f \in k[X]$ is called an AGL_1*-polynomial* if $p = \deg(f)$ is prime and $\mathrm{Mon}(f)$ is solvable; equivalently, $\mathrm{Mon}_{\overline{k}}(f)$ is either cyclic or dihedral, that is, a permutation subgroup of $AGL_1(p)$.

A *function field* F over k is a finite extension of $k(t)$, where t is transcendental over k. Denote by g_F its *genus*. Let F_1/F be an extension of function fields over k. For a place Q of F_1 lying above a place P of F, write $e(Q \mid P)$ for the ramification index (cf. [Sti09, Definition 3.1.5]) of Q over P. Let $Q_1, \ldots, Q_r$ be the places of F_1 lying above a place P of F. The multiset

$$E_{F_1/F}(P) := [\, e(Q_1 \mid P), \ldots, e(Q_r \mid P) \,]$$

is called the *ramification type* of P in F_1. The place P is called a *branch point* of F_1/F if $e(Q_i \mid P) > 1$ for some i. Letting S be the set of branch points, we recall that S is finite. The multiset $\{\, E_{F_1/F}(P) : P \in S \,\}$ is called the *ramification type* of F_1/F.

Assume now that $F = k(t)$ and that the Galois closure of $F_1/k(t)$ has Galois group G, viewed as a transitive group of degree $n := [F_1 : k(t)]$. Write $S = \{P_1, \ldots, P_u\}$. For each $P \in S$, there is an associated $\pi_P \in G$ of cycle type $E_{F_1/F}(P)$. Each π_{P_i} is called the *inertia group generator* at P_i, and the tuple $(\pi_{P_1}, \cdots, \pi_{P_u})$ is also called the *branch cycle description* of $F/k(t)$. It is well-defined up to simultaneous conjugation in S_n (corresponding to relabeling of the set $\{1, \ldots, n\}$) and *braid group action* (see Section 3.5), and satisfies $\pi_{P_1} \cdots \pi_{P_u} = 1$. The *Riemann–Hurwitz formula* gives:

$$2(n - 1 + g(F_1)) = \sum_{Q \text{ place of } F_1} (e(Q \mid Q \cap k(t)) - 1) = \sum_{P \in S} \mathrm{ind}(\pi_P), \tag{1}$$

where the *index* $\mathrm{ind}(\pi)$ of $\pi \in S_n$ is defined as n minus the number of orbits of $\langle \pi \rangle$.

We say that $g \circ f$, for indecomposable $f, g \in k[X]$, is a *non-unique decomposition* if there exist indecomposable $u, v \in k[X]$ such that $g \circ f = u \circ v$, but there is no linear polynomial $\eta \in k[X]$ with $g = u \circ \eta$, $f = \eta^{-1} \circ v$. It is known due to Ritt's theorems ([Rit22]; see [ZM08] for a modern treatment) that non-unique decomposition is equivalent to the existence of a Ritt move. Recall that there is a *Ritt move* for $g \circ h$ if $\gcd(\deg(g), \deg(h)) = 1$ and there exist indecomposable polynomials $u, v \in k[X]$ such that

$$\deg(u) = \deg(g),\ \deg(v) = \deg(h),\ g \circ h = v \circ u,$$

and moreover, after possibly interchanging (g, h) and (v, u), there exist linear polynomials $\ell_1, \ell_2, \ell_3, \ell_4 \in k[X]$ such that the quadruple

$$\left(\ell_1 \circ g \circ \ell_2,\ \ell_2^{-1} \circ h \circ \ell_3,\ \ell_1 \circ v \circ \ell_4,\ \ell_4^{-1} \circ u \circ \ell_3 \right)$$

is of one of the following types:

$$\begin{gathered} (T_n,\ T_m,\ T_m,\ T_n), \\ (X^n,\ X^s h(X^n),\ X^s h(X)^n,\ X^n), \end{gathered} \tag{2}$$

where $m, n > 0$ are coprime, $s \geqslant 0$ is coprime to n, and $h \in k[X] \backslash X k[X]$.

3.2. **Monodromy groups of indecomposable polynomials.** We recall the most important results on indecomposable polynomials and their monodromy groups. The following essentially summarizes the classification results of [Mül95] (together with some more elementary considerations regarding the possibilities for indecomposables with solvable monodromy group, cf. [Mül98, Lemma 2.9]).

Proposition 3.1. Let k be an algebraically closed field of characteristic 0, and let $f \in k[X]$ be an indecomposable polynomial of degree > 1. Then one of the following holds:

1. $\mathrm{Mon}(f)$ is solvable, and moreover one of the following holds.
   - **a.** $f \sim X^p$ for a prime p. Here, the ramification type of f is $([p], [p])$.
   - **b.** $f \sim T_p$ for a prime $p \geqslant 3$. Here, the ramification type of f is $([2^{(p-1)/2}.1], [2^{(p-1)/2}.1], [p])$.
   - **c.** $\deg(f) = 4$ and $\mathrm{Mon}(f) = S_4$. Here either
     - **i.** $f \sim X^3(X-1)$, with ramification type $([3.1], [2.1^2], [4])$, or
     - **ii.** $f \sim X^2(X^2 + aX + a)$ for some $a \in k \backslash \{0, \frac{32}{9}, 4\}$,[3] with ramification type $([2.1^2], [2.1^2], [2.1^2], [4])$.
2. $\mathrm{Mon}(f)$ is a nonsolvable almost simple group, and moreover one of the following holds.
   - **a.** $\mathrm{Mon}(f) = S_n$ $(n \geqslant 5)$ or A_n $(n \geqslant 5$ odd), with many possible ramification types.
   - **b.** $\mathrm{Mon}(f) \in \{PGL_2(5), PSL_3(2), PGL_2(7), P\Gamma L_2(8), P\Gamma L_2(9), PSL_2(11), M_{11}, PSL_3(3), PSL_4(2), P\Gamma L_3(4), M_{23}, PSL_5(2)\}$, of degree $6, 7, 8, 9, 10, 11, 11, 13, 15, 21, 23$ and 31, respectively. Here, all possible ramification types for f are explicitly known.

[3] The exclusion of the three values $a = 0$, $a = \frac{32}{9}$ and $a = 4$ is due to the fact that these (and only these, as a quick discriminant calculation shows) decrease the number of branch points, with exactly the value $\frac{32}{9}$ leading to an indecomposable, namely as in Case 1c)i.

3.3. **Kernel estimates.** In this section we collect various auxiliary results which will prove useful when lower-bounding the kernel $G \cap \ker(\pi)$ for transitive groups $G \leqslant U \wr V$ (where $\pi : U \wr V \to V$) is the projection), in particular for the various cases where U is one of the solvable primitive monodromy groups occuring in Proposition 3.1.

Note that, when $V \leqslant S_n$ is a transitive group, $G \leqslant AGL_1(p) \wr V$ and $\Gamma = \ker(\pi : G \to V)$ is an elementary-abelian p-group, Γ becomes a submodule of the $\mathbb{F}_p[V]$-module C_p^n, and the fact that V permutes the components setwise implies that the associated representation on C_p^n is monomial. It is thus induced from the point stabilizer $V_1 \leqslant V$ by a degree-1 representation $\psi : V_1 \to \mathbb{F}_p^\times$, which describes the action of the block stabilizer $\pi^{-1}(V_1)$ on a block (cf., e.g., [CR66, Exercise 43.1]). When ψ is the trivial representation, C_p^n becomes naturally[4] isomorphic to the $\mathbb{F}_p[V]$-permutation module $\mathbb{F}_p \cdot \mathbf{e}_1 \oplus \cdots \oplus \mathbb{F}_p \cdot \mathbf{e}_n$, and often this is enforced by the structure of G, e.g., when $G \leqslant C_p \wr V$, or when $G \leqslant D_p \wr V$ and V_1 does not have a quotient C_2.

In particular, in the case where additionally V is a cyclic group of order n and $\langle \sigma \rangle \leqslant G$ a preimage of V under π with $\sigma^n \in C_p^n$, by the above, the $\mathbb{F}_p[V]$-(permutation) module $\mathbb{F}_p^n$ becomes the cyclic code $\mathbb{F}_p[x]/(x^n - 1)$.

Due to this special importance of the permutation module, the action of a $G \leqslant S_n$ acting on a direct product U^n should always be understood as the action via permutation of components in the following; in particular, when $U = \mathbb{F}_p$ and $\mathbf{v} \in U^q$, the module $\langle G \cdot \mathbf{v} \rangle$ shall denote the submodule of the $\mathbb{F}_p[G]$-permutation module generated by $\mathbf{v}$.

In the following, for a field K and an integer $n \geqslant 1$, we denote by $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ the canonical basis of K^n.

3.3.1. *On groups $G \leqslant U \wr V$ with U cyclic.* The following results are useful to obtain "large kernel" conclusions for subgroups of $C_p \wr C_q (= \mathbb{F}_p^q \rtimes C_q)$, $C_p \wr D_q$ or $C_p \wr S_4$, under the assumption that the kernel contains a certain "short vector".

Lemma 3.2. *Let p, q be primes with $p \not\equiv 1 \bmod q$, and let $\mathbf{v} = \mathbf{e}_i + \mu \mathbf{e}_\mathbf{j} \in \mathbb{F}_p^q$, with $i \neq j$ and with $\mu \in \mathbb{F}_p^\times$. Then $\langle C_q \cdot \mathbf{v} \rangle = \begin{cases} \mathrm{Aug}(\mathbb{F}_p^q), & \text{if } \mu = -1, \\ \mathbb{F}_p^q, & \text{otherwise.} \end{cases}$*

Proof. Due to transitivity of C_q in the permutation action, we may assume $j = 0$ without loss of generality. The cyclic code $\langle C_q \cdot \mathbf{v} \rangle$ thus has generator polynomial $\gcd(X^q - 1, X^i + \mu)$. Any root of $X^i + \mu$ in $\overline{\mathbb{F}_p}$ has multiplicative order dividing $i(p-1)$, and since $i < q$ and $p \not\equiv 1 \bmod q$, this order is coprime to q. Hence, $\gcd(X^q - 1, X^i + \mu)$ cannot have any irreducible factor apart from $X - 1$, which also cannot be a multiple factor since one of $X^q - 1$ and $X^i + \mu$ is separable. Of course $X - 1 \mid X^i + \mu$ if and only if $\mu = -1$. The assertion now follows via noting that the polynomial $X - 1$ generates the augmentation ideal. □

The next lemma gives a similar conclusion for cyclic groups C_q not necessarily of prime order. To state it, for $m \geqslant 2$ and even $q \geqslant 2$, we define

$$\mathrm{Aug}^-(C_m^q) = \{(a_1, \ldots, a_q) \in C_m^q \mid a_1 a_2^{-1} \cdots a_{q-1} a_q^{-1} = 1\}.$$

[4] Namely, via mapping $\mathbf{e}_i$ to a suitable generator of the i-th component of C_p^n.

Lemma 3.3. *Let p be a prime, $q \geqslant 2$ an arbitrary integer and $\mathbf{v} = \mathbf{e}_j + \mathbf{e}_{i+j} \in \mathbb{F}_p^q$, $i \neq 0$. Let $o(i)$ denote the additive order of $i \in \mathbb{Z}/q\mathbb{Z}$. Then*

$$\langle C_q \cdot \mathbf{v} \rangle = \begin{cases} \left(\mathrm{Aug}(C_2^{o(i)})\right)^{\frac{q}{o(i)}}, & \text{if } p = 2, \\ \left(\mathrm{Aug}^-(C_p^{o(i)})\right)^{\frac{q}{o(i)}}, & \text{if } p \geqslant 3 \text{ and } o(i) \text{ is even}, \\ \mathbb{F}_p^q, & \text{otherwise.} \end{cases}$$

(Here, the $\frac{q}{o(i)}$ copies of $C_p^{o(i)}$ in the direct product are to be understood as the sets $\{x \in C_p^q \mid \mathrm{supp}(x) = \{j + k \cdot \frac{q}{o(i)} \mid k = 1, \dots, o(i)\}\}$, for $j = 1, \dots, \frac{q}{o(i)}$.)

Proof. $\langle C_q \cdot \mathbf{v} \rangle$ is the cyclic $\mathbb{F}_p$-code of length q with generator polynomial

$$\gcd(X^q - 1, X^i + 1) = \begin{cases} X^{q/o(i)} + 1, & \text{if } o(i) \text{ is even or } p = 2, \\ 1, & \text{else.} \end{cases}$$

In the latter case, $\langle C_q \cdot \mathbf{v} \rangle = \mathbb{F}_p^q$, so assume the former case, i.e., $\dim(\langle C_q \cdot \mathbf{v} \rangle) = q - \frac{q}{o(i)}$. Due to the containment of the generator $\mathbf{e}_0 + \mathbf{e}_i$ in $\left(\mathrm{Aug}^-(C_p^{o(i)})\right)^{\frac{q}{o(i)}}$ (resp., in $\left(\mathrm{Aug}(C_2^{o(i)})\right)^{\frac{q}{o(i)}}$ when $p = 2$), equality of the two modules follows readily. □

The next results are useful for analysing groups $G \leqslant U \wr V$ with V dihedral, resp., $V = S_4$.

Lemma 3.4. *Let $q \geqslant 5$ be a prime, and $\mathbf{v} \in \mathbb{F}_2^q$ a vector such that $\mathrm{supp}(\mathbf{v})$ is of size 4 and invariant under some reflection of D_q. Then $\langle C_q \cdot \mathbf{v} \rangle = \mathrm{Aug}(\mathbb{F}_2^q)$.*

Proof. Invariance under a reflection implies that $\mathrm{supp}(\mathbf{v})$ is of the form $\{i_0, i_0 + i, j, j + i\}$ for suitable $i_0, i, j \in \mathbb{F}_q$. We may assume $i_0 = 0$ without loss of generality. The cyclic code $\langle C_q \cdot \mathbf{v} \rangle$ thus has generator polynomial $\gcd(X^q - 1, 1 + X^i + X^j + X^{j+i}) = \gcd(X^q - 1, (X^j - 1)(X^i - 1)) = X - 1$, i.e., $\langle C_q \cdot \mathbf{v} \rangle = \mathrm{Aug}(\mathbb{F}_2^q)$ as claimed. □

Corollary 3.5. Let $q \geqslant 5$ be a prime, and let $\mathbf{v} \in \mathbb{F}_2^q$ with $|\mathrm{supp}(\mathbf{v})| = 3$. Then $\langle D_q \cdot \mathbf{v} \rangle = \mathbb{F}_2^q$.

Proof. Write $\mathrm{supp}(\mathbf{v}) = \{i, j, k\} \subset \mathbb{F}_q$. Since $q > 3$, we may assume (after reordering) that $j - i \neq k - j$. Without loss of generality, we may assume $j = 0$. Let $\sigma \in D_q$ be the reflection of coordinates $d \mapsto -d$ ($d \in \mathbb{F}_q$). Then

$$\mathbf{w} := \mathbf{v} + \sigma \cdot \mathbf{v} = \mathbf{e}_i + \mathbf{e}_{-i} + \mathbf{e}_k + \mathbf{e}_{-k}$$

has support invariant under σ. Lemma 3.4 implies that $\langle C_q \cdot \mathbf{w} \rangle$ contains $\mathrm{Aug}(\mathbb{F}_2^q)$. Moreover, as $\langle D_q \cdot \mathbf{v} \rangle \supseteq \langle C_q \cdot \mathbf{w} \rangle$ and $\mathbf{v} \notin \mathrm{Aug}(\mathbb{F}_2^q)$, it follows that $\langle D_q \cdot \mathbf{v} \rangle = \mathbb{F}_2^q$. □

Lemma 3.6. *Let $\mathbf{v} \in \mathbb{F}_p^4$ with $1 \leqslant |\mathrm{supp}(\mathbf{v})| \leqslant 3$. Then $\langle S_4 \cdot \mathbf{v} \rangle$ contains $\mathrm{Aug}(\mathbb{F}_p^4)$.*

Proof. Without loss of generality, we may assume that $v_1 \neq 0$ and $v_2 = 0$. Then

$$\mathbf{e}_1 - \mathbf{e}_2 = \frac{\mathbf{v} - (1,2) \cdot \mathbf{v}}{v_1} \in \langle S_4 \cdot \mathbf{v} \rangle,$$

which implies that $\mathrm{Aug}(\mathbb{F}_p^4) \leqslant \langle S_4 \cdot \mathbf{v} \rangle$. □

The fact that monodromy groups of polynomials necessarily contain a cyclic transitive subgroup can also often be helpful in obtaining lower bounds for kernels.

Lemma 3.7. *Let σ be an mn cycle in $C_n \wr S_m$ with $m, n \geqslant 2$. Then σ^m is a nontrivial element of $\mathrm{diag}(C_n^m)$.*

Proof. Write $\sigma = ((a_1, \dots, a_m), \tau)$, where $a_i \in C_n$ and τ is an m cycle in S_m. A direct computation shows that

$$\sigma^m = \left(\prod_{i=1}^{m} a_i, \dots, \prod_{i=1}^{m} a_i \right) \in \mathrm{diag}(C_n^m),$$

which is nontrivial. □

3.3.2. *On groups $G \leqslant U \wr V$ with U non-cyclic.* For the case of subgroups $G \leqslant U \wr V$ with certain *noncyclic* groups U (notably, U a noncyclic solvable monodromy group of an indecomposable polynomial), the following is useful to obtain "large kernel" conclusions.

Lemma 3.8. *Let $d \geqslant 3$.*

(1) Let q be an odd prime, $G \leqslant AGL_1(q) \wr S_d$ a transitive subgroup, and $K := \ker(G \to S_d)$. Assume that there exist elements $x_1, \dots, x_s \in K$ ($s \geqslant 1$) of order coprime to q such that $|\bigcap_{j=1}^{s} \mathrm{supp}(x_j)| = 1$. Then K contains C_q^d as a minimal normal subgroup.

(2) Let $G \leqslant S_4 \wr S_d$ be a transitive subgroup, and $K := \ker(G \to S_d)$. Assume that there exist elements $x_1, \dots, x_s \in K$ ($s \geqslant 1$) of order 3 such that $|\bigcap_{j=1}^{s} \mathrm{supp}(x_j)| = 1$. Then K contains V_4^d as a minimal normal subgroup.

Lemma 3.8 is a special case of the following more general statement, which is of interest in its own right, even though not used in full generality in this paper.

Lemma 3.9. *Let $H = W.U$, where W is a faithful $\mathbb{F}_p[U]$-module. Let $G \leqslant H \wr S_d$ be such that $\pi : G \to S_d$ maps onto a transitive subgroup of S_d, and let $\Gamma = \ker(\pi) = G \cap H^d$. Furthermore, let $\rho : \Gamma \to U^d$ be the natural projection and $\Delta = \ker(\rho) = \Gamma \cap W^d$. Assume all of the following:*

i) The image of Γ under projection to one (hence any, due to transitivity of G in the blocks action) component equals $W.U'$ for a subgroup $U' \leqslant U$ such that $W = W_1 + \cdots + W_r$ is a direct sum of irreducible $\mathbb{F}_p[U']$-modules W_j, $j = 1, \dots, r$.

ii) There exist elements $x_1, \dots x_s \in \Gamma$ ($s \geqslant 1$) and $i \in \{1, \dots, d\}$ such that, for all $j = 1, \dots, r$,

$$\bigcap_{m=1}^{s} \mathrm{supp}(\rho_j(x_m)) \subseteq \{i\}, \tag{3}$$

where $\rho_j(x)$ denotes the image of $\rho(x)$ in $GL(W_j)^d$.

Then $\Delta \supseteq W'^d$, where W' is defined as the sum of the W_j for which equality holds in (3).

Proof. We begin by noting an important consequence of the assumptions:
Observation 1: Given any $\gamma \in \Gamma$ whose i-th component γ_i lies in $W_j \backslash \{0\}$ and any $1 \neq u \in U$ acting nontrivially on W_j, there exists $\tilde{\gamma} \in \Gamma$ conjugate to γ such that $\tilde{\gamma}_i$ lies in W_j and is not fixed by u (i.e., $\tilde{\gamma}_i^u \neq \tilde{\gamma}_i$). Indeed, irreducibility of W_j implies that the module generated by γ_i^g, $g \in W.U'$ is all of W_j, and nontrivial action of u then implies that there exists $g \in W.U'$ such that γ_i^g is not fixed by u. It thus suffices to take $\tilde{\gamma} = \gamma^h$, where $h \in \Gamma$ is an element with i-th component entry equal to g, which is possible by Assumption i).

Now, let $x_1, \dots, x_s$ be as in Assumption ii), and fix an index $j \in \{1, \dots, r\}$ for which equality holds in (3). As in ii), let $i \in \{1, \dots, d\}$ denote the unique element of $\bigcap_{m=1}^{s} \mathrm{supp}(\rho_j(x_m))$.

Claim 1: For any $k = 0, \dots, s$, there exists $z \in \Gamma$ whose i-th component z_i lies in $W_j \backslash \{0\}$ and such that for all $n = 1, \dots, r$, $\mathrm{supp}(\rho_n(z)) \subseteq (\bigcap_{m=1}^{k} \mathrm{supp}(\rho_n(x_m))) \backslash \{i\}$.

The base case $k = 0$ simply amounts to the assertion that the image of Γ under projection to the i-th component contains W_j, which holds due to Assumption i). Assume inductively

that the claim holds for $k-1$, with some element $z \in \Gamma$. Due to Observation 1, there exists a Γ-conjugate $\tilde{z}$ of z with $\tilde{z}_i \in W_j$ not fixed by the i-th component entry $(x_k)_i$ of x_k. Of course, since conjugation in Γ is defined component-wise, we have $\mathrm{supp}(\rho_n(z)) = \mathrm{supp}(\rho_n(\tilde{z}))$ (for any $n \in \{1,\dots,r\}$). Let $\widehat{z} := [\tilde{z}, x_k]$. Then $\widehat{z}_i \in W_j \backslash \{0\}$ by construction, and moreover $\rho_n(\widehat{z})$ is trivial on every component $m \neq i$ on which at least one of $\rho_n(\tilde{z})$ and $\rho_n(x_k)$ is not supported; in other words, due to the induction hypothesis, $\mathrm{supp}(\rho_n(\widehat{z})) \subseteq (\bigcap_{m=1}^{k} \mathrm{supp}(\rho_n(x_m))) \backslash \{i\}$. This completes the proof of Claim 1.

We next choose $z \in \Gamma$ fulfilling Claim 1 for $k = s$. Due to Assumption iii), this implies $\mathrm{supp}(\rho_n(z)) = \varnothing$, i.e., all component entries of z act trivially on W_n, for all $n \in \{1,\dots,r\}$. Faithfulness of U on W' thus implies that all component entries lie in W, i.e., $z \in \Delta$.

Claim 2: For any $k = 0,\dots,s$, there exists $z' \underline{\in \Delta}$ with $\{i\} \subseteq \mathrm{supp}(z') \subseteq \bigcap_{m=1}^{k} \mathrm{supp}(\rho_n(x_m))$ for all $n = 1,\dots,r$, and such that the i-th component z'_i of z' lies in W_j.

For this, we again argue by induction over k. The base case $k = 0$ is obtained with $z' = z$ as chosen above. Assume inductively that there exists $z' \in \Delta$ with $z'_i \in W_j$ and $\{i\} \subseteq \mathrm{supp}(z') \subseteq \bigcap_{m=1}^{k-1} \mathrm{supp}(\rho_n(x_m))$. Using again Observation 1), we obtain $\tilde{z} \in \Delta$ with $\mathrm{supp}(z) = \mathrm{supp}(\tilde{z})$, and such that the i-th component $(\tilde{z})_i$ lies in W_j and is not fixed by $(\rho_j(x_k))_i \neq 1$. Finally, consider the commutator $\widehat{z} := [\tilde{z}, x_k] \in \Delta$.

This has trivial W_n-part on all components not simultaneously supported by $\tilde{z}$ and $\rho_n(x_k)$, i.e., by construction of $\tilde{z}$, on all components outside $\bigcap_{m=1}^{k} \mathrm{supp}(\rho_n(x_m))$ (for all $n \in \{1,\dots,r\}$). At the same time, the i-th component is a non-zero element of W_j by construction. This completes the induction step, and by setting $k = s$, we may assume $\mathrm{supp}(\widehat{z}) = \{i\}$. Conjugating $\widehat{z}$ by all $\gamma \in \Gamma$, we obtain that the set of elements of Δ supported only on the i-th component contains all of W_j, and thus (upon repeating the construction for all $W_j \subseteq W'$), all of W'. Thus $\Delta \supseteq W'^d$. □

Proof of Lemma 3.8 using Lemma 3.9. In both cases 1) and 2) of Lemma 3.8, the claimed containment follows directly from Lemma 3.9 (with $r = 1$ and $W = W'$): in 1), take $C_p < H \leqslant AGL_1(p)$, with $W = C_p$ being the one-dimensional module under the action of $\{1\} \neq U' \leqslant C_{p-1}$. Similary, in 2), take $ASL_2(2) = A_4 \leqslant H \leqslant S_4 = AGL_2(2)$, with $W = \mathbb{F}_2^2$ and $C_3 \leqslant U' \leqslant S_3 \cong S_4/W$. Finally, minimality follows from the fact that, in the proof of Lemma 3.9, every non-zero vector $0 \neq z \in W$ is admissible as a starting vector of the construction, i.e., the normal subgroup generated by z is all of W^d. □

We collect some situations in which we wish to apply Lemma 3.8 later on.

Lemma 3.10. *In the setting of Lemma 3.8, the condition* $|\bigcap_{j=1}^{s} \mathrm{supp}(x_j)| = 1$ *for some* $x_1,\dots,x_s \in K$ *is in particular fulfilled in the following cases.*

- *a) Whenever* $K/\mathrm{soc}(K)$ *contains the augmentation subgroup* $\mathrm{Aug}(C_2^d)$ *(in case (1) of Lemma 3.8), resp.* $\mathrm{Aug}(C_3^d)$ *(in case (2)).*
- *b) Whenever there exists* $x \in K$ *(of the respective order specified in (1) and (2) of Lemma 3.8) with* $1 \leqslant |\mathrm{supp}(x)| < d$*, and the blocks image* $A := \mathrm{Im}(G \to S_d)$ *is primitive (in particular, the latter is automatic whenever* $d \geqslant 3$ *is a prime).*

Proof. a) is obvious. For b), it suffices to note the following: if $S \subseteq K$ is a maximal (with respect to inclusion) subset of elements of the respective specified order such that $\Delta := \bigcap_{x \in S} \mathrm{supp}(x) \neq \varnothing$, then Δ is a block under the action of A. Indeed, suppose $\varnothing \neq \Delta \cap \Delta^g \neq \Delta$ for some $g \in A$; then $\bigcap_{x \in S \cup S^g} \mathrm{supp}(x) = \Delta \cap \Delta^g \neq \varnothing$, contradicting maximality of S. □

3.3.3. *On groups $G \leqslant U \wr V$ with $V \in \{A_n, S_n\}$.* For groups $\mathrm{Mon}(g \circ h)$ with nonsolvable $\mathrm{Mon}(g) \in \{A_n, S_n\}$, large kernel conclusions are often more easily obtained. The following is immediate from [Mor80].

Lemma 3.11. *Let $V = A_n, S_n$ for $n \geqslant 4$, and let p be a prime. Then the only V-invariant subgroups of C_p^n are* 0, $\mathrm{diag}(C_p^n)$, $\mathrm{Aug}(C_p^n)$ *and* C_p^n.

The following lemma is useful for analyzing the case of compositions $g \circ T_p$ where g is an S_n-polynomial ($n \geqslant 4$).

Lemma 3.12. *Let $U \in \{C_p, D_p\}$ for a prime p, $V \in \{A_n, S_n\}$ ($n \geqslant 4$) and let $G \leqslant U \wr V$ be a transitive subgroup projecting onto V, with block kernel $\Gamma := \ker(G \to V)$. Then one of the following holds:*

i) Γ contains a subgroup C_p^{n-1}.
ii) G embeds into $U \times V$.
iii) $n = 4$, and $G/(\Gamma \cap C_p^4)$ (for $p > 2$) resp. G (for $p = 2$) is isomorphic to $SL_2(3) (\cong 2.A_4)$ or $GL_2(3) (\cong 2.S_4)$.
iv) $n = 6$, and G is a nonsplit extension $G \cong 3.V$.

Proof. Let $H = G/(\Gamma \cap C_p^n)$ (for $p > 2$), resp. $H = G$ (for $p = 2$). Then H embeds into $C_2 \wr S_n$, and surjects onto S_n or A_n. We next consider the exact sequence

$$1 \to H \cap C_2^n \to H \cap (C_2 \wr A_n) \to A_n \to 1. \tag{4}$$

For $n \geqslant 5$, this sequence splits by [KNR24, Lemma 7.2]. For $n = 4$, one may verify directly that there is exactly one nonsplit extension embedding into $C_2 \wr A_4$, namely $\mathrm{SL}_2(3)$.

In total, exempting the case that H contains $SL_2(3)$ as a subgroup of index at most 2 (i.e., Case iii) of the assertion), $\Gamma \cap C_p^n$ becomes a submodule of the $\mathbb{F}_p[A_n]$-permutation module. But the latter only has two nontrivial submodules, of dimensions 1 and $n-1$ by Lemma 3.11. To show that we are in Case i) of our assertion, we thus only need to show $|\Gamma \cap C_p^n| > p$. Assume on the contrary that $|\Gamma \cap C_p^n| = p$. Then $\Gamma \in \{C_p, D_p\}$.

Moreover, A_n acts trivially on Γ (this is obvious when $n \geqslant 5$, and holds also for $n = 4$ since a nontrivial action via the cyclic quotient C_3 of A_4 would be incompatible with the assumption $G \leqslant D_p \wr V$ (meaning that a block stabilizer acts on the block as a subgroup of D_p)). Now if the extension $\Gamma.A_n$ were nonsplit, then due to the splitting of (4), $C_p.A_n$ would have to be a nonsplit central extension, which firstly enforces $p > 2$ as already seen, and then exists only for $p = 3$ and $n = 6, 7$; the case $n = 7$, however, cannot occur since a nonsplit extension $3.A_7$ does not have a faithful transitive degree 21 action. Excluding thus finally Case iv) of the assertion, we obtain that G contains $C_p \times A_n$ or $D_p \times A_n$ as a subgroup of index at most 2. Then G itself must embed into $U \times V$. □

3.4. **Ritt moves and direct products.** For this subsection, assume that $k = \overline{k}$ is an algebraically closed field of characteristic 0.

Proposition 3.13. Suppose $g, h \in k[X]$ are indecomposable polynomials such that $g \circ h$ admits a Ritt move. Then $\mathrm{Mon}(g \circ h)$ embeds into $\mathrm{Mon}(g) \times \mathrm{Mon}(h)$, with equality as long as $g \circ h$ is not linearly equivalent to T_{pq} for primes p, q.

Proof. Following (Corollary 2.11 and) Theorem 2.13 of [ZM08], one has an equality $g \circ h = \tilde{h} \circ \tilde{g}$ with isomorphisms $\mathrm{Mon}(\tilde{g}) \cong \mathrm{Mon}(g)$ and $\mathrm{Mon}(\tilde{h}) \cong \mathrm{Mon}(h)$ of permutation groups. Denote by U and V the subgroups of $G := \mathrm{Mon}(g \circ h)$ fixing a root of $g(X) - t$ and of $\tilde{h}(X) - t$ respectively. In particular the image of U acting on cosets of $U \cap V$ equals (the

image of G acting on cosets of V, i.e.) $\mathrm{Mon}(h)$, and the image of V acting on cosets of $U \cap V$ equals $\mathrm{Mon}(g)$. Since $U \cap V$ equals the stabilizer of a root of $g(h(X)) - t$, its core $\mathrm{core}_G(U \cap V)$ is trivial; on the other hand it is elementary that $G/\mathrm{core}_G(U \cap V)$ injects into $G/\mathrm{core}_G(U) \times G/\mathrm{core}_G(V) = \mathrm{Mon}(g) \times \mathrm{Mon}(h)$. If additionally, $g \circ h$ is not linearly equivalent to T_{pq}, then by Ritt's theorems (see (2)), one of g and h (say, h, without loss of generality) is linearly equivalent to X^p. In particular, $\mathrm{Mon}(g \circ h)$ is then a subgroup of $\mathrm{Mon}(g) \times C_p$, surjecting onto $\mathrm{Mon}(g)$. If $\mathrm{Mon}(g \circ h) < \mathrm{Mon}(g) \times C_p$ was a proper subgroup, it would have to equal $\mathrm{Mon}(g)$, which is however impossible, since $\ker(\mathrm{Mon}(g \circ h) \to \mathrm{Mon}(g)) > 1$ due to the presence of a full cycle in $\mathrm{Mon}(g \circ h)$. □

Proposition 3.14. Let $g, h \in k[X]$ be indecomposable polynomials such that the following hold:

a) h is an AGL_1-polynomial.
b) g is *not* an AGL_1-polynomial.
c) $\mathrm{Mon}(g \circ h)$ embeds into $\mathrm{Mon}(h) \times \mathrm{Mon}(g)$.

Then one of the following holds.

1. $g \circ h$ admits a Ritt move.
2. $h \sim X^p$, and moreover

$$(p, \mathrm{Mon}(g)) \in \{(2, PSL_3(2)), (2, M_{11}), (2, PSL_3(3)), (3, A_5), (3, PGL_2(7))\}.$$

Proof. Let $U := \mathrm{Mon}(g)$, $V := \mathrm{Mon}(h)$ (viewed in their natural permutation actions), and let $G := \mathrm{Mon}(g \circ h)$ embed into $V \times U$. By assumptions a) and b), we have $V \in \{C_p, D_p\}$ for a prime p, and either $U = S_4$ or U is an almost simple group. Since $\mathrm{Mon}(g \circ h) \to \mathrm{Mon}(g)$ is surjective, we know that G surjects onto U, and, up to excluding the single case $(U, V) = (S_4, C_2)$ (for which the assertion can be checked directly), there is only a single normal subgroup $N \lhd G$ (namely, $N = G \cap (V \times \{1\})$) with quotient U.[5] Fix an isomorphism $\sigma : G/N \to U$, and denote by $\pi : G \to U$ the composition of projection $G \to G/N$ with σ. It follows that the stabilizer in G of a root of $g(X) - t$ must be of the form $H := G \cap (V \times U_1) = \pi^{-1}(U_1)$, where $U_1 < U$ is a point stabilizer. We are interested in the stabilizer $G_1 < G$ of a root of $g(h(X)) - t$. If G_1 has another nontrivial overgroup apart from H, then this implies a non-unique decomposition for $g \circ h$, i.e., a Ritt move.

Since $\mathrm{Mon}(h) \in \{C_p, D_p\}$, we know that the image of H acting on cosets of G_1 is C_p or D_p. In all cases where U_1 has no quotient C_p or D_p, there is only a single candidate for such an action, namely $G_1 = G \cap (V_1 \times U_1)$, where $V_1 \leqslant V$ is a point stabilizer. But this clearly has the nontrivial overgroup $G \cap (V_1 \times U)$, showing that we are indeed in Case 1 of the assertion. Examining the point stabilizers of the exceptional monodromy groups $U \notin \{A_n, S_n\}$, this already yields Case 1 of the assertion unless $p \in \{2, 3\}$. Moreover, in case U_1 has a quotient C_p ($p = 2$ or 3) or D_p ($p = 3$) which is however inherited (via restriction) from the same quotient of U, we still obtain Case 1 of the assertion.

We are therefore left with the case where U_1 has a "new" quotient C_p or D_p compared to U. Going in particular through the list of monodromy groups of indecomposable polynomials from [Mül95], one finds that apart from the possibilities given in Case 2 (which can be verified with Magma to indeed occur as monodromy groups of a suitable polynomial with a *unique*

[5] Indeed, when $U = \mathrm{Mon}(g) \neq S_4$, it is almost simple, and this N then becomes the largest solvable normal subgroup.

decomposition), this leaves only the possibilities $U = S_5$ (for which $U_1 = S_4$ has a "new" D_3-quotient), $U = PSL_3(2)$ (for which again $U_1 \cong S_4$ has a new D_3-quotient) and $U = PSL_3(3)$ (whose stabilizer again has a new D_3-quotient). For the last two cases, a direct check in Magma's transitive group database yields that no embedding of G into $U \times D_3$ is such that the point stabilizer has a unique maximal overgroup, whereas for the first case, the only such candidate group (i.e., embedding into $S_5 \times D_3$ and having a unique maximal overgroup of the point stabilizer) is $15T21 \cong 3.S_5$, which however has no generating genus-0 tuples corresponding to a polynomial ramification type. This concludes the proof. □

Remark 3.15. a) The final result of Theorem 1.2 shows that the conclusion of Proposition 3.14 actually holds without changes even when dropping assumptions a) and b).

b) Note that the assumption that $G := \mathrm{Mon}(g \circ h)$ is in fact the geometric monodromy group of a polynomial was not used in the proof for the case $\mathrm{Mon}(g) = A_n, S_n$ for $n \geqslant 6$ (and for $n = 5$, only to rule out the one further exceptional case $G = 15T21$).

3.5. **Topological ideas: coalescing of branch points and braid group action.** A useful idea to lower-bound the monodromy group of a polynomial f with $r \geqslant 4$ branch points and branch cycles $\pi_1, \ldots, \pi_r$ (with $\pi_1 \cdots \pi_r = 1$) is the following observation: assume that π_1 is the inertia group generator at infinity, i.e., is a full cycle in $\mathrm{Mon}_{\overline{k}}(f)$. Of course, $\langle \pi_1, \ldots, \pi_{r-1} \rangle \supseteq \langle \pi_1, \ldots, \pi_{r-2} \rangle$, where the left side equals $\mathrm{Mon}_{\overline{k}}(f)$, and the right side is still a transitive subgroup of $\mathrm{Mon}_{\overline{k}}(f)$ (due to the presence of the full cycle π_1); the group $\langle \pi_1, \ldots, \pi_{r-2} \rangle$ is thus the monodromy group of a polynomial[6] with branch cycles $\pi_1, \ldots, \pi_{r-2}, \pi_{r-1}\pi_r$, which topologically corresponds to a deformation of a family of covers $\mathbb{P}^1 \to \mathbb{P}^1$, letting the $r-1$th and r-th branch point coalesce (see, e.g., [Cou96]).

Note furthermore that the branch cycles of a polynomial map f of degree d and with r branch points are only uniquely defined up to relabelling of the points $1, \ldots, d$ (i.e., conjugation in S_d) and action of the *Hurwitz braid group* B_r. The latter is defined as the group generated by braids $\beta_1, \ldots, \beta_{r-1}$ fulfilling the relations

$$\beta_i\beta_j = \beta_j\beta_i, \text{ for all } i < j-1,$$
$$\beta_i\beta_{i+1}\beta_i = \beta_{i+1}\beta_i\beta_{i+1}, \text{ for all } 1 \leqslant i \leqslant r-2, \text{ and}$$
$$\beta_1\beta_2 \cdots \beta_{r-1}\beta_{r-1} \cdots \beta_1 = 1;$$

and acting on r-tuples of branch cycles via

$$(\pi_1, \ldots, \pi_r)^{\beta_i} := (\pi_1, \ldots, \pi_{i-1}, \pi_i\pi_{i+1}\pi_i^{-1}, \pi_i, \ldots, \pi_r).$$

See [MM99, Chapter III.1] for the topological interpretation of this action. In our applications, applying the braid group action can be useful for polynomials $f = g \circ h$ where g is the generic type S_4 polynomial (i.e., with four branch points, of ramification type $[4]$, $[2.1^2]$, $[2.1^2]$, $[2.1^2]$). It is well-known (and of course easy to verify computationally for the case of degree 4) that the 4-tuples $(\pi_1, \ldots, \pi_4)$ of generic type as above lie in a single orbit of the braid group. Since the braid group action does not change the group generated by the respective r-tuple, we may therefore assume without loss of generality that the branch cycles for the generic type S_4 polynomial are $(1,2,3,4), (1,2), (1,3), (1,4)$ (with multiplication of permutations defined

[6] That the tuple $(\pi_1, \ldots, \pi_{r-2}, \pi_{r-1}\pi_r)$ indeed yields the monodromy group of a *polynomial* can be seen easily from the fact that the full cycle π_1 is contained, together with the fact that the genus given by the tuple $(\pi_1, \ldots, \pi_{r-2}, \pi_{r-1}\pi_r)$ is upper bounded by the one given by $(\pi_1, \ldots, \pi_{r-2}, \pi_{r-1}, \pi_r)$ (which however is zero); the latter fact can easily seen combinatorially from the Riemann-Hurwitz genus formula (1), or from the topological interpretation via deformation of covers.

from right to left), and therefore letting either the second and third or the third and fourth branch point coalesce (in the sense explained above) yields an S_4 polynomial of special type.

4. Solvable case: proofs of Theorems 2.1, 2.2, 2.3 and 2.4

Let k be an algebraically closed field of characteristic 0.

4.1. **Proof of Theorem 2.1.** Suppose first that $\mathrm{Mon}(h) = C_p$. Let u be the finite branch point of h. Then, unless one of the following holds:

- $\mathrm{Mon}(g) = C_q$ and u is a ramification point of g – equivalently, $g \circ h$ is linearly equivalent to X^{pq};
- $\mathrm{Mon}(g) = D_q$, $p = 2$, and u is a special point of g – equivalently, $g \circ h$ is linearly equivalent to T_{2q};

squaring the inertia group generator at $g(u)$ yields an element of $x \in C_p^q$, commuting with a certain reflection of D_q (namely, the p-th power of the same inertia group generator), and with $|\mathrm{supp}(x)| \in \{1, 2\}$. If $|\mathrm{supp}(x)| = 1$, we have $\Gamma = C_p^q$. If $|\mathrm{supp}(x)| = 2$, the above commuting implies $x = \mathbf{e}_i + \mathbf{e}_j$ as an element of $\mathbb{F}_p^q$, and thus:

- If p is odd, then by Lemma 3.3, we obtain $\Gamma = C_p^q$.
- If $p = 2$, then by Lemma 3.3, we have $\mathrm{Aug}(C_2^q) \leqslant \Gamma$. However, by Lemma 3.7, $(1, \dots, 1) \in \Gamma \backslash \mathrm{Aug}(C_2^q)$, and hence $\Gamma = C_2^q$.

Suppose next that $\mathrm{Mon}(h) = D_p$ for a prime $p \geqslant 3$. Then, unless $g \circ h$ is linearly equivalent to T_{pq}, the polynomial $g \circ h$ has a branch point, whose the inertia generator, or its square, yields an element of $\Gamma/\mathrm{soc}(\Gamma)$ whose support is of size 1 or 2 or 4, and is invariant under a reflection. In the first case, we have $\Gamma/\mathrm{soc}(\Gamma) = C_2^q$. In the second case, by Lemma 3.3, $\Gamma/\mathrm{soc}(\Gamma)$ contains $\mathrm{Aug}(C_2^q)$. In the third case, $q \geqslant 5$ and by Lemma 3.4, $\Gamma/\mathrm{soc}(\Gamma)$ also contains $\mathrm{Aug}(C_2^q)$. Applying Lemmas 3.8 and 3.10, it follows that $\mathrm{soc}(\Gamma) = C_p^q$. Finally, in the case where $\Gamma/\mathrm{soc}(\Gamma) = \mathrm{Aug}(C_2^q)$, it follows that $\Gamma = \{(a_k)_{k=1}^q \in D_p^q \mid a_1 \cdots a_q \in C_p\}$ [7].

4.2. **Proof of Theorem 2.2.**

4.2.1. *Assume $h = T_p$.* First, as soon as some inertia group generator $c \in \mathrm{Mon}(g \circ h)$ powers to an involution $c^k \in \Gamma$ supported on at most 3 blocks, Lemma 3.6 (applied to the $\mathbb{F}_2[S_4]$ module $\Gamma/(C_p^4 \cap \Gamma)$) yields that $\Gamma/(C_p^4 \cap \Gamma)$ contains the augmentation subgroup. Lemma 3.8(1) and Lemma 3.10a) then allow to conclude $\Gamma \supseteq C_p^4$. The only situations in which the condition $\mathrm{supp}(c^k) \in \{1, 2, 3\}$ is not at least fulfilled for one branch point are the following.

1) When g is the special S_4 polynomial and both branch points of T_p are the preimages of the branch point of g of ramification type $[3, 1]$ (i.e., Case 3b of the theorem; indeed, here the inertia group generator c fulfills that $c^3 \in \Gamma$ has support of size 4).
2) When both branch points of T_p are special points over some branch point of g of ramification type $[2, 1, 1]$.

Moreover, even in the above cases, one necessarily has $\dim(\Gamma \cap C_p^4) \geqslant 3$ by Lemma 3.12 (applied with $n = 4$, $U = \mathrm{Mon}(h)$, $V = \mathrm{Mon}(g)$ and $G = \mathrm{Mon}(g \circ h)$). Note here that the exceptional cases of Lemma 3.12 where $\mathrm{Mon}(g \circ h)$ embeds into $\mathrm{Mon}(g) \times \mathrm{Mon}(h)$, and where $\mathrm{Mon}(g \circ h)/(\Gamma \cap C_p^4) \cong GL_2(3)$ are both impossible; indeed, the former would imply a Ritt move for $g \circ h$ by Proposition 3.14 (whereas a Ritt move involving both T_p and an S_4 polynomial does not exist by Ritt's theorems), and the latter would imply that all 4-cycles of

[7] For $n \geqslant 2$, let $\mathcal{L}_{p,n} = \{(a_k)_{k=1}^n \in D_p^n \mid a_1 \cdots a_q \in C_p\}$. Denote by $D_p^n \times_{C_2} D_p$ the fiber product along the canonical epimorphisms $D_p^n \twoheadrightarrow D_p^n/\mathcal{L}_{p,n} = C_2$ and $D_p \twoheadrightarrow D_p/C_p = C_2$. Then $\mathcal{L}_{p,n+1} \cong D_p^n \times_{C_2} D_p$.

$\mathrm{Mon}(g) \cong S_4$ would lift to order 8 elements modulo $(\Gamma \cap C_p^4)$ (whereas clearly, the fact that the inertia group generator at infinity is a $4p$-cycle shows that this element remains of order 4 modulo $(\Gamma \cap C_p^4)$).

The only remaining task to complete the proof of the theorem for $h = T_p$ is then to show that in Case 2) above, one has $\Gamma \supseteq C_p^4$ as long as the two finite branch points of T_p are special points over two *different* $[2,1,1]$ branch points of g (in particular, g is necessarily the generic S_4 type here), since indeed the case when both lie over the *same* branch point is Case 3c of the theorem. To deal with this remaining case, we use the setup explained in Section 3.5. Namely, letting $\gamma_1, \dots, \gamma_4$ denote the branch points of $g \circ T_p$ and $\pi_1, \dots, \pi_4$ the respective branch cycles, we may assume without loss of generality that projection $\mathrm{Mon}(g \circ T_p) \to \mathrm{Mon}(g) \cong S_4$ yields the tuple $(\overline{\pi_1}, \dots, \overline{\pi_4}) = ((1,2,3,4),(1,2),(1,3),(1,4))$. Exactly two of the points $\gamma_2, \gamma_3, \gamma_4$ are extended by a branch point of T_p. Assume first that γ_2 is extended by a branch point of T_p. Then the triple $(\pi_1, \pi_2, \pi_3\pi_4)$ projects to a triple of ramification type $([4],[2.1^2],[3.1])$ in S_4. Moreover, $\langle \pi_1, \pi_2 \rangle$ is a transitive subgroup of $\mathrm{Mon}(g \circ T_p) \leqslant D_p \wr S_4$, and is the monodromy group of a polynomial $\tilde{f} = \tilde{g} \circ \tilde{h}$, where $\tilde{g}$ is the special S_4 polynomial and $\mathrm{Mon}(\tilde{h}) \leqslant D_p$, see Section 3.5. Since the second inertia group generator is still π_2, this branch point is still extended by a branch point of ramification index 2, whence necessarily $\mathrm{Mon}(\tilde{h}) = D_p$. The other branch point of $\tilde{h}$ of ramification index 2 must necessarily lie over the third branch point of $\tilde{f}$, whose inertia group generator however projects to cycle type $[3,1]$ in S_4. For this configuration, we have however already seen that $\Gamma \supseteq C_p^4$. The same must therefore hold in $\mathrm{Mon}(f)$. If γ_2 is *not* extended by a branch point of T_p, the analogous argument with the triple $(\pi_1, \pi_2\pi_3, \pi_4)$ gives the result. This concludes the case $h = T_p$.

4.2.2. *Assume $h = X^p$.* By Lemma 3.6, one has $\dim(\Gamma \cap C_p^4) \geqslant 3$ as soon as there exists an inertia group generator $c \in \mathrm{Mon}(g \circ X^p)$ powering to an element $c^k \in \Gamma$ with $1 \leqslant |\operatorname{supp}(c^k)| \leqslant 3$. Since the ramification indices at finite branch points of g are all 2 or 3, the latter condition is certainly fulfilled by the inertia group generator at the unique finite branch point of $g \circ X^p$ with ramification index divisible by p, as soon as $p \geqslant 5$. For $p \in \{2,3\}$, all possible configurations could in principle be calculated with Magma, but theoretical arguments are available as well. E.g., for $p = 3$, the only situation in which Lemma 3.6 is not directly applicable arises when the finite branch point $u = 0$ of X^3 is a special point of g lying over a branch point of ramification index 3. This enforces that g is the special S_4 polynomial, and then corresponds to Case 1 of the theorem. For all $p \neq 2$, Lemma 3.7 moreover implies that as soon as $\dim(\Gamma \cap C_p^4) \geqslant 3$, one even as $\Gamma \supseteq C_p^4$, due to the containment of both the augmentation subgroup $\mathrm{Aug}(C_p^4)$ and the diagonal submodule $\mathrm{diag}(C_p^4)$.

We are thus left with $h = X^2$. Let c be the inertia group generator at the branch point $g(0)$ of $g \circ X^2$, and again let k be the smallest natural number such that $c^k \in \Gamma$. If $\operatorname{supp}(c^k) \in \{1,2,3\}$, then once again $\Gamma \supseteq \mathrm{Aug}(C_2^4) \cong C_2^3$ by Lemma 3.6; and if $\operatorname{supp}(c^k) \in \{1,3\}$, then even $\Gamma = C_2^4$ (since c^k is then an odd permutation, i.e., not contained in $\mathrm{Aug}(C_2^4)$). The only cases left to consider are therefore when the branch point 0 of $h = X^2$ extends a branch point of g of ramification type $[2,1,1]$ (since indeed $c^k = 1$ in case 0 is a special point, and $\operatorname{supp}(c^k) = 2$ in case 0 is the ramification point over this $[2,1,1]$-branch point). If g is the generic type S_4 polynomial, a coalescing argument similar to the one carried out above reduces to the situation $\tilde{f} = \tilde{g} \circ X^2$ where $\tilde{g}$ is the special S_4 polynomial and the branch point 0 of X^2 extends the $[3,1]$-branch point of $\tilde{g}$; here we already know $\Gamma = C_2^4$. There remains the case in which g is special and 0 extends the unique $[2,1,1]$ branch point of G. The case where 0 is a special point corresponds to Case 2 of the theorem, and the monodromy group can directly be

checked to equal $\mathrm{GL}_2(3)$ with Magma. The case where 0 is a ramification point corresponds to Case 3a of the theorem, and Lemma 3.6 yields $\Gamma \supseteq \mathrm{Aug}(C_2^4)$.

4.3. **Proof of Theorem 2.3.** Note first that, in order to prove $\Gamma = S_4^p$, it suffices to prove $\Gamma/(\Gamma \cap A_4^p) = C_2^p$. Indeed, due to Lemma 3.8(1) and Lemma 3.10(a), the latter condition implies $\Gamma/(\Gamma \cap V_4^p) = S_3^p$; and analogously, this condition, due to Lemma 3.8(2) and Lemma 3.10(a), implies $\Gamma \supseteq V_4^p$.

Note furthermore that h has at least one branch point $u \in k$ whose inertia group is generated by a transposition in $\mathrm{Mon}(h)$. Let $c \in \mathrm{Mon}(X^p \circ h)$ (resp., $\mathrm{Mon}(T_p \circ h)$) be the inertia group generator at u^p (resp., at $T_p(u)$), and let $k \in \mathbb{N}$ be minimal such that c^k is contained in Γ and of order $\leqslant 2$. We know that $\Gamma/(\Gamma \cap A_4^p) = C_2^p$ and hence $\Gamma = S_4^p$ as soon as c^k is a transposition. If furthermore $p > 2$, then $\Gamma/(\Gamma \cap A_4^p) = C_2^p$ and hence $\Gamma = S_4^p$ follows also as soon as c^k is a double transposition supported on two blocks, since indeed then $\Gamma/(\Gamma \cap A_4^p)$ contains $\mathrm{Aug}(C_2^p)$, but also contains the diagonal, which is generated by the p-th power of the inertia group generator at ∞. This leaves us with only the following cases to consider:

Case 1. $p \geqslant 3$, $g = X^p$. In this case the only situations left to consider are where either no transposition branch point of h lies over a non-branch point of g, or (all) three such points lie over the same non-branch point of g.

Case 1.1. The former case is only possible when h is special and the transposition branch point u of h equals the ramification point $u = 0$ of g. Since in this case, the unique branch point of h of ramification type $[3, 1]$ lies over a non-branch point of X^p, the respective inertia group generator is an element of $\Gamma \cap A_4^p$ supported on only one block, from which it follows that $\Gamma \supseteq A_4^p$. This concludes (the case $p \geqslant 3$ of) Case 2a of the theorem.

Case 1.2. The latter case implies that h is generic with three transposition branch points u, v, w fulfilling $u^p = v^p = w^p$. For $p = 3$, one may verify directly that one gets monodromy group $S_4 \times C_3$, corresponding to the "Ritt move" Case 1 of the theorem. Assume from now on $p \geqslant 5$. Here, since we have an inertia group generator $c \in \Gamma$ which is a triple transposition supported on exactly three blocks, it follows from Lemma 3.8(1) (applied with the quotient $\Gamma/(\Gamma \cap V_4^p) \leqslant S_3^p$ in the role of K) and Lemma 3.10b) that $C_3^p \leqslant \Gamma$ and hence $A_4^p \leqslant \Gamma$.[8] This concludes Case 2c of the theorem.

Case 2. $p = 2$, i.e., $g = X^2$; and moreover no inertia group generator of $g \circ h$ powers to a transposition. This is only possible if one branch point u of h with transposition inertia is the ramification point $u = 0$ of g; and moreover h is either the special S_4-polynomial, or h is generic with two more finite branch points v, w mapping to the same point under $g = X^2$. In both cases, the group structure can be verified directly with Magma. The former case behaves as the case $p \geqslant 3$, and together with it forms Case 2a of the theorem, whereas the latter case is Case 2f of the theorem.

Case 3. $p \geqslant 3$, $g = T_p$. In this case, we can additionally use Lemma 3.4, which yields that $\Gamma/(\Gamma \cap A_4^p) \supseteq \mathrm{Aug}(C_2^p)$ (and hence $\Gamma = S_4^p$ by the same argument as at the beginning of the proof) as soon as Γ contains a quadruple transposition supported on four blocks which are invariant as a set under a suitable reflection of D_p. We distinguish further between the case "h special" and "h generic".

[8] Note that there are indeed cases here where $[S_4^p : \Gamma]$ is arbitrarily large. E.g., whenever $p = 2^q - 1$ is a Mersenne prime, suitable choice of the preimages of u^p lead to the projection of the corresponding inertia group generator to $S_4^p/A_4^p = C_2^p$ generating the (cyclic!) binary Hamming code of length $2^q - 1$, which has dimension $2^q - q - 1$. Suitable choice of branch points therefore leads to a case with $[S_4^p : \Gamma] = 2^q$.

Case 3.1. h special. Here the only case left to consider is when the unique transposition branch point u of h is a special point of T_p (i.e., $u = \pm 2$). In this case, the branch point of h of ramification type $[3,1]$ is either an unramified point of T_p, or a ramification point of ramification index 2; if $c \in \mathrm{Mon}(T_p \circ h)$ denotes the respective inertia group generator, it follows in both cases that $c^2 \in \Gamma \cap A_4^p$ is an element of order 3 supported on at most two blocks. By Lemma 3.2, this implies that the $\mathbb{F}_3[C_p]$ module $(\Gamma \cap A_4^p)/(\Gamma \cap V_4^p)$ contains $\mathrm{Aug}(C_3^p)$. By Lemma 3.8(2) and Lemma 3.10a), one has $V_4^p \supseteq \Gamma$. This concludes Case 2b of the theorem.

Case 3.2. h is generic. Here the only cases left to consider are the following:

Case 3.2.1. In case at least one of the three finite branch points u, v, w of h lies over a non-branch point of T_p, all three of them must lie over the same non-branch point, i.e., $T_p(u) = T_p(v) = T_p(w) \notin \{\pm 2\}$. For $p = 3$, the group structure may again be directly verified with Magma, yielding Case 2e of the theorem. Hence, assume $p \geqslant 5$. Here, it follows from Corollary 3.5 that $\Gamma/(A_4^p \cap \Gamma) = C_2^p$.

Case 3.2.2. In case all of u, v, w lie over branch points of T_p, two of them (without loss u, v must be ramification points over the same branch point of T_p. If, however, w is not also a ramification point over the same branch point, then the respective inertia group generator $c \in \mathrm{Mon}(T_p \circ h)$ fulfills that $c^2 \in \Gamma$ is an involution supported on exactly four blocks, invariant as a set under a reflection of D_p (namely the projection of c to D_p). As remarked above, this case would yield $\Gamma = S_4^p$, so that we are after all left with the case that all of u, v, w are ramification points over the same branch point of T_p (i.e., Case 2d of the theorem). In this case, $c^2 \in \Gamma$ is an involution whose support is of size $6 < p$. It then follows from Lemma 3.8(1) (applied with the quotient $\Gamma/(\Gamma \cap V_4^p) \leqslant S_3^p$ in the role of K) and Lemma 3.10b) that $\Gamma \supseteq A_4^p$.

4.4. **Proof of Theorem 2.4.** Since h has at most three finite branch points (all of ramification index 2 or 3), it follows that, if there is at least one branch point of $g \circ h$ which is a non branch point of g, then either $\Gamma/(\Gamma \cap A_4^4)$ contains an involution (namely, the third power of an inertia group generator) of support $\leqslant 2$, or $\Gamma \cap A_4^4$ contains an element of order 3 and support 1. From this, it follows quickly that $\Gamma \supseteq A_4^4$, whence we may restrict to the case that every branch point of $g \circ h$ is a branch point of g, and in particular $g \circ h$ has at most four branch points.

Now the assertion is most conveniently checked using a direct Magma search for genus zero 3- and 4-tuples inside $S_4 \wr S_4 \leqslant S_{16}$.

5. Nonsolvable case: proofs of Theorems 2.5, 2.6, and 2.7

Let k be an algebraically closed field of characteristic 0.

In the following, we call an indecomposable polynomial $g \in k[X]$ (as well as its monodromy group $\mathrm{Mon}(g)$) *exceptional*, if its monodromy group is nonsolvable, but does not contain the alternating group. Recall that exceptional indecomposable polynomials are known due to [Mül95], and their monodromy groups belong to a short finite list, cf. Proposition 3.1.

5.1. **Proof of Theorem 2.5.** This follows from [KNR24, Corollary 4.4], except in the case when there is a Ritt move for $g \circ h$, in which case necessarily $h = X^p$ up to linear equivalence, by Ritt's theorems. Finally, the assertion $\mathrm{Mon}(g \circ h) \cong \mathrm{Mon}(g) \times \mathrm{Mon}(h)$ for the latter case follows directly from Proposition 3.13.

5.2. **Proof of Theorem 2.6.** Set $n := \deg(g)$.

5.2.1. *Assume* $\mathrm{Mon}(g) = S_n$ *or* $\mathrm{Mon}(g) = A_n$. The case where there is a Ritt move for $g \circ h$ is covered by Theorem 2.5. In the following, we may assume there is no Ritt move for $g \circ h$. Assume that Γ does not contain a subgroup C_p^{n-1}. Then by Lemma 3.12, either $(p, n) = (3, 6)$ or $\mathrm{Mon}(g \circ h)$ embeds into $\mathrm{Mon}(h) \times \mathrm{Mon}(g)$. The former case can in fact be excluded since the nonsplit extension $3.S_6 \leqslant S_{18}$ does not contain an 18-cycle, and hence cannot be the monodromy group of a polynomial.

Since we have however excluded the existence of a Ritt move, Proposition 3.14 yields $p = 3$, $h = X^3$ and $\mathrm{Mon}(g) \cong A_5$ as the only possibility; cf. Table 1.

5.2.2. *Assume* $\mathrm{Mon}(g)$ *is exceptional.* Assume first that $h = X^p$. Since the list of polynomial ramification type of exceptional nonsolvable monodromy groups is known explicitly (cf. [Mül95]), the verification for $p = 2, 3$ amounts to a Magma calculation (going through genus-0 tuples of elements in $C_p \wr \mathrm{Mon}(g)$ projecting onto one of the possible tuples in $\mathrm{Mon}(g)$, and keeping note of the subgroups generated by such tuples). Assume therefore $p \geqslant 5$. The precise list of exceptional nonsolvable ramification types (in particular, the fact that, for all exceptional polynomial monodromy tuples, the ramification indices at any finite branch points have only the prime divisors 2 and 3) quickly yields an element of order p in $\ker(\mathrm{Mon}(g \circ h) \to \mathrm{Mon}(g))$ whose support (as an element of C_p^n is strictly smaller than $\{1, \dots, n\}$, namely an appropriate power of the unique inertia group generator at a finite branch point of $g \circ h$ with ramification index divisible by p. But by [Mor80], for $p \geqslant 5$, the only nontrivial submodules of the $\mathbb{F}_p$ permutation module of the simple group $\mathrm{soc}(\mathrm{Mon}(g))$ are the diagonal and augmentation. Since we have already identified a nondiagonal element of order p, we obtain that $\ker(\mathrm{Mon}(g \circ h) \to \mathrm{Mon}(g))$ contains augmentation, as claimed.

Assume now that $h = T_p$, $p \geqslant 3$. The case $p = 3$ can be dealt with by direct Magma computation, see the proof of Theorem 2.7, and yields exactly one exceptional monodromy group $\mathrm{Mon}(g \circ h) = 39\mathrm{T}248$ (with $\mathrm{Mon}(g) = PSL_3(3)$ and further specifications as given in Table 1). Therefore, let $p \geqslant 5$ from now on. Assume that g is such that $|\Gamma \cap C_p^n| < p^{n-1}$. In particular $|\Gamma/(\Gamma \cap C_p^n)| \leqslant 2$ by Lemma 3.8(1) and Lemma 3.10b), since Γ is invariant under the primitive group $\mathrm{Mon}(g)$. Now consider the group $\tilde{G} := \mathrm{Mon}(g \circ h)/(\Gamma \cap C_p^n) \leqslant C_2 \wr \mathrm{Mon}(g)$. This is the monodromy group of $g \circ \psi$, where ψ is the degree-2 rational function[9] parameterizing the unique quadratic subextension of the splitting field of $T_p(X) - t$. Set $\tilde{\Gamma} := \ker(\tilde{G} \to \mathrm{Mon}(g))(= \Gamma/(\Gamma \cap C_p^n))$. A Magma computation,[10] using the list of exceptional ramification types from [Mül95], now yields the following intermediate result:

Whenever $|\tilde{\Gamma}| = 2$, the extension $\tilde{\Gamma}.\mathrm{Mon}(g)$ is split.

In total, we have therefore reduced to the case that the extension $\tilde{\Gamma}.\mathrm{Mon}(g)$ is split. This means that $\Gamma \cap C_p^n$ becomes a submodule of a module $Ind_H^{\mathrm{Mon}(g)}\chi$ where $H \leqslant \mathrm{Mon}(g)$ is a point stabilizer and χ is either the trivial character or a quadratic character of H, cf. Section 3.3.1. In the former case, $Ind_H^{\mathrm{Mon}(g)}\chi$ is the permutation module, and since $p \geqslant 5$, it follows from [Mor80] that $\dim(\Gamma \cap C_p^n) \in \{1, n-1, n\}$. The same assertion for quadratic χ may be verified directly with Magma, namely by explicitly constructing and decomposing the induced modules for all $5 \leqslant p \mid |\mathrm{Mon}(g)|$, and by computing the corresponding complex characters to deal with $p \nmid |\mathrm{Mon}(g)|$. To conclude the proof, we therefore only need to exclude the case $|\Gamma \cap C_p^n| = p$. In that case, Γ is diagonal, i.e., $\Gamma = D_p$ or $\Gamma = C_p$.

[9] Namely, ramified exactly at the two finite branch points ± 2 of T_p, and unramified at ∞.

[10] One may assume for the computation that the set of branch points of $g \circ \psi$ is the same as that of g, since putting one or two branch points of ψ over a non-branch point of g results in an element of $\tilde{\Gamma}$ with support of size 1 or 2, yielding $|\tilde{\Gamma}| \geqslant 2^{n-1}$, as seen many times before in analogous situations.

We therefore either have a) $\mathrm{Mon}(f) = C_p.(C_2.\mathrm{Mon}(g))$, where the central subgroup C_2 of $C_2.\mathrm{Mon}(g)$ acts nontrivially on C_p; or b) $\mathrm{Mon}(f) = C_p.\mathrm{Mon}(g)$, where the image of $\mathrm{Mon}(g) \to \mathrm{Aut}(C_p)$ contains C_2 (i.e., $\mathrm{Mon}(g)$ has an index-2 normal subgroup N whose quotient acts diagonally on C_p and on N). We claim that in both cases, $\mathrm{Mon}(f) \leqslant D_p \times \mathrm{Mon}(g)$, from which Proposition 3.14 implies that $g \circ T_p$ admits a Ritt move. The latter is however impossible by Ritt's theorems.

To prove the claim and conclude the proof, note in a) that the fact that $\ker(C_2.\mathrm{Mon}(g) \to \mathrm{Aut}(C_p))$ does not contain the central subgroup C_2 enforces the extension $C_2.\mathrm{Mon}(g)$ to split, i.e., $\mathrm{Mon}(f) = C_p.(C_2 \times \mathrm{Mon}(g))$, where moreover the central[11] extension $C_p.\mathrm{Mon}(g)$ is also split (indeed, for none of the simple groups $\mathrm{soc}(\mathrm{Mon}(g))$, the Schur multiplier has a prime divisor $p > 3$). This gives $\mathrm{Mon}(f) = D_p \times \mathrm{Mon}(g)$. Similarly, in b), we obtain $\mathrm{Mon}(f) = C_p \rtimes \mathrm{Mon}(g)$, with $\mathrm{Mon}(g)$ acting on C_p (trivially or) via $C_2 \leqslant \mathrm{Aut}(C_p)$. In this last case, there is an index-2 normal subgroup $N \leqslant \mathrm{Mon}(g)$ such that $\mathrm{Mon}(f) = (C_p \times N).C_2$, with the outer C_2 acting diagonally on C_p and N, clearly yielding an embedding into $D_p \times \mathrm{Mon}(g)$. This concludes the proof.

5.3. **Proof of Theorem 2.7.** We begin by noting that the cubic subextension of the Galois closure of $h(X) - t$, with an S_4-polynomial h, is always given by $\varphi(x) - t$ with a rational function φ; namely of ramification type $([3], [2.1], [2.1])$ for the special S_4-polynomial h, and of ramification type $([2.1], [2.1], [2.1], [2.1])$ for the generic S_4-polynomial; indeed, this follows instantly from the projection $S_4 \to S_4/V_4 \cong S_3$. We now consider the quotient of $\mathrm{Mon}(g \circ h)$ by the normal subgroup $V_4^{\mathrm{Mon}(g)} \cap \Gamma$. This is the monodromy group of $g \circ \varphi$, with a rational function $\varphi \in k(x)$ as above.

First, assume $\mathrm{Mon}(g) \in \{A_n, S_n\}$, $n = \deg(g)$. Via noting that the exceptional case $\mathrm{Mon}(g \circ \varphi) \leqslant 3.S_6$ of Lemma 3.12 cannot occur (e.g., since in the nonsplit extension $3.S_6 \leqslant S_{18}$ the 6-cycles of S_6 do not lift to elements of order 12, which would however have to be the case for the inertia group generator at infinity), it follows from Lemma 3.12 that either $\ker(\mathrm{Mon}(g \circ \varphi) \to \mathrm{Mon}(g)) \supseteq C_3^{n-1}$ (in which case there is nothing to prove), or $\mathrm{Mon}(g \circ \phi) \leqslant \mathrm{Mon}(g) \times S_3$. Proposition 3.14 (with Remark 3.15b), since φ is not a polynomial[12]) now implies that $g \circ \varphi$ has a non-unique decomposition, i.e., $g \circ \varphi = \tilde{\varphi} \circ \tilde{g}$, for some degree-3 function $\tilde{\varphi}$. Note that $g \circ \varphi$ is equivalent to a Laurent polynomial, meaning that there are only two poles. It now can either be verified directly (considering ramification at infinity), or by invoking [Pak09, Theorem 1.1] that a Laurent polynomial with a non-unique decomposition cannot be the composition of functions with S_3- and nonsolvable monodromy.

Next assume that $\mathrm{Mon}(g)$ is exceptional. This case can in principle be dealt with by exhaustive computation inside the wreath products $S_4 \wr \mathrm{Mon}(g)$, since $\deg(g \circ h)$ is absolutely bounded by $31 \cdot 4$; however, brute force computations inside the larger degree groups seem difficult, and we therefore give some useful simplifications. Again, consider the 3-part $\tilde{\Gamma}$ of $\ker(\mathrm{Mon}(g \circ \varphi) \to \mathrm{Mon}(g))$ as above. For the exceptional g with $\deg(g) > 15$, i.e., $\mathrm{Mon}(g) \in \{P\Gamma L_3(4), M_{23}, PSL_5(2)\}$, all extensions $C_2^k.\mathrm{Mon}(g) \leqslant C_2 \wr \mathrm{Mon}(g)$ are split, whence $\tilde{\Gamma}$ becomes an $\mathbb{F}_3[\mathrm{Mon}(g)]$-module, and in particular a submodule of the permutation module under

[11] Note that $\mathrm{Mon}(g)$ acts trivially on C_p (hence, "central extension"). Indeed, due to the embedding $\mathrm{Mon}(f) \leqslant D_p \wr \mathrm{Mon}(g)$, the block stabilizer acts on a block (and hence on the whole p-part of the kernel due to diagonality) as $C_2 \leqslant \mathrm{Aut}(C_p)$; since the center C_2 of $C_2.\mathrm{Mon}(g)$ does act nontrivially, the kernel of the action of $C_2.\mathrm{Mon}(g)$ on C_p must be a normal subgroup of $\mathrm{Mon}(g)$ containing the point stabilizer in $\mathrm{Mon}(g)$, i.e., must be all of $\mathrm{Mon}(g)$.

[12] The one exceptional case $G = 15T21$ from Remark 3.15 can be excluded ad hoc; e.g., this group has no element of cycle structure [10.5], which would however be needed as the inertia group generator at infinity.

the simple group $\mathrm{soc}(\mathrm{Mon}(g))$. But due to [Mor80], either $|\tilde{\Gamma}| \geqslant 3^{\deg(g)-1}$ or $|\tilde{\Gamma}| = 3$. We therefore only need to deal with the case of a diagonal extension $\mathrm{Mon}(g\circ\varphi) = S_3.\mathrm{Mon}(g) \leqslant S_{3\deg(g)}$. In all cases, the only such group is the direct product, with a nonunique decomposition, which is impossible, as in the case $\mathrm{Mon}(g) = A_n, S_n$.

For $\deg(g) \leqslant 15$, the group $\mathrm{Mon}(g\circ\varphi)$ is in the realm of Magma's transitive group database, and we can directly search for cases of transitive subgroups of $S_3 \wr \mathrm{Mon}(g)$ projecting onto $\mathrm{Mon}(g)$ and with block kernel acting on a block as S_3 such that there is (no Ritt move, i.e.) a unique maximal block system and such that $|\tilde{\Gamma}| < 3^{\deg(g)-1}$. This yields exactly the candidate groups $\texttt{TransitiveGroup}(k, j)$ for

$$(k, j) \in \{(39, 134), (39, 206), (39, 218), (39, 248), (33, 60), (33, 69), (33, 83), (33, 97), (30, 1650), (30, 2251)\},$$

and now inside these a direct search for generating genus zero tuples leaves only $39T206$, $39T248$ (both with $\mathrm{Mon}(g) = PSL_3(3)$) and $33T60$ (with $\mathrm{Mon}(g) = PSL_2(11)$). Since in all cases, the 3-part of Γ is of order > 3 and Γ is invariant under the primitive group $\mathrm{Mon}(g)$, it follows from Lemma 3.8(2) with Lemma 3.10b) that $\Gamma \supseteq V_4^{\mathrm{Mon}(g)}$.

6. Higher compositions

6.1. **Some sample results on composition of three and more indecomposables.** Let k be an algebraically closed field of characteristic 0. In this section we demonstrate some ways in which the results and techniques of this paper can be used to obtain lower bounds for kernels also in case of composition of more than two indecomposable polynomials. The most straightforward conclusion of this form is possible in the setting of Theorem 2.5, in which the indecomposability of g is indeed not necessary to obtain the large kernel conclusion (in the absence of a Ritt move for $f = g \circ h$), see [KNR24, Corollary 4.4]. Below are some additional considerations.

The below sample result is concerned with compositions involving not necessarily indecomposable Chebyshev polynomials.

As defined in Section 3.3, for $m \geqslant 2$ and even $n \geqslant 2$, we let

$$\mathrm{Aug}^-(C_m^n) = \{(a_1, \dots, a_n) \in C_m^n \mid a_1 a_2^{-1} \cdots a_{n-1} a_n^{-1} = 1\}.$$

Proposition 6.1. Suppose $g = T_q$ and $h = \ell \circ X^p$, with an integer $q \geqslant 3$, a prime $p \geqslant 2$ and a linear polynomial $\ell = aX + b$. Let $G = \mathrm{Mon}(g \circ h)$ and $\Gamma = \ker(G \to \mathrm{Mon}(g))$. Then $\Gamma = C_p^q$, unless one of the following cases occurs:

1. $p = 2$ and $b = \pm 2$, in which case $\Gamma = \mathrm{diag}(C_2^q)$.
2. $b = \zeta_{2q}^i + \zeta_{2q}^{-i}$ for some $i \in (\mathbb{Z}/q\mathbb{Z})\backslash\{0\}$, in which case

$$\Gamma = \begin{cases} \left(\mathrm{Aug}^-(C_p^{o(i)})\right)^{\frac{q}{o(i)}} & \text{if } o(i) \text{ is even,} \\ C_2^{q-\frac{q}{o(i)}+1} & \text{if } p = 2 \text{ and } o(i) \text{ is odd.} \end{cases}$$

(Here, $o(i)$ denotes the additive order of $i \in \mathbb{Z}/q\mathbb{Z}$.)

Proof. Let $f = g\circ h$. Denote by Ω the splitting field of $f(X)-t$ over $k(t)$, and by $c_1, \dots, c_r \in G$ the branch cycles. Begin by noting that, since the fixed field L of Γ is of genus zero, the Galois group $\Gamma = \mathrm{Gal}(\Omega/L)$ is generated by the inertia group generators at ramified places in Ω/L, i.e., it is the normal closure in G of $\{\langle c_1\rangle \cap \Gamma, \dots, \langle c_r\rangle \cap \Gamma\}$. Here, the group $\langle c_j\rangle \cap \Gamma$ can only be nontrivial when some ramification point of g at the respective branch point is a branch point (of ramification index p) of h. This happens of course for the inertia group at infinity

(where $\langle c_j\rangle \cap \Gamma$ is the diagonal, which is normal in G), and for at most one further index i. Write $c := c_j$ for this index j. There are the following three possibilities:

i) If $|\operatorname{supp}(\langle c\rangle \cap \Gamma)| = 1$, whence necessarily $\Gamma = C_p^q$. This happens whenever the finite branch point b of h extends a non-branch point of g, or when $p > 2$ and the finite branch point of h is a special point over a branch point of g.

ii) If $p = 2$ and the finite branch point b of h is a special point of g, then f is of ramification type $(2q, 2, 2)$, i.e., $G \cong D_{2q}$. This is Case 1 of the proposition.

iii) The only other possibility is that b is a ramification point (necessarily of ramification index 2) of g. These points are well known to be $\zeta_{2q}^i + \zeta_{2q}^{-i}$, $i = 1, \dots, q-1$ (so that we are in Case 2), where moreover the transposition corresponding to this ramification point (among the cycles of the inertia group generator $\gamma \in D_q$) may be assumed of the form $(j, j+i) \pmod q$ for some j. Moreover the generator c^k of $\langle c\rangle \cap \Gamma$ commutes with γ (acting on the permutation module $\mathbb{F}_p^q$). Therefore, $c^k = \mathbf{e}_j + \mathbf{e}_{j+i}$ and the normal closure $\langle D_q{\cdot}c^k\rangle$ of c^k in G equals $\langle C_q{\cdot}c^k\rangle$. By Lemma 3.3, we have

$$\langle C_q \cdot c^k\rangle = \begin{cases} \left(\operatorname{Aug}(C_2^{o(i)})\right)^{\frac{q}{o(i)}}, & \text{if } p = 2, \\ \left(\operatorname{Aug}^-(C_p^{o(i)})\right)^{\frac{q}{o(i)}}, & \text{if } p \geqslant 3 \text{ and } o(i) \text{ is even}, \\ \mathbb{F}_p^q, & \text{otherwise} \end{cases}.$$

(Note that of course for $p = 2$ and $o(i)$ even, our definitions of $\operatorname{Aug}(C_2^{o(i)})$ and $\operatorname{Aug}^-(C_2^{o(i)})$ coincide.) To determine Γ, it then only remains to verify whether the diagonal is already contained in the above. Clearly, this is true in the last case, as well as whenever $o(i)$ is even, so that we are reduced to $p = 2$ and $o(i)$ odd. Here, $\operatorname{Aug}(C_2^{o(i)})$ clearly does not contain the diagonal, yielding that $\dim(\Gamma) = \dim(\langle D_q{\cdot}c^k\rangle) + 1$, thus completing the proof.

□

Remark 6.2. Suppose $g = T_q$ and $h = \ell \circ X^p$, with $q \geqslant 3$, and with $p \geqslant 2$ prime. If $p = 2$, furthermore assume that $g \circ h$ is not linearly related to T_{2q}. Let $\Gamma = \ker(\operatorname{Mon}(g\circ h) \to \operatorname{Mon}(g))$ Then the following hold.

(1) If q is an odd prime, then $\Gamma = C_p^q$.
(2) If q is an odd composite integer, then Γ contains $C_p^{q-q/r+1}$, where r is the smallest prime divisor of q.
(3) If $q = 2r$ with r prime then Γ contains C_p^{q-1} unless $g \circ h \sim T_q \circ X^p = T_r \circ (X^{2p} - 2)$.
(4) If $q = 2^m$ with $m \geqslant 2$ and $p = 2$, then Γ contains $C_2^{2^{m-1}}$.

Suppose $g = X^q$ and $h = \ell \circ X^p$. Unless $g \circ h$ is linearly related to X^{pq}, we have $\Gamma = C_p^q$.

Proof. The case $g = T_q$ follows immediately from Proposition 6.1. The case $g = X^q$ follows in the same way as in the proof of Proposition 2.1. □

The following theorem shows that arbitrarily long compositions of polynomials linearly equivalent to Chebyshev polynomials always have large kernel in the absence of Ritt moves.

Theorem 6.3. *Let $f_1, \dots, f_r \in k[X]$ be polynomials of odd prime degrees $p_1, \dots, p_r$, $r \geqslant 2$, with $\operatorname{Mon}^{-}_{k}(f_i) = D_{p_i}$, $i = 1, \dots, r$, and such that $f_i \circ f_{i+1} \not\sim T_{p_i p_{i+1}}$ for all $i = 1, \dots, r-1$. Set $h = f_1 \circ \cdots \circ f_{r-1}$, $f = h \circ f_r$, and $\Gamma = \ker(\operatorname{Mon}(f) \to \operatorname{Mon}(h))$. Then the following hold:*

a) $\Gamma \supseteq C_{p_r}^{\deg(h)}$.

b) $\Gamma/C_{p^r}^{\deg(h)} \supseteq C_2^{\deg(h)\cdot(1-\frac{1}{p_{r-1}})}$.

Proof. By induction over r. Obviously it suffices to prove the assertion for algebraically closed fields $k = \overline{k}$. The case $r = 2$ follows from Theorem 2.1. Assume that the assertion holds for $r - 1 \geqslant 2$. In order to control the p_r-part of Γ, we first estimate the 2-part. For this, let $K = \Gamma \cap C_{p_r}^{\deg(h)}$, $N = \ker(\mathrm{Mon}(f) \to \mathrm{Mon}(f_1 \circ \cdots \circ f_{r-2}))$ and $G := \mathrm{Mon}(f)/K$. Then $G = \mathrm{Mon}(f_1 \circ \cdots \circ f_{r-1} \circ \varphi_r)$, where $\varphi_r \in k(X)$ denotes the quadratic rational function parameterizing the unique quadratic subextension of the Galois closure of $f_r(X) - t$. In particular, G embeds into $H \wr \mathrm{Mon}(f_1 \circ \cdots \circ f_{r-2})$, where $H := \mathrm{Mon}(f_{r-1} \circ \varphi_r)$.

By Theorem 2.1, we have $\mathrm{Aug}(C_2^{p_{r-1}}).D_{p_{r-1}} \leqslant H \leqslant C_2 \wr D_{p_r}$. We next claim that the image $\tilde{H}$ of the blocks kernel $\tilde{\Gamma} := \ker(\mathrm{Mon}(f_1 \circ \cdots \circ \varphi_r) \to \mathrm{Mon}(f_1 \circ \cdots \circ f_{r-2})) \cong N/K$ under projection to any of the $(\deg(f_1 \circ \cdots \circ f_{r-2}))$ blocks still contains $\mathrm{Aug}(C_2^{p_{r-1}})$. For this, note that $\tilde{H}$ is a normal subgroup of H and contains an element of order p_r as is evident from ramification over infinity. But then $\tilde{H}$ contains the normal closure a p_r-Sylow group of H, i.e., contains all its elements of order p_r. Since $\mathrm{Aug}(C_2^{p_{r-1}}).C_{p_r} = (C_2 \wr C_{p_r}) \cap \mathrm{Alt}(2p_r)$ has no element of order $2p_r$, all elements in $\mathrm{Aug}(C_2^{p_{r-1}}).C_{p_r}$ outside of $\mathrm{Aug}(C_2^{p_{r-1}})$ are of order p_r, whence $\tilde{H} \supseteq \mathrm{Aug}(C_2^{p_{r-1}}).C_{p_r}$, showing the claim.

We will now choose a setup allowing us to invoke Lemma 3.9. Let $\widehat{\sigma}$ be a generator of a cyclic transitive subgroup in $\mathrm{Mon}(f_1 \circ \cdots \circ f_{r-2})$ (e.g., an inertia group generator at infinity), and σ a preimage of $\widehat{\sigma}$ in G. Set $\tilde{G} := \langle \tilde{\Gamma}, \sigma \rangle$. Then $\tilde{G} \leqslant \tilde{H} \wr C_d$ (for $d := \deg(f_2 \circ \cdots \circ f_{r-2})$), and $\tilde{\Gamma}$ is still the blocks kernel in $\tilde{G}$. Moreover, there is a natural map $\rho : \tilde{\Gamma} \to D_{p_{r-1}}^d$ whose image equals the kernel $\ker(\mathrm{Mon}(f_1 \circ \cdots \circ f_{r-1}) \to \mathrm{Mon}(f_1 \circ \cdots \circ f_{r-2}))$. By the induction hypothesis, $\rho(\tilde{\Gamma})$ contains $C_{p_{r-1}}^d$. Also note that $\mathrm{Aug}(C_2^{p_{r-1}})$ is of course a direct sum of faithful irreducible modules, since the only nontrivial normal subgroup $C_{p_{r-1}} \leqslant D_{p_{r-1}}$ acts faithfully on each nondiagonal submodule of $C_2^{p_{r-1}}$. Now, applying Lemma 3.9 (to $\tilde{G}$, $\tilde{\Gamma}$, $\tilde{H}$ etc.), gives $\mathrm{Aug}(C_2^{p_{r-1}})^d \subseteq \ker(\rho) = \ker(\mathrm{Mon}(h \circ \varphi_r) \to \mathrm{Mon}(h)) = \Gamma/(\Gamma \cap C_{p^r})$, which gives the order of the 2-part asserted in b).

From this, a) will follow by yet another application of Lemma 3.9: this time, take more simply $\tilde{\Gamma} = \Gamma$ and $\tilde{G} = \langle \Gamma, \sigma \rangle$ for a cyclic transitive subgroup $\langle \sigma \rangle$ of $\mathrm{Mon}(f)$. Then $\tilde{G} \leqslant D_{p_r} \wr C_{d'}$ for $d' := \deg(h)$. Setting $\rho : D_{p_r}^d \to C_2^{d'}$, we note that we have just shown $\rho(D_{p^r}^{d'})$ to contain $\mathrm{Aug}(C_2^{p_{r-1}})^{d'/p_{r-1}}$. Since $p_{r-1} \geqslant 3$, the group $\mathrm{Aug}(C_2^{p_{r-1}})$ contains two elements whose supports have just one element in common. The same then of course holds for $\mathrm{Aug}(C_2^{p_{r-1}})^{d'/p_{r-1}}$. Hence, Lemma 3.9 applies with the faithful $\mathbb{F}_p[C_2]$-module C_p, yielding $\Gamma \supseteq C_{p^r}^{\deg(h)}$, as asserted in a). □

6.2. **An application to arithmetic dynamics.** Let k be a field of characteristic 0. Theorem 6.3 has an immediate consequence for dynamical monodromy groups $\varprojlim_n \mathrm{Mon}(f^n)$ of polynomials of prime degree. Recall that such f are either AGL_1-polynomials or have almost simple monodromy group, with a "large kernel" conclusion for the latter case already having been obtained in [KNR24, Corollary 4.5]. Corollary 6.4 below extends this by taking care of the case of polynomials f linearly related (over $\overline{k}$) to T_p. To state it, write $[G]^n$ for the n-fold wreath product of G with itself, $[G]^\infty = \varprojlim_n [G]^n$, and recall that for profinite groups $G \leqslant H \leqslant [S_d]^\infty$, the *relative Hausdorff dimension* of G in H is

$$\mathcal{H}_H(G) := \liminf_{n\to\infty} \frac{\log|\pi_n(G)|}{\log|\pi_n(H)|},$$

where $\pi_n(G)$ is the image of G under projection to $[S_d]^n$.

Corollary 6.4. Let $f \in k[X]$ be a polynomial of odd prime degree p such that f is linearly related, but not conjugate[13] over $\overline{k}$, to $\pm T_p$. Then $G := \mathrm{Mon}_{\overline{k}}(f^\infty) := \varprojlim_n \mathrm{Mon}(f^n)$ contains $[C_p]^\infty$, the infinite iterated wreath product of groups C_p. Moreover, the relative Hausdorff dimension of G in $H := [D_p]^\infty$ is

$$\mathcal{H}_H(G) \geqslant 1 - \frac{\log_p(2)}{p(1+\log_p(2))}.$$

Proof. By assumption, $\mathrm{Mon}_{\overline{k}}(f) = D_p$. Since f is not conjugate to $\pm T_p$, $f \circ f$ is not linearly related to T_{p^2}. The first assertion now follows from Theorem 6.3a). Regarding the second one, Theorem 6.3 gives a lower bound of $p^{\sum_{k=0}^{n-1} p^k} \cdot 2^{p^{n-1}}$ for the order of $\mathrm{Mon}_{\overline{k}}(f^n)$, whereas $|[D_p]^n| = (2p)^{\sum_{k=0}^{n-1} p^k}$. Thus $\frac{\log|G|}{\log|H|} \geqslant \frac{(\sum_{k=0}^{n-1} p^k)+\log_p(2)p^{n-1}}{(\sum_{k=0}^{n-1} p^k)\cdot(1+\log_p(2))}$, and therefore $\liminf_{n\to\infty} \frac{\log|G|}{\log|H|} \geqslant \frac{1}{1+\log_p(2)} \liminf_{n\to\infty}(1+\log_p(2)\frac{p^{n-1}(p-1)}{p^n-1}) = \frac{p(1+\log_p(2))-\log_p(2)}{p(1+\log_p(2))} = 1 - \frac{\log_p(2)}{p(1+\log_p(2))}$. □

Note that Corollary 6.4 applies in particular to many PCF (post-critically finite) polynomials with dihedral monodromy group. The asserted containment of $[C_p]^\infty$ in $\varprojlim_n \mathrm{Mon}(f^n)$ is then notably different from the case of PCF *unicritical* polynomials f, which have $[[C_p]^\infty : \varprojlim_n \mathrm{Mon}_{\overline{k}}(f^n)] = \infty$ (e.g., [AH25]). For the case $p = 3$, Corollary 6.4 in fact applies to all non-unicritical polynomials not conjugate to $\pm T_3$ (see [AMT20] for a list of PCF cubics over $\mathbb{Q}$), and gives a values of approximately 0.871 for the Hausdorff dimension.

Appendix A. Exceptional monodromy groups of 2-step decomposable polynomials with small kernel

Here we collect the monodromy groups of polynomials $f = g \circ h$ with g, h indecomposable, such that $\ker(\mathrm{Mon}(f) \to \mathrm{Mon}(g))$ is not large in our sense, and moreover $g \circ h$ does not fall into Cases 1 or 2 of Theorem 1.2; see in particular Theorems 2.2 and 2.6. We give the geometric monodromy group $G := \mathrm{Mon}_{\overline{k}}(f)$ and the arithmetic monodromy group $A := \mathrm{Mon}_k(f)$. Note that all but three of the groups G are their own symmetric normalizer, whence automatically $G = A$; the other three have index 2 in their symmetric normalizer, giving one additional option for A.

In all but the first line of the table, $\mathrm{Mon}(f)$ is nonsolvable; moreover, in all cases one has $h \sim X^2$, $h \sim X^3$ or $h \sim T_3$. We furthermore keep track of whether the group extension over the kernel $\ker(\mathrm{Mon}(f) \to \mathrm{Mon}(g))$ is split or not, and whenever possible give the precise label of $\mathrm{Mon}(f)$ in Magma's transitive group database (since. e.g., this information is needed in case of isomorphism $\mathrm{Mon}(f) \cong \mathrm{Mon}(g) \times \mathrm{Mon}(h)$, in order to exclude the presence of a Ritt move (see Proposition 3.13)). Note that the groups $\mathrm{Mon}(f)$ of the largest occurring degree 62 are currently not in the scope of the transitive group database, although they may be uniquely identified by the fact that there is only a single conjugacy class of transitive subgroups of $C_2 \wr PSL_5(2)$ of each indicated type. We also note that, due to the explicitly known polynomials with exceptional nonsolvable monodromy groups (e.g., [Mül95], [CNC99], [Elk13]) and due to the fact that only very specific ramification types can yield the monodromy groups in Table 1, it is in principle possible to compute all polynomials giving rise to these monodromy groups, although the calculations would be very tedious. We only mention, as a sample result, that the case $\mathrm{Mon}(f) = 15T15 \cong C_3 \times A_5$ occurs exactly for $f = g \circ h$ linearly equivalent to $(X^3(X^2+5X+40)) \circ (X^3+\alpha)$ with α a root of $X^2+5X+40$. Indeed, the only way to produce this monodromy group is to compose the A_5-polynomial with ramification

[13] Here f, g are called conjugate over $\overline{k}$ if $g = \mu \circ f \circ \mu^{-1}$ for a linear $\mu \in \overline{k}[X]$.

$\deg(g)$	$\mathrm{Mon}_{\overline{k}}(h)$	$G := \mathrm{Mon}_{\overline{k}}(f)$	comments	$A := \mathrm{Mon}_k(f)$
4	C_2	$2.S_4 \cong GL_2(3)$	nonsplit, $8T23$	G
6	C_2	$2.PGL_2(5)$	nonsplit, $12T124$	G
7	C_2	$C_2 \times PSL_3(2)$	$14T17$	G
7	C_2	$2^4.PSL_3(2)$	nonsplit, $14T42$	G
7	C_2	$2^4 \rtimes PSL_3(2)$	$14T43$	G
8	C_2	$2.PGL_2(7)$	nonsplit, $16T1036$	G
10	C_2	$2.P\Gamma L_2(9)$	nonsplit, $20T265$	G
11	C_2	$C_2 \times M_{11}$	$22T26$	G
13	C_2	$C_2 \times PSL_3(3)$	$26T47$	G
15	C_2	$2^5 \rtimes PSL_4(2)$	$30T1893$	G
15	C_2	$2^{11} \rtimes PSL_4(2)$	$30T3819$	G
21	C_2	$2^{10} \rtimes P\Gamma L_3(4)$	$42T3846$	G
23	C_2	$2^{12} \rtimes M_{23}$	$46T39$	G
31	C_2	$2^{16} \rtimes PSL_5(2)$		G
31	C_2	$2^{26} \rtimes PSL_5(2)$		G
5	C_3	$C_3 \times A_5$	$15T15$	G or $15T21$
8	C_3	$C_3 \times PGL_2(7)$	$24T2668$	G
11	C_3	$3^6 \rtimes PSL_2(11)$	$33T63$	G or $33T69$
13	C_3	$3^7 \rtimes PSL_3(3)$	$39T210$	G or $39T218$
13	D_3	$(3^{10} \rtimes 2) \rtimes PSL_3(3)$	$39T248$	G

TABLE 1. Groups occurring as monodromy groups of length-2 decomposable polynomials $f = g \circ h$ with "small kernel", not linearly equivalent to X^n or T_n, and without a Ritt move.

type $([5], [3.1^2], [2^2.1])$ with X^3 in such a way that the branch point 0 of X^3 is one of the special points over the $[3.1^2]$ branch point. Up to linear equivalence, this yields the above polynomial.

Coincidentally, none of the polynomials f corresponding to the groups in Table 1 can be defined over $\mathbb{Q}$ or even $\mathbb{R}$, which can most easily be seen from the fact that none of the arithmetic monodromy groups A contain an element x of the normalizer of a cyclic transitive subgroup $\langle\tau\rangle$ with $x\tau x^{-1} = \tau^{-1}$, something that would however be necessary for definability over $\mathbb{R}$ due to the action of complex conjugation on the inertia group at infinity, cf., e.g., [MM99, Theorem I.10.3].

APPENDIX B. SOME EXTENSIONS OF LEMMA 3.9

For the sake of future applications to lower-bounding monodromy groups of compositions of arbitrarily many polynomials, we record here some generalizations of Lemma 3.9, namely to not necessarily semisimple modules W'.

Lemma B.1. *Let $H = W.U$, where W is a faithful submodule of the $\mathbb{F}_p[U]$ permutation module. Let $G \leqslant H \wr S_d$ be such that $\pi : G \to S_d$ maps onto a transitive subgroup of S_d, and let $\Gamma = \ker(\pi) = G \cap H^d$. Furthermore, let $\rho : \Gamma \to U^d$ be the natural projection and $\Delta = \ker(\rho) = \Gamma \cap W^d$. Assume all of the following:*

i) The image of Γ under projection to one (hence any, due to transitivity of G in the blocks action) component equals $W.U'$ for a subgroup $U' \leqslant U$ such that $W = W_1 + \cdots + W_r$ is a direct sum of indecomposable $\mathbb{F}_p[U']$-modules W_j, $j = 1, \ldots, r$.

ii) Moreover $\tilde{W}_j := W_j/(W_j \cap D)$ *is an irreducible* $\mathbb{F}_p[U']$*-module for all* $j \in \{1, \dots, r\}$*, where* $D \subseteq W$ *is the diagonal*

iii) There exist elements $x_1, \dots x_s \in \Gamma$ *(*$s \geqslant 1$*) and* $i \in \{1, \dots, d\}$ *such that, for all* $j = 1, \dots, r$*,*

$$\bigcap_{m=1}^{s} \operatorname{supp}(\rho_j(x_m)) = \bigcap_{m=1}^{s} \operatorname{supp}(\tilde{\rho}_j(x_m)) \subseteq \{i\}, \tag{5}$$

where $\rho_j(x)$ *and* $\tilde{\rho}_j(x)$ *denote the image of* $\rho(x)$ *in* $GL(W_j)^d$ *and in* $GL(\tilde{W}_j)^d$*, respectively.*

Then $\Delta \supseteq W'^d$*, where* W' *is defined as the sum of the* W_j *for which equality holds in* (5)*.*

Proof. Note that the irreducibility of W_j was only used to guarantee that Observation 1 in the proof of Lemma 3.9 holds. Using instead the irreducibility assumption on $\tilde{W}_j$, this can be replaced by

Observation 1': Given any $\gamma \in \Gamma$ whose i-th component γ_i lies in $W_j \backslash D$ and any $1 \neq u \in U$ acting nontrivially on $\tilde{W}_j$, there exists $\tilde{\gamma} \in \Gamma$ conjugate to γ such that $\tilde{\gamma}_i$ lies in W_j and $\tilde{\gamma}_i^u \not\equiv \tilde{\gamma}_i \bmod D$.

The remainder of the proof can therefore be carried out in analogy with the one of Lemma 3.9, with Observation 1' ensuring that, for any i, j yielding equality in (5) (in particular, such that the i-th component entries of $x_1, \dots, x_s$ all act nontrivially on $\tilde{W}_j$), all commutators formed in the proof have i-th component entry in $W_j \backslash D$. The proof is concluded via noting that, since the dimension of the diagonal submodule $W_j \cap D$ is at most 1, the $\mathbb{F}_p[U']$-submodule of W_j generated by any element of $W_j \backslash D$ is necessarily W_j itself. Thus $\Delta \supseteq W_j^d$ follows as before. □

Example B.2. In the setting of Lemma B.1, let $\mathrm{Aug}(\mathbb{F}_2^4).S_4 \leqslant H \leqslant C_2 \wr S_4$. Since the S_4-permutation module $\mathbb{F}_2^4$ has irreducible heart $\mathrm{Aug}(\mathbb{F}_2^4)/\mathrm{diag}(\mathbb{F}_2^4)$, Assumption ii) holds with $W' = \mathrm{Aug}(\mathbb{F}_2^4)$. Moreover, any element of order 3 in S_4 acts nontrivially on the heart. Thus, if $d \geqslant 3$ and Γ/Δ contains a subgroup subgroup C_3^{d-1}, Assumption iii) clearly holds as well (namely, with $s = 2$ elements of order 3, each supported on only two components), yielding the conclusion $\Delta \supseteq (\mathrm{Aug}(\mathbb{F}_2^4))^d$.

A situation still not falling into the scope of Lemma B.1 is $H \leqslant C_p \wr C_p$ (p prime), since the $\mathbb{F}_p[C_p]$ permutation module is indecomposable with submodules of every dimension $0 \leqslant d \leqslant p$. To obtain a reasonably simple criterion here, we restrict to a particular special case of Assumption iii).

Lemma B.3. *Let* $H = W.U$*, where* W *is an* $\mathbb{F}_p[U]$*-module. Let* $G \leqslant H \wr S_d$ *be such that* $\pi : G \to S_d$ *maps onto a transitive subgroup of* S_d*, and let* $\Gamma = \ker(\pi) = G \cap H^d$*. Furthermore, let* $\rho : \Gamma \to U^d$ *be the natural projection and* $\Delta = \ker(\rho) = \Gamma \cap W^d$*. Assume all of the following:*

i) The image of Γ *under projection to one component contains* $H' := W.U'$ *for some subgroup* $U' \leqslant U$ *such that* W *is an indecomposable* $\mathbb{F}_p[U']$*-module.*

ii) $\Gamma/\Delta \supseteq U'^d$*.*

Set $W_0 := W$ *and* $W_i := [W_{i-1}, H']$ *for* $i \geqslant 1$*, where* $[W_{i-1}, H']$ *denotes the module generated by commutators. Then the following hold:*

1) $\Delta \supseteq W_2^d$*,*

2) If additionally $W_1 \subsetneq W$ *is the unique maximal* $\mathbb{F}_p[U']$*-submodule of* W*, then either* $W_1 = W_2$ *or* Δ/W_2^d *contains an element of support size* 2 *in* $(W_1/W_2)^d$*.*

Proof. Let $u, v \in U'$. Due to Assumption ii), there exists $x, y \in \Gamma$ with $\rho(x) = (u, 1, \dots, 1)$ and $\rho(y) = (v, 1, \dots, 1)$. I.e., $x = (\tilde{u}, w_2, \dots, w_d)$ for some $\tilde{u} \in H$ mapping to u under the projection $H \to U$, and for some $w_2, \dots, w_d \in W$; and analogously for y. Moreover, for every $w \in W$, there exists $z \in \Gamma$ with first component $z_1 = w$, due to Assumption i). Then the commutator $[z, x]$ is an element of Δ with first coordinate $[w, \tilde{u}]$. Thus, the commutator $[[z, x], y] \in \Delta$ is supported only on the first component, with entry $[[w, \tilde{u}], \tilde{v}]$. As u, v run through all of U' and w through all W, these elements generate all of W_2, so that $\Delta \supseteq W_2^d$, showing 1). Next, consider the quotient module $\tilde{\Delta} := \Delta / W_2^d$. We distinguish two cases, depending on the component entries of the element x above.

Case 1: For all x as above, it holds that $w_j \in W_1$ for all $j \in \{2, \dots, d\}$. Then all but the first component entry of $[z, x]$ are in fact in W_2. On the other hand, as soon as $W_1 \subsetneq W$, we may pick z such that its first component entry w is in $W \backslash W_1$. The additional assumption of W_1 being the unique maximal submodule of W implies that the $\mathbb{F}_p[U']$-submodule generated by w is all of W. If the module $[w, H]$ generated by all commutators $[w, h]$, $h \in H'$ is contained in W_2, then $W_1 = [W, H'] = [w, H'] = W_2$. We may thus assume that there exists $\tilde{u} \in H'$ with $[w, \tilde{u}] \notin W_2$, so that for this choice of w and $\tilde{u}$, the element $[z, x]$ maps to an element of $\tilde{\Delta}$ supported exactly on the first component, trivially implying 2).

Case 2: There exists x as above and $j \in \{2, \dots, d\}$ with $w_j \notin W_1$. As in Case 1), we may assume that there exists $h \in H'$ with $[w_j, h] \notin W_2$. By Assumption ii), we may pick $\tilde{x} \in \Gamma$ with $\mathrm{supp}(\rho(\tilde{x})) = \{j\}$ and whose j-th component $\tilde{x}_j$ has the same image as h under projection $H \to U$. Then $[\tilde{x}, x]$ is supported at most on the first and the j-th component, and additionally the j-th component entry equals $[w_j, h] \notin W_2$. This again implies 2). □

Remark B.4. The commutator approach used in the above proof shows that in fact $W_2^d \subseteq [\Gamma, \Gamma] \cap \Delta$, and even more precisely that $W_2^d \subseteq [\Gamma_0, \Gamma_0] \cap \Delta$ with $\Gamma_0 \subseteq \Gamma$ the preimage of $U'^d \subseteq \Gamma / \Delta$.

Example B.5. For $W = \mathbb{F}_p^p$ the permutation module under the cyclic group $U' = C_p$ (i.e., $H' = C_p \wr C_p$), W_j is the unique submodule of codimension j in W; in particular, one has $W_1 = \mathrm{Aug}(\mathbb{F}_p^p)$ and $W_1 / W_2 \cong \mathbb{F}_p$. In the case where $\pi(G) \leqslant S_d$ additionally acts primitively (e.g., when d is a prime), an element of support size 2 necessarily generates a submodule of codimension 1 in $(W_1/W_2)^d$. Lemma B.3 thus asserts that in this case Δ contains a submodule of codimension $\leqslant 1$ of $(\mathrm{Aug}(\mathbb{F}_p^p))^d$, and due to Remark B.4, this submodule is even contained in $\Delta \cap [\Gamma_p, \Gamma_p]$ with a p-Sylow subgroup Γ_p of Γ.

References

[AH25] Ophelia Adams and Trevor Hyde, *Profinite iterated monodromy groups of unicritical polynomials*, 2025, https://arxiv.org/abs/2504.13028.

[AMT20] Jacqueline Anderson, Michelle Manes, and Bella Tobin, *Cubic post-critically finite polynomials defined over* $\mathbb{Q}$, LMS Journal of Computation and Mathematics **23** (2020), 20–34.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[BKN26] Angelot Behajaina, Joachim König, and Danny Neftin, *The Davenport–Lewis–Schinzel problem on the reducibility of* $f(x) - g(y)$, 2026.

[CNC99] Pierrette Cassou-Noguès and Jean-Marc Couveignes, *Explicit factorizations of* $g(y) - h(z)$, Acta Arith. **87** (1999), no. 4, 291–317 (English).

[Cou96] Jean-Marc Couveignes, *Tools for the computation of families of coverings*, London Math. Soc. Lecture Note Ser. (Gainesville, United States) (Cambridge University Press, ed.), London Math. Soc. Lecture Note Ser., vol. 256, Helmut Völklein, David Harbater, Peter Müller and J. G. Thompson, October 1996, pp. 38–65.

[CR66] C.W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing Series, Interscience Publishers, 1966.

[DLS61] Harold Davenport, D. J. Lewis, and Andrzej Schinzel, *Equations of the form $f(x) = g(y)$*, Q. J. Math., Oxf. II. Ser. **12** (1961), 304–312 (English).

[Elk13] Noam Elkies, *The complex polynomials $P(x)$ with $Gal(P(x) - t) \cong M_{23}$*, ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, The Open Book Series **1** (2013), 359–367.

[KNR24] Joachim König, Danny Neftin, and Shai Rosenberg, *Polynomial compositions with large monodromy groups and applications to arithmetic dynamics*, 2024, https://arxiv.org/pdf/2401.17872.

[MM99] Gunter Malle and B.Heinrich Matzat, *Inverse Galois Theory*, Berlin-Heidelberg: Springer, 1999.

[Mor80] Brian Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proc. Lond. Math. Soc. (3) **41** (1980), 1–20 (English).

[Mül95] Peter Müller, *Primitive monodromy groups of polynomials*, Recent developments in the inverse Galois problem. A joint summer research conference, July 17-23, 1993, University of Washington, Seattle, WA, USA, Providence, RI: American Mathematical Society, 1995, pp. 385–401 (English).

[Mül98] ———, *Kronecker conjugacy of polynomials*, Trans. Am. Math. Soc. **350** (1998), no. 5, 1823–1850 (English).

[Pak09] Fedor Pakovich, *Prime and composite Laurent polynomials*, Bulletin des Sciences Mathématiques **133** (2009), no. 7, 693–732.

[Rit22] Joseph F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), no. 1, 51–66.

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed. ed., Grad. Texts Math., vol. 254, Berlin: Springer, 2009 (English).

[ZM08] Michael E. Zieve and Peter Müller, *On Ritt's polynomial decomposition theorems*, 2008, https://arxiv.org/pdf/0807.3578.

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

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

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