# DECOMPOSITIONS OF LAURENT POLYNOMIALS

MICHAEL E. ZIEVE

Abstract. In the 1920's, Ritt studied the operation of functional composition $g \circ h(x) = g(h(x))$ on complex rational functions. In the case of polynomials, he described all the ways in which a polynomial can have multiple 'prime factorizations' with respect to this operation. Despite significant effort by Ritt and others, little progress has been made towards solving the analogous problem for rational functions. In this paper we use results of Avanzi–Zannier and Bilu–Tichy to prove analogues of Ritt's results for decompositions of Laurent polynomials, i.e., rational functions with denominator $x^n$.

## 1. Introduction

In the 1920's, Ritt [28] studied the possible ways of writing a complex polynomial as a composition of lower-degree polynomials. To this end, a polynomial $f \in \mathbb{C}[x]$ with $\deg(f) > 1$ is called *indecomposable* if it cannot be written as a composition $f(x) = g(h(x))$ with $g, h \in \mathbb{C}[x]$ and $\deg(g), \deg(h) < \deg(f)$. By induction, any polynomial of degree more than one can be written as the composition of indecomposable polynomials. Although this decomposition need not be unique, Ritt proved that its length is unique, and moreover he gave a recursive procedure for obtaining any decomposition from any other. Ritt's results are quite fundamental, and have been applied in various wide-ranging contexts (cf. [3, 6, 13, 14, 24, 25, 26, 27, 35], among others).

Unfortunately, there are no known analogues of Ritt's results in the case of rational functions. Ritt himself was the first to study this [29, 30]. He noted [30] that the action of the group $A_4$ on the Riemann sphere, together with the fact that $A_4$ has maximal chains of subgroups $1 < C_2 < V_4 < A_4$ and $1 < C_3 < A_4$, implies that a certain degree-12 rational function can be written as both the composition of two indecomposables and the composition of three indecomposables. (This example is reproduced in the context of modular forms in [15, 21].) Further, if $f(x)$ is the map on $x$-coordinates induced by multiplication-by-$p$ on the elliptic curve $y^2 = x^3+1$, for any prime $p$ with $p \equiv 2 \pmod 3$, then $f$ is indecomposable but there is a decomposable

*Date*: October 10, 2007.

1991 *Mathematics Subject Classification.* Primary 12F10; Secondary 11R58, 14H30.

I thank Fedor Pakovich for posing the problem of studying the Laurent polynomial analogue of Ritt's first theorem, and for remarking that an affine curve parametrized by Laurent polynomials has at most two points at infinity.

$g \in \mathbb{C}(x)$ for which $x^3 \circ f = g \circ x^3$ [19]. Further families of counterexamples to the rational function analogues of Ritt's results are given in [19]; however, as noted there, all known examples fit into one of three simple types, which suggests there may be a concise description of all examples. On the other hand, proving such a possibility seems far beyond current techniques.

In this paper we study a situation which lies between the polynomial and rational function cases: namely, we study *Laurent polynomials*, i.e., rational functions of the form $f(x)/x^n$ with $f \in \mathbb{C}[x]$. We will prove that decompositions of Laurent polynomials satisfy variants of Ritt's results. Our statements involve the Dickson polynomials $D_n(x)$, which are defined by the functional equation $D_n(x + 1/x) = x^n + 1/x^n$; these are related to the classical Chebychev polynomials $T_n(x)$ via $D_n(x) = 2T_n(x/2)$. We say a rational function of degree $> 1$ is *indecomposable* if it cannot be written as the composition of rational functions of strictly lower degrees, and a *complete decomposition* of a rational function is an expression of the rational function as the composition of indecomposable rational functions. We note (cf. Lemma 2.3) that a decomposable Laurent polynomial can actually be written as the composition of two Laurent polynomials of strictly lower degrees, rather than just as the composition of lower-degree rational functions. Writing $\mathcal{L}$ for the set of all complex Laurent polynomials, our Laurent polynomial analogue of the classical 'first theorem of Ritt' is as follows:

**Theorem 1.1.** *If $f = p_1 \circ p_2 \circ \cdots \circ p_r = q_1 \circ q_2 \circ \cdots \circ q_s$ where $p_i, q_j \in \mathbb{C}(x)$ are indecomposable and $f \in \mathcal{L}$, then the sequences $(\deg(p_1), \ldots, \deg(p_r))$ and $(\deg(q_1), \ldots, \deg(q_s))$ are permutations of one another (so $r = s$). Moreover, there is a finite sequence of complete decompositions of $f$ which begins with $p_1 \circ \cdots \circ p_r$ and ends with $q_1 \circ \cdots \circ q_s$, where consecutive decompositions in the sequence differ only in that two adjacent indecomposables in the first decomposition are replaced in the second decomposition by two others having the same composition.*

Our Laurent polynomial analogue of the 'second theorem of Ritt' is:

**Theorem 1.2.** *If $f = g_1 \circ h_1 = g_2 \circ h_2$ where $g_1, g_2, h_1, h_2 \in \mathbb{C}(x)$ are indecomposable and $f \in \mathcal{L}$, then (after perhaps exchanging the pairs $(g_1, h_1)$ and $(g_2, h_2)$) there exist degree-one $\mu_1, \ldots, \mu_4 \in \mathbb{C}(x)$ such that*

$$\begin{aligned} g_1 &= \mu_1 \circ G_1 \circ \mu_3 \\ g_2 &= \mu_1 \circ G_2 \circ \mu_4 \\ h_1 &= \mu_3^{-1} \circ H_1 \circ \mu_2 \\ h_2 &= \mu_4^{-1} \circ H_2 \circ \mu_2, \end{aligned}$$

*where one of the following holds (with $n$ prime):*

(1.2.1) *$G_1 = G_2$ and $H_1 = H_2$ with $G_1, H_2 \in \mathcal{L}$ and either $G_1 \in \mathbb{C}[x]$ or $H_2 = x^n$;*

(1.2.2) *$G_1 = H_2 = x^n$, $H_1 = x^r q(x^n)$, and $G_2 = x^r q(x)^n$ with $q \in \mathbb{C}(x)$ and $r \in \mathbb{Z}_{>0}$ coprime to $n$;*

(1.2.3) *$G_1 = H_2 = D_m$ and $H_1 = G_2 = D_n$, where $m \neq n$ is prime;*
(1.2.4) *$G_1 = D_n$, $H_1 = G_2 = x + 1/x$, and $H_2 = x^n$;*
(1.2.5) *$G_1 = G_2 = D_n$, $H_1 = x+1/x$, and $H_2 = \zeta x + 1/(\zeta x)$, where $\zeta^n = 1$.*

We emphasize that, in (1.2.2), we do not require $q \in \mathcal{L}$. In fact, our proof shows we can require either $q \in \mathcal{L}$ or $q = Q(\frac{1}{x+1})$ with $Q \in x\mathbb{C}[x]$. To see why the latter case gives rise to Laurent polynomials (after composing with $\mu_2$), put $q = Q(\frac{1}{x+1})$ with $Q \in x\mathbb{C}[x]$, so $xq(x^2) \circ i\frac{x-1}{x+1} = i\frac{x-1}{x+1}Q(\frac{(x+1)^2}{4x})$, which is in $\mathcal{L}$.

These results generalize the classical theorems of Ritt, which are obtained by requiring all the rational functions to be polynomials. Stated in the other direction, if we begin with Ritt's results and attempt to generalize them to decompositions of Laurent polynomials, we must replace the various polynomials in Ritt's results by rational functions, and also we must allow the new possibilities (1.2.4) and (1.2.5). In fact, (1.2.5) can be obtained from two applications of (1.2.4), in addition to composing with linears: for, if $\zeta^n = 1$ then

$$\begin{aligned} D_n \circ \left(\zeta x + \frac{1}{\zeta x}\right) &= D_n \circ \left(x + \frac{1}{x}\right) \circ \zeta x \\ &= \left(x + \frac{1}{x}\right) \circ x^n \circ \zeta x \\ &= \left(x + \frac{1}{x}\right) \circ x^n \\ &= D_n \circ \left(x + \frac{1}{x}\right). \end{aligned}$$

One consequence of Ritt's results, which actually was deduced as a step in Ritt's proofs, is a certain 'rigidity' property of polynomial decompositions:

**Corollary 1.3.** *If $g_1 \circ h_1 = g_2 \circ h_2$ where $g_1, g_2, h_1, h_2 \in \mathbb{C}[x] \setminus \mathbb{C}$ and* $\deg(g_1) = \deg(g_2)$*, then there is a linear $\mu \in \mathbb{C}[x]$ such that $g_2 = g_1 \circ \mu$ and $h_2 = \mu^{-1} \circ h_1$.*

Note that (1.2.5) provides counterexamples to the Laurent polynomial analogue of Corollary 1.3. Further counterexamples are obtained by putting $n = 2$ in (1.2.4). We will determine all examples:

**Proposition 1.4.** *If $f = g_1 \circ h_1 = g_2 \circ h_2$ where $f \in \mathcal{L} \setminus \mathbb{C}$ and $g_1, g_2, h_1, h_2 \in \mathbb{C}(x)$ satisfy* $\deg(g_1) = \deg(g_2)$*, then, perhaps after exchanging $(g_1, h_1)$ and $(g_2, h_2)$, there exist $G \in \mathbb{C}[x]$, $H \in \mathcal{L}$, and degree-one $\mu_1, \mu_2 \in \mathbb{C}(x)$ such that*

$$\begin{aligned} g_1 &= G \circ G_1 \circ \mu_1 \\ g_2 &= G \circ G_2 \circ \mu_2 \\ h_1 &= \mu_1^{-1} \circ H_1 \circ H \\ h_2 &= \mu_2^{-1} \circ H_2 \circ H, \end{aligned}$$

*where one of the following holds (in which $n \in \mathbb{Z}_{>0}$):*

(1.4.1) $G_1 = G_2 = H_1 = H_2 = x$;

(1.4.2) $G_1 = H_2 = x^n$, $H_1 = (x^n+1)/x^r$, *and* $G_2 = (x+1)^n/x^r$, *where* $0 < r < n$ *and* $\gcd(r,n) = 1$;

(1.4.3) $G_1 = -G_2 = D_n$, $H_1 = x + 1/x$, *and* $H_2 = \zeta x + 1/(\zeta x)$, *where* $\zeta^n = -1$;

(1.4.4) $G_1 = D_2$, $H_1 = G_2 = x + 1/x$, *and* $H_2 = x^2$.

*Moreover, in* (1.4.2)–(1.4.4) *we may assume* $H = \alpha x^s$ *with* $\alpha \in \mathbb{C}^*$ *and* $s \in \mathbb{Z}_{>0}$.

Ritt proved a generalization of the polynomial version of Theorem 1.2, which can be used to describe all polynomials $g_1, g_2, h_1, h_2$ with $g_1 \circ h_1 = g_2 \circ h_2$ [3]. We will prove the following analogue for Laurent polynomials:

**Theorem 1.5.** *Let $f \in \mathcal{L} \setminus \mathbb{C}$ and $g_1, g_2, h_1, h_2 \in \mathbb{C}(x)$ satisfy $f = g_1 \circ h_1 = g_2 \circ h_2$. Then, perhaps after switching $(g_1, h_1)$ and $(g_2, h_2)$, we have*

$$\begin{aligned} g_1 &= G \circ G_1 \circ \mu_1 \\ g_2 &= G \circ G_2 \circ \mu_2 \\ h_1 &= \mu_1^{-1} \circ H_1 \circ H \\ h_2 &= \mu_2^{-1} \circ H_2 \circ H \end{aligned}$$

*for some $G \in \mathbb{C}[x]$, some $H \in \mathcal{L}$, and some degree-one $\mu_1, \mu_2 \in \mathbb{C}(x)$, where one of the following holds (in which $m, n$ are coprime positive integers, and $p \in \mathbb{C}[x] \setminus \{0\}$):*

(1.5.1) $G_1 = H_2 = x^n$, $H_1 = x^r p(x^n)$, *and* $G_2 = x^r p(x)^n$, *where* $r \in \mathbb{Z}$ *with* $\gcd(r,n) = 1$;

(1.5.2) $G_1 = x^2$, $H_1 = (x - \frac{1}{x})p(x + \frac{1}{x})$, $G_2 = (x^2-4)p(x)^2$, *and* $H_2 = x + 1/x$;

(1.5.3) $G_1 = H_2 = D_m$ *and* $H_1 = G_2 = D_n$;

(1.5.4) $G_1 = (\frac{x^2}{3} - 1)^3$, $H_1 = x^2 + 2x + \frac{1}{x} - \frac{1}{4x^2}$, $G_2 = 3x^4 - 4x^3$, *and* $H_2 = \frac{1}{3}((x + 1 - \frac{1}{2x})^3 + 4)$;

(1.5.5) $G_1 = D_{dm}$, $H_1 = x^n + 1/x^n$, $G_2 = -D_{dn}$, *and* $H_2 = (\zeta x)^m + 1/(\zeta x)^m$, *where* $d \in \mathbb{Z}_{>1}$ *and* $\zeta^{dmn} = -1$;

(1.5.6) $G_1 = D_m$, $H_1 = G_2 = x^n + 1/x^n$, *and* $H_2 = x^m$.

*Moreover, in all cases besides* (1.5.1) *and* (1.5.3), *we may assume* $H = \alpha x^s$ *with* $\alpha \in \mathbb{C}^*$ *and* $s \in \mathbb{Z}_{>0}$.

The analogous result for decompositions of polynomials [3] involves only cases (1.5.1) and (1.5.3).

Ritt's proofs of the polynomial versions of Theorems 1.1 and 1.2 are independent of one another, and have quite distinct flavors. His proof of Theorem 1.1 for polynomials is essentially group theoretic: if $f$ is a polynomial then the inertia group $I$ at any infinite place of (the Galois closure of) $\mathbb{C}(x)/\mathbb{C}(f(x))$ is transitive, so one can translate questions about decompositions of $f$ into questions about subgroups of $I$, which are not difficult to resolve since $I$ is cyclic. On the other hand, Ritt's proof of Theorem 1.2 for polynomials is a genus computation, as he determines all polynomials $g_1, h_1$ of coprime degrees for which the curve $g_1(x) - h_1(y)$ has genus zero. For Laurent polynomials we require a different approach, since there is no longer a transitive inertia group, so Theorem 1.1 cannot be proved via group theory. Instead we first prove Theorem 1.5, using results of Avanzi–Zannier [2] and Bilu–Tichy [6], which in turn rely on Ritt's second theorem and related genus computations (among other things). After determining the possible decompositions of the specific rational functions appearing in Theorem 1.5, we can then deduce Theorems 1.1 and 1.2. We pay special attention to decompositions of $H_1$ and $G_2$ from (1.2.2), in view of their role in potential analogues of Ritt's results for rational functions: these $H_1$ and $G_2$ are especially important since they have the same shape as one of the main sources of rational function counterexamples (the one including the elliptic curve examples mentioned above).

Ritt's proofs used the language of Riemann surfaces; several authors have rewritten his proofs in different languages [7, 8, 9, 11, 12, 16, 17, 20, 22, 31, 32, 33, 34]. For some applications the recursive procedure in Theorem 1.2 is not sufficient, and one needs more precise information about the collection of all the different decompositions of a polynomial; see [23] for the state of the art on polynomial decomposition. We do not know whether there are Laurent polynomial analogues of the latter results.

The contents of this paper are as follows. In the next section we prove some general results about decompositions of Laurent polynomials, based on which we outline our strategy for proving our main results. In Sections 3 and 4 we describe all decompositions of the various special Laurent polynomials occurring in the statements of the above results. We use these specific decompositions to prove preliminary versions of Theorem 1.5 in Sections 5 and 6, and finally we conclude in Section 7 by proving the results stated in this introduction.

## 2. Preliminary reductions

Recall that the set $\mathcal{L}$ of Laurent polynomials consists of all rational functions whose denominator is a power of $x$, or equivalently, all rational functions having no poles besides 0 and $\infty$. This perspective yields the following result:

**Lemma 2.1.** *If $f = g \circ h$ where $f \in \mathcal{L} \setminus \mathbb{C}$ and $g, h \in \mathbb{C}(x)$, then there is a degree-one $\mu \in \mathbb{C}(x)$ such that $G := g \circ \mu$ and $H := \mu^{-1} \circ h$ satisfy one of the following:*

(2.1.1) *$G \in \mathbb{C}[x]$ and $H \in \mathcal{L}$;*

(2.1.2) *$G \in \mathcal{L}$ and $H = x^n$ for some $n \in \mathbb{Z}_{>0}$.*

*Proof.* The poles of $f = g \circ h$ are the preimages under $h$ of the poles of $g$; by hypothesis, these preimages form a subset of $\{0, \infty\}$. Hence $g$ has at most two poles. First suppose $g$ has a unique pole, say $\alpha$. Pick a degree-one

$\mu \in \mathbb{C}(x)$ for which $\mu(\infty) = \alpha$, so that $G := g \circ \mu$ has $\infty$ as its unique pole, whence $G \in \mathbb{C}[x]$. Then $f = G \circ H$ where $H := \mu^{-1} \circ h$, and $H$ can have no poles besides 0 and $\infty$, so $H \in \mathcal{L}$, as in (2.1.1). Now suppose $g$ has two poles, say $\alpha$ and $\beta$. Since $g \circ h$ has at most two poles, both $\alpha$ and $\beta$ must have unique preimages under $h$, which must be 0 and $\infty$. Say $\alpha = h(0)$ and $\beta = h(\infty)$, and put $\gamma = h(1)$. Pick a degree-one $\mu \in \mathbb{C}(x)$ which maps $0 \mapsto \alpha$ and $\infty \mapsto \beta$ and $1 \mapsto \gamma$. Then the poles of $G := g \circ \mu$ are 0 and $\infty$, so $G \in \mathcal{L}$, and $H := \mu^{-1} \circ h$ has its unique pole at $\infty$ (so $H \in \mathbb{C}[x]$) and has 0 as its unique root (so $H$ is a monomial) and maps $1 \mapsto 1$ (so $H$ is monic). □

Thus, in what follows we will restrict to decompositions $f = G \circ H$ where $G$ and $H$ satisfy (2.1.1) or (2.1.2). We refer to decompositions of these types as 'Type 1' and 'Type 2' decompositions. A pair of decompositions of the same Laurent polynomial must be in one of three categories: both decompositions could be Type 1, both could be Type 2, or one could be Type 1 and the other Type 2. It is easy to describe the pairs of Type 2 decompositions of a Laurent polynomial:

**Proposition 2.2.** *If $g_1 \circ x^n = g_2 \circ x^m$ with $g_i \in \mathcal{L}$ and $n, m > 0$, then there exists $G \in \mathcal{L}$ such that $g_1 = G \circ x^{\operatorname{lcm}(n,m)/n}$ and $g_2 = G \circ x^{\operatorname{lcm}(n,m)/m}$.*

In other words, if we write a Laurent polynomial $f$ as $f = G \circ x^N$ with $N$ maximal, then every Type 2 decomposition of $f$ is (up to linears) $G(x^n) \circ x^{N/n}$.

*Proof.* Writing $f = g_1 \circ x^n$, the field $\mathbb{C}(f)$ is contained in $\mathbb{C}(x^n) \cap \mathbb{C}(x^m) = \mathbb{C}(x^d)$, where $d = \operatorname{lcm}(n, m)$. Write $d = Nn = Mm$, so $g_1 \circ x^n = G_1 \circ x^d$ for some $G_1 \in \mathbb{C}(x)$ (which is automatically a Laurent polynomial), whence $g_1 = G_1 \circ x^N$. Likewise $g_2 = G_2 \circ x^M$, and we have $G_1 \circ x^d = f = G_2 \circ x^d$, so $G_1 = G_2$. Thus $f = G_1(x^{Nn})$, and its two Type 2 decompositions are $G_1(x^N) \circ x^n$ and $G_1(x^M) \circ x^m$. □

Next we consider Laurent polynomials with two Type 1 decompositions: $f = g_1 \circ h_1 = g_2 \circ h_2$ with $g_i \in \mathbb{C}[x]$ and $h_i \in \mathcal{L}$. Then there is an irreducible factor $E(x, y)$ of $g_1(x) - g_2(y)$ such that $E(h_1(x), h_2(x)) = 0$, so $E(x, y) = 0$ defines a genus-zero curve having at most two closed points lying over $x = \infty$ (since $f$ has at most two poles). To classify the possibilities in this case, we use a result of Bilu and Tichy [6] describing the polynomials $g_1, g_2$ for which the curve $g_1(x) = g_2(y)$ has an irreducible component with these properties. Note that in this situation there automatically exist nonconstant $h_1, h_2 \in \mathcal{L}$ such that $g_1 \circ h_1 = g_2 \circ h_2$, coming from a rational parametrization of the component in question.

Finally we consider Laurent polynomials with decompositions of both types: $f = g_1 \circ h_1 = g_2 \circ x^n$ where $g_1 \in \mathbb{C}[x]$ and $h_1, g_2 \in \mathcal{L}$ (and $n > 1$). Letting $\zeta$ be a primitive $n^{\text{th}}$ root of unity, we have

$$g_1 \circ h_1(\zeta x) = g_2 \circ x^n \circ \zeta x = g_2 \circ x^n = g_1 \circ h_1(x).$$

Let $h_2(x) = h_1(\zeta x)$. To classify the possibilities where $h_2 \neq h_1$, we use a result of Avanzi and Zannier [2] describing the polynomials $g_1$ for which there are distinct nonconstant rational functions $h_1, h_2$ such that $g_1 \circ h_1 = g_1 \circ h_2$. Finally, if $h_1(\zeta x) = h_1(x)$ then $h_1 = H(x^n)$ for some $H \in \mathcal{L}$, where $g_1 \circ H = g_2$. Thus, these possibilities come from decompositions of the Laurent polynomial $g_2$, which can be controlled inductively.

We now recall the well-known connection between decompositions of a rational function $f$ and intermediate fields between $\mathbb{C}(x)$ and $\mathbb{C}(f(x))$, as well as the corresponding results for polynomials and Laurent polynomials.

**Lemma 2.3.** *For $f \in \mathbb{C}(x) \setminus \mathbb{C}$, the fields between $\mathbb{C}(x)$ and $\mathbb{C}(f)$ are precisely the fields $\mathbb{C}(h)$, where $g, h \in \mathbb{C}(x)$ satisfy $f = g \circ h$; moreover, for $h, H \in \mathbb{C}(x)$, we have $\mathbb{C}(h) = \mathbb{C}(H)$ if and only if there is a degree-one $\mu \in \mathbb{C}(x)$ such that $h = \mu \circ H$. If $f$ is a Laurent polynomial (respectively, polynomial) and $f = g \circ h$ with $g, h \in \mathbb{C}(x)$, then there is a degree-one $\mu \in \mathbb{C}(x)$ such that both $g \circ \mu$ and $\mu^{-1} \circ h$ are Laurent polynomials (respectively, polynomials).*

*Proof.* The first statement follows from Lüroth's theorem. Now suppose $f = g \circ h$ where $g, h \in \mathbb{C}(x)$ and $f \in \mathbb{C}[x]$; since $\infty$ is the unique pole of $f$, it follows that $g$ has a unique pole $\alpha$, and $\infty$ is the unique preimage of $\alpha$ under $h$. Pick a degree-one $\mu \in \mathbb{C}(x)$ which maps $\infty \mapsto \alpha$, so both $g \circ \mu$ and $\mu^{-1} \circ h$ are rational functions whose unique pole is $\infty$, hence they are polynomials. Next suppose $f = g \circ h$ where $g, h \in \mathbb{C}(x)$ and $f \in \mathcal{L}$; then $f$ has no poles besides $0$ and $\infty$, so $g$ also has at most two poles, and the preimages of these poles under $h$ are a subset of $\{0, \infty\}$. Pick a degree-one $\mu \in \mathbb{C}(x)$ which maps the poles of $g$ to either $\{\infty\}$ or $\{0, \infty\}$; then both $g \circ \mu$ and $\mu^{-1} \circ h$ have no poles outside $\{0, \infty\}$, hence are Laurent polynomials. □

## 3. Decompositions of Laurent polynomials of special types

In this section we describe all decompositions of certain special Laurent polynomials occurring in our results. Knowledge of these decompositions will be used in the proofs of our main results.

We begin with $f = x^n + 1/x^n$ (where $n \in \mathbb{Z}_{>0}$), whose decompositions turn out to be the main source of Laurent polynomial decompositions that are not polynomial decompositions.

**Lemma 3.1.** *If $g, h \in \mathbb{C}(x)$ satisfy $g \circ h = x^n + x^{-n}$ for some $n > 0$, then there is a divisor $d$ of $n$ and a degree-one $\mu \in \mathbb{C}(x)$ such that one of the following holds:*

(3.1.1) *$g \circ \mu = x^{n/d} + x^{-n/d}$ and $\mu^{-1} \circ h = x^d$;*

(3.1.2) *$g \circ \mu = \beta^n D_{n/d}$ and $\mu^{-1} \circ h = (x/\beta)^d + (\beta/x)^d$ where $\beta^{2n} = 1$.*

*Proof.* Writing $f = x^n + x^{-n}$, we see that $\mathbb{C}(x)/\mathbb{C}(f)$ is Galois, with Galois group $G$ being dihedral of order $2n$ and consisting of the automorphisms $x \mapsto \zeta x^e$ with $\zeta^n = 1$ and $e \in \{1, -1\}$. Let $C$ be the cyclic subgroup of $G$ consisting of the automorphisms $x \mapsto \zeta x$. Let $H$ be a subgroup of $G$, and let $d = \#(H \cap C)$; then $H \cap C$ consists of the automorphisms $x \mapsto \delta x$ with $\delta^d = 1$, so the fixed field $\mathbb{C}(x)^{H\cap C}$ equals $\mathbb{C}(x^d)$. If $H = H \cap C$ then the chain of groups $1 < H < G$ corresponds (via Lemma 2.3) to the decomposition $f = (x^{n/d} + x^{-n/d}) \circ x^d$. Now suppose $H \neq H \cap C$, so $\#H = 2d$. Pick some $\zeta$ for which $H$ contains the automorphism $x \mapsto \zeta/x$. Then $\mathbb{C}(x)^H = \mathbb{C}(x^d + (\zeta/x)^d) = \mathbb{C}((x/\beta)^d + (\beta/x)^d)$ where $\beta^2 = \zeta$ (so $\beta^{2n} = 1$), and the corresponding decomposition is $f = (\beta^n D_{n/d}) \circ ((x/\beta)^d + (\beta/x)^d)$. □

We also recall the possible decompositions of $x^n$ and $D_n$:

**Lemma 3.2.** *If $g \circ h = x^n$ with $g, h \in \mathbb{C}[x]$ and $n > 0$, then there is a linear $\mu \in \mathbb{C}[x]$ and a divisor $d$ of $n$ such that $g \circ \mu = x^d$ and $\mu^{-1} \circ h = x^{n/d}$. If $g \circ h = D_n$ with $g, h \in \mathbb{C}[x]$ and $n > 0$, then there is a linear $\mu \in \mathbb{C}[x]$ and a divisor $d$ of $n$ such that $g \circ \mu = D_d$ and $\mu^{-1} \circ h = D_{n/d}$.*

*Proof.* This follows from Corollary 1.3, together with the fact that $D_d \circ D_{n/d} = D_n$ (which follows from the functional equation defining $D_n$). □

Rather than writing out all the decompositions of the rational functions in (1.5.4), we show that (1.5.4) is a consequence of (1.5.1) and (1.5.2), if we allow compositions with linear polynomials. Namely, putting $p = \frac{x}{2} + \sqrt{2}$ and $\nu = x\sqrt{2}$, we have

$$x^2 + 2x + \frac{1}{x} - \frac{1}{4x^2} = \left(x + \frac{1}{x}\right) \cdot p\left(x - \frac{1}{x}\right) \circ \nu,$$

so for

$$f := \left(\frac{x^2}{3} - 1\right)^3 \circ \left(x^2 + 2x + \frac{1}{x} - \frac{1}{4x^2}\right)$$

we have

$$\begin{aligned} f &= \left(\frac{x}{3} - 1\right)^3 \circ x^2 \circ \left(x + \frac{1}{x}\right) \cdot p\left(x - \frac{1}{x}\right) \circ \nu \\ &= \left(\frac{x}{3} - 1\right)^3 \circ (x^2 + 4)p(x)^2 \circ \left(x - \frac{1}{x}\right) \circ \nu, \end{aligned}$$

where the last equality comes from (1.5.2). Now put $\mu = \sqrt{2}(x - 1)$, so

$$(x^2 + 4)p(x)^2 \circ \mu = x^4 + 4x + 3$$

and

$$\mu^{-1} \circ \left(x - \frac{1}{x}\right) \circ \nu = x + 1 - \frac{1}{2x},$$

and thus if we put $\lambda = 3x - 4$ then

$$\begin{aligned} f &= x^3 \circ \left(\frac{x}{3} - 1\right) \circ (x^4 + 4x + 3) \circ \left(x + 1 - \frac{1}{2x}\right) \\ &= x^3 \circ \frac{x^4 + 4x}{3} \circ \left(x + 1 - \frac{1}{2x}\right) \\ &= x\left(\frac{x+4}{3}\right)^3 \circ \lambda \circ \lambda^{-1} \circ x^3 \circ \left(x + 1 - \frac{1}{2x}\right) \qquad \text{(from (1.5.1))} \\ &= (3x-4)x^3 \circ \frac{x+4}{3} \circ x^3 \circ \left(x + 1 - \frac{1}{2x}\right) \\ &= (3x^4 - 4x^3) \circ \frac{(x + 1 - \frac{1}{2x})^3 + 4}{3}. \end{aligned}$$

## 4. Decompositions of Ritt-twistable Laurent polynomials

In this section we study decompositions of the Laurent polynomials occurring in (1.5.1) and (1.5.2). Some of the results we prove will be used in the proofs of our main results. We also prove other results giving a full picture of the decompositions of these special Laurent polynomials, in view of the important role these examples play in the study of rational function analogues of Ritt's results.

Case (1.5.1) involves Laurent polynomials of the form $x^r q(x^n)$ and $x^r q(x)^n$, where $q \in \mathcal{L} \setminus \{0\}$ and $\gcd(r, n) = 1$. These are the natural Laurent polynomial analogues of the polynomials occurring in Ritt's results (which have the same shape but with $q \in \mathbb{C}[x]$). The Laurent polynomials in (1.5.2), however, have a different shape, namely $H_1 = (x - 1/x)p(x + 1/x)$ and $G_2 = (x^2 - 4)p(x)^2$, with $p \in \mathbb{C}[x] \setminus \{0\}$. We now show that there are linear changes of variables which transform $H_2$ and $G_2$ into the same general shape as the previous Laurent polynomials, namely $xq(x^2)$ and $xq(x)^2$, although here we must allow $q$ to be a rational function that is not in $\mathcal{L}$. Specifically, if we put

$$q = 4i\frac{p(2\frac{x-1}{x+1})}{x+1}, \tag{4.1.1}$$

then

$$xq(x^2) = H_1 \circ \frac{x+i}{x-i} \tag{4.1.2}$$

$$xq(x)^2 = G_2 \circ \frac{2x-2}{x+1}. \tag{4.1.3}$$

It is shown in [23] that a polynomial of the form $x^r q(x^n)$ (with $\gcd(r, n) = 1$) can only decompose into polynomials of the same shape (composed with linears), and likewise for $x^r q(x)^n$. We will prove the analogous result for Laurent polynomials; the corresponding assertion is not generally true when $q$ is one of the rational functions in (4.1.1), but nevertheless we determine all decompositions in this situation. We remark (cf. [19]) that Ritt's original

$A_4$ example (after linear changes) provides an example of an 'odd' rational function $xq(x^2)$ which can be written as the composition of two rational functions that are not linear changes of odd rational functions; similar examples occur for $q$ as in (4.1.1).

**Proposition 4.2.** *Let $n, r \in \mathbb{Z}$ satisfy $n > 1$ and $\gcd(n, r) = 1$, and pick $p \in \mathbb{C}[x]$ with $x \nmid p$. Suppose $g, h \in \mathbb{C}(x)$ satisfy $g \circ h = x^r p(x)^n$. Then there is a degree-one $\mu \in \mathbb{C}(x)$ such that $g \circ \mu = x^i G^n$ and $\mu^{-1} \circ h = x^j H^n$ for some $\delta \in \mathbb{C}$, some $i, j \in \mathbb{Z}$, and some $G, H \in \mathbb{C}[x]$.*

*Proof.* If $r \geq 0$ then $x^r p(x)^n$ is a polynomial, in which case the result is proved in [23] if $g, h \in \mathbb{C}[x]$, and the general case follows from Lemma 2.3. Henceforth assume $r < 0$.

By Lemma 2.1, after replacing $g$ and $h$ by $g \circ \mu$ and $\mu^{-1} \circ h$ for suitable degree-one $\mu \in \mathbb{C}(x)$, we may assume $g, h \in \mathcal{L}$ and either $g \in \mathbb{C}[x]$ or $h = x^m$ with $m \in \mathbb{Z}_{>0}$. First suppose $h = x^m$. Letting $\zeta$ be a primitive $m^{\text{th}}$ root of unity, we have $g \circ h(\zeta x) = g \circ h(x)$, so $\zeta^r x^r p(\zeta x)^n = x^r p(x)^n$. Thus $p(\zeta x)$ is a constant times $p(x)$, so $p = x^s G(x^m)$ with $G \in \mathbb{C}[x]$ and $x \in \mathbb{Z}_{\geq 0}$. Since $x^r p(x)^n = g \circ x^m$, we have $r + ns = mi$ with $i \in \mathbb{Z}_{\geq 0}$, so $g = x^i G(x)^n$. Putting $j = m$ and $H = 1$ gives the desired conclusion. Henceforth assume $g \in \mathbb{C}[x]$.

Write $h = A/x^s$ where $s \in \mathbb{Z}_{>0}$ and $A \in \mathbb{C}[x]$ with $x \nmid A$. Write $g = \theta \prod_\alpha (x - \alpha)^{n_\alpha}$, where the $\alpha$ are the distinct complex roots of $g$ (and $n_\alpha \in \mathbb{Z}_{>0}$ and $\theta \in \mathbb{C}^*$). Then $x^r p(x)^n = \theta \prod_\alpha (A - \alpha x^s)^{n_\alpha} / x^{s \sum_\alpha n_\alpha}$. Note that each $p_\alpha := A - \alpha x^s$ is a polynomial, and no two $p_\alpha$'s have a common root, and $x = 0$ is not a root of any $p_\alpha$. Thus, for each $\alpha$, every root of $p_\alpha^{n_\alpha}$ has multiplicity divisible by $n$, so every root of $p_\alpha$ has multiplicity divisible by $n/\gcd(n, n_\alpha)$.

Suppose $\alpha, \beta$ are distinct roots of $g$ such that neither $n_\alpha$ nor $n_\beta$ is divisible by $n$. Then $A - \alpha x^s = a^i$ and $A - \beta x^s = b^j$ where $a, b \in \mathbb{C}[x]$ and $i, j > 1$ are divisors of $n$. Thus $a^i - b^j = (\beta - \alpha)x^s$, so $\widehat{a} := a(x^i)/(\beta - \alpha)^{1/i}$ and $\widehat{b} := b(x^i)/(\beta - \alpha)^{1/j}$ satisfy $\widehat{a}^i - \widehat{b}^j = x^{is}$. Note that $x \nmid \widehat{a}\widehat{b}$. Now

$$\widehat{b}^j = \widehat{a}^i - (x^s)^i = \prod_{\zeta^i = 1} (\widehat{a} - \zeta x^s),$$

and the various polynomials $\widehat{a} - \zeta x^s$ are coprime (since $x \nmid \widehat{a}$), so for each $\zeta$ we have $\widehat{a} - \zeta x^s = A_\zeta^j$ for some $A_\zeta \in \mathbb{C}[x]$. Moreover, we may assume that $\widehat{b} = \prod_\zeta A_\zeta$. Pick some $\zeta \neq 1$ with $\zeta^i = 1$. Since $x \nmid \widehat{a}$, we have $x \nmid A_1 A_\zeta$ and $\gcd(A_1, A_\zeta) = 1$. But

$$\prod_{\xi^j = 1} (A_1 - \xi A_\zeta) = A_1^j - A_\zeta^j = (\zeta - 1)x^s,$$

and any two polynomials $A_1 - \xi A_\zeta$ are coprime, so every $A_1 - \xi A_\zeta$ is an $s^{\text{th}}$ power. Since each of these polynomials divides $x^s$, it follows that one of them is a constant times $x^s$, and the rest are constants. But since at least one of $A_1$ and $A_\zeta$ is nonconstant, there is at most one $\xi$ for which $A_1 - \xi A_\zeta$ is constant, whence $j = 2$. Similarly $i = 2$, so $\zeta = -1$. Solving for $A_1$ and $A_\zeta$, and then $\widehat{a}$ and $\widehat{b}$, we find that $a = \gamma + \delta x^s$ and $b = \pm(\gamma - \delta x^s)$ for some $\gamma, \delta \in \mathbb{C}^*$. Since $a^2 - b^2 = (\beta - \alpha)x^s$, we have $4\gamma\delta = \beta - \alpha$; moreover, $A = \alpha x^s + a^2 = \delta^2 x^{2s} + (\beta + \alpha)x^s/2 + \gamma^2$. Conversely, given $A$ and $s$, this last equation determines the values of $\alpha + \beta$, $\gamma^2$, and $\delta^2$, and hence also $16\gamma^2\delta^2 = (\beta - \alpha)^2 = (\alpha + \beta)^2 - 4\alpha\beta$ and finally $\alpha\beta$. Thus $A$ and $s$ uniquely determine the set $\{\alpha, \beta\}$. It follows that $n \mid n_\chi$ for every root $\chi$ of $g$ besides $\alpha$ and $\beta$, whence $g = ((x - \alpha)(x - \beta)p^2)^{n/2}$ for some $p \in \mathbb{C}[x]$. But then $n \mid \deg(g)$, so the order of the pole of $x^r p^n$ at $x = 0$ is divisible by $n$, but this order is $-r$, contradiction.

This last argument also implies that $g$ is not an $n^{\text{th}}$ power, so $g$ has a unique root $\alpha$ for which $n \nmid n_\alpha$. Moreover, for this $\alpha$ we have $\gcd(n, n_\alpha) = 1$. Thus $g = (x - \alpha)^{n_\alpha} G^n$ for some $G \in \mathbb{C}[x]$, and $A - \alpha x^s = H^n$ for some $H \in \mathbb{C}[x]$, whence $h = -\alpha + H^n/x^s$, as desired. □

To determine the decompositions of Laurent polynomials of the form $x^r p(x^n)$, we use the following result of Avanzi and Zannier [2, §5]:

**Proposition 4.3** (Avanzi–Zannier)**.** *Let $g \in \mathbb{C}[x]$ be indecomposable, and suppose $h_1, h_2 \in \mathbb{C}(x) \setminus \mathbb{C}$ satisfy $g \circ h_1 = \gamma g \circ h_2$ where $\gamma \in \mathbb{C}^* \setminus \{1\}$. Then $(g, h_1, h_2) = (\theta G \circ \mu,\ \mu^{-1} \circ H_1 \circ H,\ \mu^{-1} \circ H_2 \circ H)$ where $\theta \in \mathbb{C}^*$, $\mu \in \mathbb{C}[x]$ is linear, $H \in \mathbb{C}(x) \setminus \mathbb{C}$, and one of the following occurs:*

(4.3.1) *$H_2 = x$, $H_1 = \delta x$, and $G \in x^r\mathbb{C}[x^n]$, where $r \in \mathbb{Z}_{>0}$, $\delta^r = \gamma$, $n \in \mathbb{Z}_{\geq 0}$, and $\delta^n = 1$;*

(4.3.2) *$G = D_n$ with $n$ an odd prime, $\gamma = -1$, $H_1 = x + 1/x$, and $H_2 = H_1 \circ \delta x$ where $\delta^n = -1$;*

(4.3.3) *$H_1 = (1 - \delta x^m)/(\delta x^{m+n} - 1)$, $H_2 = -1 + (x^n - 1)/(\delta x^{m+n} - 1)$, and $G = x^m(x + 1)^n$, where $m, n \in \mathbb{Z}_{>0}$ are coprime and $\delta^n = \gamma$;*

(4.3.4) *$G = D_3(x) + \delta$, where $\delta \in \mathbb{C} \setminus \{0, 2, -2\}$ and either*
  (i) *$\gamma = (\delta + 2)/(\delta - 2)$, $H_1 = -1 + 3(\gamma x^2 + 1)/(\gamma x^3 + 1)$, and $H_2 = -2 + 3(1 - x)/(\gamma x^3 + 1)$; or*
  (ii) *$\gamma = (\delta - 2)/(\delta + 2)$, $H_1 = -2 + 3\gamma(1 - x)/(x^3 + \gamma)$, and $H_2 = -1 + 3(x^2 + \gamma)/(x^3 + \gamma)$;*

(4.3.5) *$G = x^4 - \frac{4}{3}(\alpha + 1)x^3 + 2\alpha x^2$, $H_1 = \frac{(E-\alpha)(E-\frac{1}{\alpha})(x-\frac{6\alpha}{x})+4(\alpha+1)(E^3+1)}{6(E^4+1)}$, and $H_2 = EH_1$, where $\gamma = -1$, $\alpha^4 + 1 = 2(\alpha^3 + \alpha)$, and*

$$E = \frac{-1}{2\sqrt{2(2\alpha^2 - 5\alpha + 2)}}\left(x + \frac{6\alpha}{x}\right) - \left(\alpha + \frac{1}{\alpha}\right);$$

(4.3.6) *$G = x^4 - \frac{4}{3}(\alpha + \beta)x^3 + 2\alpha\beta x^2 + 1$, where $\omega = e^{2\pi i/3}$, $\gamma \in \{\omega, \omega^2\}$, $(\alpha + \omega^2)^3 = -2$, and $\beta = (1 - \alpha)\omega - 1$; if $\gamma = \omega$ then $H_2 = \omega^2(H_1 - \alpha)E$ and*

$$H_1 = \frac{(E^2 + pE + \frac{i}{\sqrt{3}}\alpha^2 - w(\alpha - 1))U + \frac{2i}{\sqrt{3}}((\alpha - 1)E^3 - \omega(\alpha - \omega))}{E^4 - 1} + \alpha,$$

*where* $E = (x - \delta/x)/2 + p$ *and* $U = (x + \delta/x)/(2\sqrt{-3(\alpha - 1)/2})$ *with* $p = -\frac{i\omega}{\sqrt{3}}\alpha^2 - \omega(\alpha - 1)$ *and* $\delta = -\omega(\alpha^2 - i\sqrt{3}\alpha + 3\omega)$*; if* $\gamma = \omega^2$ *then exchange the above* $H_1$ *and* $H_2$*;*

(4.3.7) $G = x(x + \alpha)^2(x + 1)^2$ *and* $H_2 = -Z^2H_1$*, where* $\gamma = -1$ *and* $Z := (x - \frac{251+7\xi}{x} + 6 - 2\xi)/32$ *with* $\xi^2 + \xi + 4 = 0$ *and* $\alpha^2 - \frac{22+5\xi}{9}\alpha + 1 = 0$*, and*

$$H_1 = \frac{(\alpha + 1)(Z^3 + 1) + (\alpha - 1)(Z^2 - \xi Z + 1)U}{2(Z^5 - 1)}$$

*with* $U := (x + \frac{251+7\xi}{x})/32$*.*

*Remark.* In the above statement we have implicitly made several corrections to the results stated in [2]. Specifically, in the definition of $P_4$ in [2], the equation for $\xi$ should be $\xi^2 - 2\xi - 2 = 0$. Our other corrections refer to [2, Prop. 5.6]. In cases (1) and (3) of that result, $g_1$ and $h_1$ should be switched; in case (8), $U$ should be replaced by $U/16$; and in case (7), the sign preceding $2/3$ in the expression for $g_1$ should be '+', and also an additional comment must be made for the case $c = \omega^2$. We also combined case (1) of [2, Prop. 5.2, 5.6] with case (3), and we combined case (2) with cases (3) and (4).

Avanzi and Zannier [2, Thm. 2] generalized Proposition 4.3 to the case of decomposable $g$, obtaining a recursive description of the possible polynomials $g$. In case the genus-zero factor can be parametrized by Laurent polynomials, we require the following non-recursive description.

**Proposition 4.4.** *Let* $g \in \mathbb{C}[x]$ *satisfy* $\deg(g) > 1$*, and let* $h_1, h_2 \in \mathcal{L} \setminus \mathbb{C}$ *and* $\gamma \in \mathbb{C} \setminus \{1\}$ *satisfy* $g \circ h_1 = \gamma g \circ h_2$*. Then, after replacing* $(g, h_1, h_2)$ *by* $(g \circ \mu,\ \mu^{-1} \circ h_1 \circ \theta x,\ \mu^{-1} \circ h_2 \circ \theta x)$ *for some* $\theta \in \mathbb{C}^*$ *and some linear* $\mu \in \mathbb{C}[x]$*, one of the following holds (where* $n \in \mathbb{Z}_{\geq 0}$ *and* $r, m \in \mathbb{Z}_{>0}$*):*

(4.4.1) $h_1 = \alpha h_2$ *and* $g \in x^r\mathbb{C}[x^n]$*, where* $\alpha^n = 1$ *and* $\alpha^r = \gamma$*;*

(4.4.2) $h_1 = x^m + 1/x^m$*,* $h_2 = h_1 \circ \alpha x$*, and* $g = G \circ D_n$*, where* $\gamma = -1$*,* $G \in x\mathbb{C}[x^2]$*, and* $\alpha^{nm} = -1$*;*

(4.4.3) $h_1 = x^m + 1/x^m$*,* $h_2 = (x^m - 1/x^m)/\sqrt{\alpha}$*, and* $g = G \circ (\frac{(1-\alpha)x^2}{2} - 2)$*, where* $G \in x^r\mathbb{C}[x^n]$*,* $\alpha^r = \gamma$*, and* $\alpha^n = 1$ *but* $\alpha \neq -1$*.*

*Proof.* Write $g = g_1 \circ \dots \circ g_s$ where the $g_i$ are indecomposable polynomials. Let $j$ be the largest integer $\leq s$ for which $H_1 := g_{j+1} \circ \dots \circ g_s \circ h_1$ and $H_2 := g_{j+1} \circ \dots \circ g_s \circ h_2$ satisfy $g_j \circ H_1 = \nu \circ g_j \circ H_2$ for some linear $\nu \in \mathbb{C}[x]$, and put $G = g_1 \circ \dots \circ g_{j-1}$. Writing $\nu(x) = \alpha x + \beta$ and comparing leading coefficients in the identity $G \circ \nu = \gamma G$, we see that $\alpha^{\deg(G)} = \gamma \neq 1$, so $\alpha \neq 1$. Now put $\lambda := x + \beta/(\alpha - 1)$, so $\lambda \circ \nu = \alpha\lambda$; replacing $G$ and $g_j$ by $G \circ \lambda^{-1}$ and $\lambda \circ g_j$, we have $g_j \circ H_1 = \alpha g_j \circ H_2$, so $G(\alpha x) = \gamma G(x)$. Hence $G \in x^r\mathbb{C}[x^n]$ for some $r > 0$ and $n \geq 0$ such that $\alpha^n = 1$ and $\alpha^r = \gamma$. If $h_1 = \widehat{\nu} \circ h_2$ with $\widehat{\nu} \in \mathbb{C}[x]$ linear, then this argument shows that (4.4.1) holds. Henceforth assume there is no such $\widehat{\nu}$, so there is no linear $\widehat{\nu} \in \mathbb{C}[x]$ such that $H_1 = \widehat{\nu} \circ H_2$.

By Proposition 4.3, there exist $\widehat{\theta} \in \mathbb{C}^*$, $H \in \mathbb{C}(x) \setminus \mathbb{C}$, and a linear $\mu\mathbb{C}[x]$ such that

$$\begin{aligned} g_j &= \widehat{\theta}\widehat{g_j} \circ \widehat{\mu} \\ H_1 &= \widehat{\mu}^{-1} \circ \widehat{H_1} \circ H \\ H_2 &= \widehat{\mu}^{-1} \circ \widehat{H_2} \circ H, \end{aligned}$$

where $\widehat{g_j}$, $\widehat{H_1}$, and $\widehat{H_2}$ satisfy the conditions required of $G$, $H_1$, and $H_2$ in one of (4.3.1)–(4.3.7). By replacing $G$ by $G \circ \widehat{\theta}x$, we may replace $g_j$ by $\widehat{g_j}$ while also replacing $H_1$ and $H_2$ by $\widehat{H_1} \circ H$ and $\widehat{H_2} \circ H$.

Since $H_1, H_2 \in \mathcal{L}$ have at most two poles, also $\widehat{H_1}$ and $\widehat{H_2}$ have at most two poles. This rules out (4.3.4)–(4.3.7). In (4.3.3) it implies $m = n = 1$, so $g_j = x^2 + x$, $\widehat{H_1} = (1 - \alpha x)/(\alpha x^2 - 1)$ and $\widehat{H_2} = (x - \alpha x^2)/(\alpha x^2 - 1)$. Putting

$$\mu_1 = \frac{4x+2}{\sqrt{1-\alpha}} \quad \text{and} \quad \mu_2 = \frac{1}{\sqrt{\alpha}} \frac{x(1+\sqrt{\alpha}) + \sqrt{1-\alpha}}{x(1+\sqrt{\alpha}) - \sqrt{1-\alpha}},$$

we have

$$\begin{aligned} 8g_j \circ \mu_1^{-1} &= \frac{1-\alpha}{2}x^2 - 2 \\ \mu_1 \circ \widehat{H_1} \circ \mu_2 &= x + \frac{1}{x} \\ \mu_1 \circ \widehat{H_2} \circ \mu_2 &= \frac{1}{\sqrt{\alpha}}\left(x - \frac{1}{x}\right). \end{aligned}$$

Now replace $G$ by $G \circ 8x$ and $g_j$ by $g_j \circ \mu_1^{-1}$, while also replacing $\widehat{H_1}$ and $\widehat{H_2}$ by $\mu_1 \circ \widehat{H_1} \circ \mu_2$ and $\mu_2 \circ \widehat{H_2} \circ \mu_2$ (and replacing $H$ by $\mu_2^{-1} \circ H$). Thus we have $g_j = \frac{1-\alpha}{2}x^2 - 2$, $\widehat{H_1} = x + x^{-1}$, and $\widehat{H_2} = (x - x^{-1})/\sqrt{\alpha}$. Since $H_1 = \widehat{H_1} \circ H$ has no poles besides 0 and $\infty$, and $\widehat{H_1}$ has poles at 0 and $\infty$, the full $H$-preimage of $\{0, \infty\}$ is $\{0, \infty\}$, so $H = (\theta x)^m$ for some nonzero $m \in \mathbb{Z}$ and $\theta \in \mathbb{C}^*$. If $m < 0$ then replace $H$ by $(\theta x)^{-m}$ and $\widehat{H_2}$ by $-\widehat{H_2}$, thereby preserving the compositions $\widehat{H_1} \circ H$ and $\widehat{H_2} \circ H$. Thus we may assume $m > 0$ by making the appropriate choice of $\sqrt{\alpha}$. Now $H_1 = \widehat{H_1} \circ H = (x^m + x^{-m}) \circ \theta x$ and $H_2 = (x^m - x^{-m})/\sqrt{\alpha} \circ \theta x$. Write $R = g_{j+1} \circ \cdots \circ g_s$, so

$$\begin{aligned} R \circ h_1 = H_1 &= \left(x^m + \frac{1}{x^m}\right) \circ \theta x \\ R \circ h_2 = H_2 &= \frac{1}{\sqrt{\alpha}}\left(x^m - \frac{1}{x^m}\right) \circ \theta x. \end{aligned}$$

By Lemma 3.1, we have $R = D_{m/d} \circ \mu$ where $d \mid m$ and $\mu \in \mathbb{C}[x]$ is linear; moreover, $h_1 = \mu^{-1} \circ (x^d + 1/x^d) \circ \theta x$. Since $R \circ h_2 = \frac{x^m + x^{-m}}{i\sqrt{\alpha}} \circ \theta i^{1/m} x$, Lemma 3.1 implies that $R = D_{m/d}(x)/(i\sqrt{\alpha}) \circ \tilde{\mu}$ and $h_2 = \tilde{\mu}^{-1} \circ (x^d + x^{-d}) \circ \theta i^{1/m} x$ for some linear $\tilde{\mu} \in \mathbb{C}[x]$. Equating coefficients in the identity

$D_{m/d}\circ\mu = R = D_{m/d}/(i\sqrt{\alpha})\circ\tilde{\mu}$, we see that either $\alpha = -1$ or $m = d$. If $m = d$ then $g = G\circ g_j\circ\mu$ and $h_1 = \mu^{-1}\circ(x^m + x^{-m})\circ\theta x$ and $h_2 = \mu^{-1}\circ(x^m - x^{-m})/\sqrt{\alpha}\circ\theta x$, as in (4.4.3). Now assume $m \neq d$, so $\alpha = -1$, whence $g_j = D_2$. Replacing $g$, $h_1$ and $h_2$ by $g\circ\mu^{-1}$, $\mu\circ h_1\circ x/\theta$, and $\mu\circ h_2\circ x/\theta$, we have $g = G\circ D_{2m/d}$ and $h_1 = x^d + x^{-d}$ and $h_2 = \pm h_1\circ i^{1/m}x$. Thus $h_2 = h_1\circ\widehat{\alpha}x$ where $\widehat{\alpha}^{2m} = -1$, and we have obtained (4.4.2) with $n = 2$.

Now assume $g_j$, $\widehat{H_1}$ and $\widehat{H_2}$ satisfy (4.3.1). Then $\widehat{H_1} = \delta x$ and $\widehat{H_2} = x$ for some $\delta\in\mathbb{C}^*$, so $H_1 = \widehat{H_1}\circ H = \delta H_2$, contradicting our hypothesis to the contrary.

Finally, assume $g_j$, $\widehat{H_1}$ and $\widehat{H_2}$ satisfy (4.3.3). Thus $\alpha = -1$ and $g_j = D_p$ with $p$ an odd prime, and moreover $\widehat{H_1} = x + 1/x$ and $\widehat{H_2} = \widehat{H_1}\circ\delta x$ where $\delta^p = -1$. Since $H_1 = \widehat{H_1}\circ H$ is a Laurent polynomial, we must have $H = (\theta x)^m$ for some nonzero $m\in\mathbb{Z}$ and $\theta\in\mathbb{C}^*$. If $m < 0$ then we can replace $m$ by $-m$ if we replace $\delta$ and $\theta$ by $1/\delta$ and $1/\theta$; since these changes do not affect $H_1$ or $H_2$, we may assume $m > 0$. Write $R = g_{j+1}\circ\cdots\circ g_s$, so $R\circ h_1 = (x + 1/x)\circ(\theta x)^m$ and $R\circ h_2 = (x+1/x)\circ\delta(\theta x)^m$. By Lemma 3.1, we have $R = D_{m/d}\circ\mu$ where $d \mid m$ and $\mu\in\mathbb{C}[x]$ is linear; moreover, $h_1 = \mu^{-1}\circ(x^d + 1/x^d)\circ\theta x$. Likewise $R = D_{m/d}\circ\tilde{\mu}$ for some linear $\tilde{\mu}\in\mathbb{C}[x]$, and moreover $h_2 = \tilde{\mu}^{-1}\circ(x^d + 1/x^d)\circ x\theta\delta^{1/m}$. The identity $D_{m/d}\circ\mu = R = D_{m/d}\circ\tilde{\mu}$ implies that $\tilde{\mu} = \epsilon\mu$ with $\epsilon\in\{1,-1\}$ and $\epsilon^{m/d} = 1$. After replacing $g$, $h_1$ and $h_2$ by $g\circ\mu^{-1}$, $\mu\circ h_1\circ x/\theta$, and $\mu\circ h_2\circ x/\theta$, we have $g = G\circ D_{pm/d}$ and $h_1 = x^d + 1/x^d$ and $h_2 = \epsilon h_1\circ x\delta^{1/m}$, so $h_2 = h_1\circ\widehat{\alpha}x$ where $\widehat{\alpha}^{mp} = -1$. Thus we have (4.4.2). □

We can now describe the decompositions of Laurent polynomials of the form $x^r p(x^n)$:

**Proposition 4.5.** *Let $n, r\in\mathbb{Z}$ satisfy $n > 1$ and $n\nmid r$, and pick $p\in\mathbb{C}[x]$ with $x\nmid p$. Suppose $g, h\in\mathbb{C}(x)$ satisfy $g\circ h = x^r p(x^n)$. Then there is a degree-one $\mu\in\mathbb{C}(x)$ such that, after replacing $g$ and $h$ by $g\circ\mu$ and $\mu^{-1}\circ h$, one of the following occurs (with $s, t, m\in\mathbb{Z}$ and $m > 0$):*

(4.5.1) *$g\in x^s\mathbb{C}[x^m]$ and $h\in x^t\mathbb{C}[x^n]$ where $n\mid mt$;*

(4.5.2) *$g = G\circ D_t$ and $h = (x^m + 1/x^m)\circ\theta x$ where $G\in x\mathbb{C}[x^2]$ and $mt\equiv r\equiv n/2 \pmod n$, with $n$ even, $t > 0$, and $\theta\in\mathbb{C}^*$.*

*Moreover, if $g\in\mathbb{C}[x]$ and $h\in\mathcal{L}$ then we may choose mu $\in\mathbb{C}[x]$.*

*Proof.* By Lemma 2.1, we may assume $g, h\in\mathcal{L}$ and either $g\in\mathbb{C}[x]$ or $h = x^t$ with $t\in\mathbb{Z}_{>0}$. In the latter case the condition $x^r p(x^n)\in\mathbb{C}[x^t]$ implies $t\mid r$ and $p = P(x^{t/\gcd(n,t)})$ with $P\in\mathbb{C}[x]$. Thus $g = x^{r/t}P(x^{n/\gcd(n,t)})$, as in (4.5.1). Henceforth assume $g\in\mathbb{C}[x]$. If $\deg(g) = 1$ then we may assume $g = x$, so again (4.5.1) holds. Now assume $\deg(g) > 1$.

Let $\zeta$ be a primitive $n^{\text{th}}$ root of unity. Then $g\circ h(\zeta x) = \zeta^r g\circ h(x)$, and $\gamma := \zeta^r \neq 1$. Write $h_2 := h(x)$ and $h_1 := h(\zeta x)$, so $g\circ h_1 = \gamma g\circ h_2$. By Proposition 4.4, there exist $\theta\in\mathbb{C}^*$ and a linear $\mu\in\mathbb{C}[x]$ such that, after replacing $g, h_1, h_2$ by $g \circ \mu$, $\mu^{-1} \circ h_1 \circ \theta x$, and $\mu^{-1} \circ h_2 \circ \theta x$, one of (4.4.1)–(4.4.3) holds. We will use the equation $h_1 = h_2 \circ \zeta x$ to analyze these possibilities.

If (4.4.1) holds then $\alpha h_2 = h_1 = h_2 \circ \zeta x$, so $h_2 \in x^t\mathbb{C}[x^n]$ with $\zeta^t = \alpha$; here also $g \in x^s\mathbb{C}[x^m]$ where $\alpha^m = 1$ and $\alpha^s = \gamma$. Thus $\zeta^{tm} = 1$, so we have (4.5.1).

If (4.4.2) holds then

$$x^m + \frac{1}{x^m} = h_1 = h_2 \circ \zeta x = \left(x^m + \frac{1}{x^m}\right) \circ \alpha\zeta x,$$

so $(\alpha\zeta)^m = 1$. Here $g = G \circ D_t$ where $\gamma = -1$ and $G \in x\mathbb{C}[x^2]$, and $\alpha^{mt} = -1$. Thus $\zeta^{mt} = -1$, and we have (4.5.2).

If (4.4.3) holds then, for some $\alpha \neq -1$, we have

$$x^m + \frac{1}{x^m} = h_1 = h_2 \circ \zeta x = \frac{1}{\sqrt{\alpha}}\left(x^m - \frac{1}{x^m}\right) \circ \zeta x,$$

so $\zeta^m = \sqrt{\alpha} = -1/\zeta^m$. But then $\alpha = \zeta^{2m} = -1$, contradiction. □

Next we consider decompositions of $(x^2-4)p(x)^2$ with $p \in \mathbb{C}[x]$; since these are polynomials, Ritt's results provide information about their decompositions, but we go further by precisely describing the shape of every decomposition:

**Proposition 4.6.** *Let $g, h, p \in \mathbb{C}[x]\setminus\{0\}$ satisfy $g \circ h = (x^2-4)p(x)^2$. Then, after replacing $g$ and $h$ by $g \circ \mu$ and $\mu^{-1} \circ h$ for some linear $\mu \in \mathbb{C}[x]$, there exist $B, D \in \mathbb{C}[x]$ and $n \in \mathbb{Z}_{>0}$ such that one of the following holds:*

(4.6.1) $g = xB^2$ *and* $h = (x^2-4)D^2$*;*

(4.6.2) $g = (x^2-4)B^2$ *and* $h = D_n$*.*

*Remark.* To verify that the polynomials $g$ and $h$ in (4.6.2) satisfy $g \circ h = (x^2-4)p(x)^2$ for suitable $p$, note that $D_n^2 - 4 = (x^2-4)E_{n-1}^2$, where the polynomial $E_{n-1}$ is a 'Dickson polynomial of the second kind', and is defined by the functional equation $E_{n-1}(x + x^{-1}) = (x^n - x^{-n})/(x - x^{-1})$.

*Proof of Proposition 4.6.* Write $g = AB^2$ and $h = CD^2$ with $A, B, C, D \in \mathbb{C}[x]$ and $A, C$ squarefree and monic. Then $(x^2-4)p(x)^2 = A(h) \cdot B(h)^2$, so $A(h)$ is a square times $x^2-4$. Write $A(x) = \prod_\alpha (x-\alpha)$, where the product ranges over the roots of $A$, and write $h - \alpha = E_\alpha^2 F_\alpha$ with $E_\alpha, F_\alpha \in \mathbb{C}[x]$ and $F_\alpha$ squarefree and monic. For distinct roots $\alpha, \alpha'$ of $A$, plainly $h-\alpha$ and $h-\alpha'$ are coprime, so $\gcd(E_\alpha, E_{\alpha'}) = 1 = \gcd(F_\alpha, F_{\alpha'})$. Since $A(h) = \prod_\alpha E_\alpha^2 F_\alpha$ is a square times $x^2-4$, and the various polynomials $F_\alpha$ are monic, squarefree and coprime, we have $x^2-4 = \prod_\alpha F_\alpha$. Moreover, differentiating the equation $h - \alpha = E_\alpha^2 F_\alpha$ implies $E_\alpha \mid h'$, and since the various polynomials $E_\alpha$ are coprime, we have $\prod_\alpha E_\alpha \mid h'$. Writing $n = \deg(h)$ and $r = \deg(A)$, it follows that $n - 1 \geq \sum_\alpha \deg(E_\alpha)$, and since

$$nr = \deg(h \circ A) = \sum_\alpha \deg(h-\alpha) = 2 + 2\sum_\alpha \deg(E_\alpha),$$

we conclude that $r \leq 2$. If $r = 1$ then, after replacing $g$ and $h$ by $g \circ \mu$ and $\mu^{-1} \circ h$ for a suitable linear $\mu \in \mathbb{C}[x]$, we may assume $A = x$; but then $C = F_0 = x^2 - 4$, so we have (4.6.1). Now assume $r = 2$, so, after inserting a linear and its inverse between $g$ and $h$ as above, we may assume $A = x^2 - 4$. There are four possibilities:

(i) $F_2 = x^2 - 4$ and $F_{-2} = 1$;
(ii) $F_2 = x - 2$ and $F_{-2} = x + 2$;
(iii) $F_2 = x + 2$ and $F_{-2} = x - 2$; or
(iv) $F_2 = 1$ and $F_{-2} = x^2 - 4$.

By replacing $g$ and $h$ by $g \circ (-x)$ and $(-x) \circ h$, we may assume that (i) or (ii) holds. In either case, the cover $h : \mathbb{P}^1 \to \mathbb{P}^1$ is totally ramified over $\infty$, and every point lying over 2 or $-2$ has even ramification index except 2 and $-2$. This data determines $h$ up to composition on both sides with linears, as was first shown by Ritt [28], and as has been reproved in every proof of Ritt's results. Thus, $h = \nu_1 \circ D_n \circ \nu_2$ for some linear $\nu_1, \nu_2 \in \mathbb{C}[x]$. In case (ii) we have $h - 2 = (x - 2)E_2^2$, so $n$ is odd; if $n = 1$ then $E_2$ is a constant, and since $(x + 2) \mid (h + 2)$ we must have $E_2 = \pm 1$, so $h = x$ and (4.6.2) holds. If (ii) holds with $n > 1$ then 2 and $-2$ are the unique finite branch points of $h : \mathbb{P}^1 \to \mathbb{P}^1$, and their unique unramified preimages are 2 and $-2$, respectively. Since $D_n$ has the same property, each $\nu_i$ preserves $\{2, -2\}$, hence equals $\pm x$, and we must have $\nu_2 = \nu_1$. Since $-D_n(-x) = D_n(x)$, this gives (4.6.2). In case (i), $n$ is even; if $n = 2$ then $-2$ is the unique finite branch point of both $h$ and $D_n$, so $\nu_1$ fixes $-2$ and thus $\nu_1 = -2 + \beta \cdot (x + 2)$. Since $h(\pm 2) = 2$ and $D_2 = x^2 - 2$, we find that $\nu_2 = \alpha x$ where $\beta = 1/\alpha^2$, which implies $h = D_2$ as desired. Now suppose $n > 2$. Then both $h$ and $D_n$ have 2 and $-2$ as their unique finite branch points, and all of their preimages are ramified except for $\pm 2$, both of which lie over 2. Thus $\nu_1$ fixes 2 and $-2$, so $\nu_1 = x$. Also $\nu_2$ preserves $\{2, -2\}$, so $\nu_2 = \pm x$, whence $h = D_n$. □

Finally, we determine the decompositions of the other Laurent polynomials in (1.5.2), namely $(x - 1/x) \cdot p(x + 1/x)$ with $p \in \mathbb{C}[x]$. As we noted in (4.1.1), composition with a degree-one rational function transforms these into the form $xq(x^2)$, but the resulting $q \in \mathbb{C}(x)$ is not a Laurent polynomial.

**Proposition 4.7.** *Let $g, p \in \mathbb{C}[x]$ and $h \in \mathcal{L}$ satisfy $p \neq 0$ and $g \circ h = (x - 1/x) \cdot p(x + 1/x)$. Then there exist $\mu, q \in \mathbb{C}[x]$ with $\mu$ linear such that one of the following holds:*

(4.7.1) $\mu^{-1} \circ h = (x - 1/x) \cdot q(x + 1/x)$ *and* $g \circ \mu \in x\mathbb{C}[x^2]$ *is an odd polynomial;*
(4.7.2) $\mu^{-1} \circ h = \frac{x^m}{\sqrt{\gamma}} + \frac{\sqrt{\gamma}}{x^m}$ *and* $g \circ \mu = G \circ D_n$ *with* $G \in x\mathbb{C}[x^2]$ *and* $\gamma^n = -1$.

*Remark.* We note that the examples in (4.7.2) do satisfy the hypotheses: for, $f := g \circ h = G \circ D_n \circ (x + 1/x) \circ x^m/\sqrt{\gamma}$. Writing $I = \sqrt{\gamma}^n$, we have $I^2 = -1$, so $f = G \circ (x + 1/x) \circ Ix^{nm} = G \circ I(x - 1/x) \circ x^{nm}$. There is a polynomial $E_{nm-1}$ (the Dickson polynomial of the second kind) satisfying $(x - 1/x) \circ x^{nm} = (x - 1/x)E_{nm-1}(x + 1/x)$. Since $G$ is odd, it follows that $f(x) = (x - 1/x) \cdot p(x + 1/x)$ for some $p \in \mathbb{C}[x]$.

*Proof of Proposition 4.7.* Write $f = (x - 1/x) \cdot p(x + 1/x)$. Since $f(1/x) = -f(x)$ (and $f \in \mathcal{L}$), we can write $f(x) = F(x) - F(1/x)$ with $F \in x\mathbb{C}[x]$. Write the leading terms of $F$ and $g$ as $\beta x^s$ and $\theta x^r$. Viewing $f$ as a finite Laurent series, its highest and lowest-degree terms have degrees $s$ and $-s$, so we can write $h = \delta(x^e + \delta_1 x^{e-1} + \cdots + \delta_{e-1}x) + \xi + \zeta(x^{-e} + \zeta_1 x^{1-e} + \cdots + \zeta_{e-1}x^{-1})$ with $\delta, \zeta \in \mathbb{C}^*$ and $\delta_i, \zeta_i, \xi \in \mathbb{C}$, where $e = s/r$. Then $\delta^r = \beta/\theta = -\zeta^r$, and moreover the $\delta_i$ are uniquely determined by $F$, since the coefficients of $x^{s-1}, \dots, x^{s-e+1}$ in the congruence $(x^e + \delta_1 x^{e-1} + \cdots + \delta_{e-1}x)^r \equiv F/\beta \pmod{x^{s-e}}$ successively determine $\delta_1, \dots, \delta_{e-1}$. Since the $\zeta_i$ are determined by the same congruence, we have $\zeta_i = \delta_i$, whence $h = H(x) + \gamma H(1/x) + \xi$ with $H \in x\mathbb{C}[x]$ and $\gamma^r = -1$. Since $f(1/x) = -f(x)$, we have $g \circ h(x) = -g \circ h(1/x)$. By Proposition 4.4, there exist $\widehat{\theta} \in \mathbb{C}^*$ and a linear $\mu \in \mathbb{C}[x]$ such that one of (4.4.1)–(4.4.3) holds for $\widehat{g} := g \circ \mu$, $h_1 := \mu^{-1} \circ h \circ \widehat{\theta}x$, and $h_2 := \mu^{-1} \circ h \circ (\widehat{\theta}x)^{-1}$. Write $\widehat{H}(x) = \mu^{-1} \circ H(x) - \mu^{-1}(0)$, so $\widehat{H} \in x\mathbb{C}[x]$ and $h_1 = \widehat{H}(\widehat{\theta}x) + \gamma\widehat{H}(1/(\widehat{\theta}x)) + \mu^{-1}(\xi)$ and $h_2 = \widehat{H}(1/(\widehat{\theta}x)) + \gamma\widehat{H}(\widehat{\theta}x) + \mu^{-1}(\xi)$.

In case (4.4.1) we have $h_1 = \alpha h_2$, where $\alpha \neq 1$. Comparing the terms of highest and lowest degrees in this identity gives $\frac{1}{\alpha} \cdot \mu^{-1} = \mu^{-1} \circ \gamma x = \alpha \cdot \mu^{-1}$, so $\alpha = \gamma = -1$. Now (4.4.1) implies $\widehat{g} \in x\mathbb{C}[x^2]$. Since $h_1$ and $h_2 = -h_1$ both have constant term $\mu^{-1}(\xi)$, this term must be zero, so $h_1(x) = \widehat{H}(x) - \widehat{H}(1/x)$. Letting $\sigma$ be the automorphism of $\mathbb{C}(x)$ mapping $x \mapsto 1/x$, we see that $R := h_1(x)/(x - 1/x)$ is fixed by $\sigma$, and thus lies in the fixed field $\mathbb{C}(x)^\sigma = \mathbb{C}(x + 1/x)$. Thus $R = q(x + 1/x)$ for some $q \in \mathbb{C}(x)$. The only poles of $1/(x - 1/x)$ are 1 and $-1$, both of which have order 1; since $h_1(1) = h_1(-1) = 0$, neither 1 nor $-1$ is a pole of $R$, so $R$ has no poles besides 0 and $\infty$. Since $R = q(x + 1/x)$, and the images of 0 and $\infty$ under $x + 1/x$ are both $\infty$, it follows that $q$ has no poles besides $\infty$, so $q \in \mathbb{C}[x]$. This proves that (4.7.1) holds.

In cases (4.4.2) and (4.4.3) we have $h_1 = x^m + 1/x^m$, so $x^m = \widehat{H}(\widehat{\theta}x)$ and $1/x^m = \gamma\widehat{H}(\frac{1}{\widehat{\theta}x})$, whence $\widehat{H}(x) = (x/\widehat{\theta})^m$ and $\widehat{\theta}^{2m} = \gamma$. Thus $h_2 = x^m/\gamma + \gamma/x^m$, which is incompatible with (4.4.3), so (4.4.2) holds. Moreover, in (4.4.2) we must have $\alpha^m = 1/\gamma$, and $\widehat{g} = G \circ D_n$ where $G$ is an odd polynomial and $\alpha^{mn} = -1$. This yields (4.7.2). □

## 5. Laurent polynomials with two Type 1 decompositions

In this section we describe all instances of Laurent polynomials with two Type 1 decompositions. Our proofs make crucial use of a result of Bilu and Tichy [6, Thm. 9.3], whose proof relies on Ritt's results among other things. The statement of this result involves the general degree-$n$ Dickson polynomial $D_n(x, \alpha)$ (with $\alpha \in \mathbb{C}$), which is defined by the functional equation $D_n(z + \alpha/z, \alpha) = z^n + (\alpha/z)^n$ (in this notation, our previously defined $D_n(x)$ is $D_n(x, 1)$).

**Proposition 5.1** (Bilu–Tichy). *Let $g_1, g_2 \in \mathbb{C}[x] \setminus \mathbb{C}$, and let $E(x, y) \in \mathbb{C}[x, y]$ be a factor of $g_1(x) - g_2(y)$. Suppose that $E(x, y) = 0$ is an irreducible* *curve of genus* 0 *which has at most two closed points lying over $x=\infty$. Then $g_1 = G\circ G_1\circ\mu_1$ and $g_2 = G\circ G_2\circ\mu_2$, where $G,\mu_1,\mu_2\in\mathbb{C}[x]$ with $\mu_1,\mu_2$ linear, and where either $(G_1,G_2)$ or $(G_2,G_1)$ is in the following list (in which $p\in\mathbb{C}[x]$ is nonzero, $m,n$ are coprime positive integers, and $\alpha,\beta\in\mathbb{C}^*$):*

(5.1.1) $(x^n,\ \alpha x^r p(x)^n)$ *where* $0\le r<n$ *and* $\gcd(r,n)=1$*;*
(5.1.2) $(x^2,\ (\alpha x^2+\beta)p(x)^2)$*;*
(5.1.3) $(D_m(x,\alpha^n),\ D_n(x,\alpha^m))$*;*
(5.1.4) $(\alpha^{-m}D_{2m}(x,\alpha),\ -\beta^{-n}D_{2n}(x,\beta))$*;*
(5.1.5) $((\alpha x^2-1)^3,\ 3x^4-4x^3)$*;*
(5.1.6) $(D_{dm}(x,\alpha^n),\ -D_{dn}(x\cos(\pi/d),\alpha^m))$ *where* $d\ge 3$.

*Moreover, there exists $(G_1,G_2)$ as above such that $E(x,y)$ is a factor of $G_1\circ\mu_1(x)-G_2\circ\mu_2(y)$, and such that in all but the last case $E(x,y)$ is a constant times $G_1\circ\mu_1(x)-G_2\circ\mu_2(y)$.*

*Remark.* In the above result we have corrected an error from [6], namely that $a^{n/d}$ and $a^{m/d}$ should be switched in the definition of 'specific pairs' in [6] in order to make [6, Thm. 9.3] be true.

Actually Bilu and Tichy proved a version of this result for polynomials over an arbitrary field of characteristic zero; since we have restricted to the complex numbers, we can simplify the statement somewhat:

**Corollary 5.2.** *Proposition 5.1 remains true if we replace* (5.1.1)–(5.1.6) *by the following (where $m,n\in\mathbb{Z}_{>0}$ are coprime, and $p\in\mathbb{C}[x]$ is nonzero):*

(5.2.1) $(x^n,\ x^r p(x)^n)$ *where* $0\le r<n$ *and* $\gcd(r,n)=1$*;*
(5.2.2) $(x^2,\ (x^2-4)p(x)^2)$*;*
(5.2.3) $(D_m(x),\ D_n(x))$*;*
(5.2.4) $((x^2/3-1)^3,\ 3x^4-4x^3)$*;*
(5.2.5) $(D_{dm}(x),\ -D_{dn}(x))$ *where* $d>1$.

Before proving Corollary 5.2, we recall some basic properties of Dickson polynomials. These follow readily from the definition; for details, and further results, see [1, 18].

$$D_1(x,\alpha)=x;\quad D_2(x,\alpha)=x^2-2\alpha; \tag{5.3.1}$$

$$D_{mn}(x,\alpha)=D_m(D_n(x,\alpha),\alpha^n); \tag{5.3.2}$$

$$\beta^n D_n(x,\alpha)=D_n(\beta x,\beta^2\alpha). \tag{5.3.3}$$

*Proof of Corollary 5.2.* If (5.1.1) holds then (5.2.1) holds, since $\alpha x^r p(x)^n = x^r(\sqrt[n]{\alpha}p(x))^n$. Likewise, if (5.1.2) holds then so does (5.2.2) (perhaps after changing $p$ and $\mu_i$), since $(\alpha x^2+\beta)p(x)^2=(x^2-4)\widehat{p}(x)^2\circ\gamma x$ where $\gamma^2 = -4\alpha/\beta$ and $\widehat{p}(x)=(\sqrt{-\beta}/2)p(x/\gamma)$. We pass from (5.1.5) to (5.2.4) in a similar manner, since $(\alpha x^2-1)^3=(x^2/3-1)^3\circ\sqrt{3\alpha}x$. If (5.1.4) holds, we use (5.3.3) with $\gamma^2=1/\alpha$ and $\delta^2=1/\beta$, getting $\alpha^{-m}D_{2m}(x,\alpha)=D_{2m}(x\gamma)$ and $-\beta^{-n}D_{2n}(x,\beta)=-D_{2n}(x\delta)$, which yields (5.2.5) (with $d=2$).

If (5.1.3) holds, let $\gamma$ be a square root of $\alpha$, so (5.3.3) implies $D_m(x,\alpha^n)=\gamma^{nm}D_m(x/\gamma^n)$, whence $G\circ D_m(x,\alpha^n)=G(\gamma^{nm}x)\circ D_m(x)\circ x/\gamma^n$. Since we could do the same thing after exchanging $n$ and $m$, and since this change would not affect $G(\gamma^{nm}x)$, it follows that (5.2.3) holds here.

If (5.1.6) holds, we again let $\gamma$ be a square root of $\alpha$, so (5.3.3) implies that $-D_{dn}(x\cos(\pi/d),\alpha^m) = -\gamma^{dmn}D_{dn}(x\cos(\pi/d)/\gamma^m)$ and $D_{dm}(x,\alpha^n) = \gamma^{dmn}D_{dm}(x/\gamma^n)$. Thus, after replacing $G(x)$ by $G(\gamma^{dmn}x)$, and composing $\mu_1$ and $\mu_2$ with $x\cos(\pi/d)/\gamma^m$ and $x/\gamma^n$, we obtain (5.2.5). □

To describe the Laurent polynomials with two Type 1 decompositions, we need two more auxiliary results. The first is a neat observation of Fried's about factorizations of polynomials of the form $g_1(x) - g_2(y)$ [10, Prop. 2]; we state the refined version given in [6, Thm. 8.1]:

**Proposition 5.4.** *For any $G_1, G_2 \in \mathbb{C}[x] \setminus \mathbb{C}$, there exist $a_1, a_2, b_2, b_2 \in \mathbb{C}[x]$ such that*

(5.4.1) $G_1 = a_1 \circ b_1$ *and* $G_2 = a_2 \circ b_2$*;*
(5.4.2) *the splitting field of $a_1(x) - z$ over $\mathbb{C}(z)$ equals the splitting field of $a_2(x) - z$ over $\mathbb{C}(z)$;*
(5.4.3) *the irreducible factors of $G_1(x) - G_2(y)$ are precisely the polynomials $A(b_1(x), b_2(y))$, where $A$ is an irreducible factor of $a_1(x) - a_2(y)$.*

We also require the factorization of $D_n(x) + D_n(y)$; as noted by Bilu [5, Prop. 3.1], (5.3.1) and (5.3.2) imply $D_{2n} = D_n^2 - 2$, so for $F_n := D_n(x) - D_n(y)$ we have $D_n(x) + D_n(y) = F_{2n}/F_n$, and hence it suffices to factor $F_n$. This last factorization is well-known; for a simple derivation see [4, Thm. 7].

**Proposition 5.5.** *Put*

$$\Phi_n(x,y) = \prod_{\substack{1\le k<n \\ k\equiv 1 \bmod 2}} (x^2 - xy\cdot 2\cos(\pi k/n) + y^2 - 4\sin^2(\pi k/n)).$$

*Then*

$$D_n(x) + D_n(y) = \begin{cases} \Phi_n(x,y) & \textit{if } n \textit{ is even} \\ (x+y)\Phi_n(x,y) & \textit{if } n \textit{ is odd.} \end{cases}$$

We now classify Laurent polynomials with two Type 1 decompositions.

**Theorem 5.6.** *Let $g_1, g_2 \in \mathbb{C}[x]\setminus\mathbb{C}$ and $h_1, h_2 \in \mathcal{L}\setminus\mathbb{C}$ satisfy $g_1\circ h_1 = g_2\circ h_2$. Then, perhaps after switching $(g_1, g_2)$ and $(h_1, h_2)$, we have*

$$g_1 = G\circ G_1\circ\mu_1$$
$$g_2 = G\circ G_2\circ\mu_2$$
$$h_1 = \mu_1^{-1}\circ H_1\circ H$$
$$h_2 = \mu_2^{-1}\circ H_2\circ H$$

*for some $G\in\mathbb{C}[x]$, some $H\in\mathbb{C}(x)$, and some linear $\mu_1,\mu_2\in\mathbb{C}[x]$, where $(G_1, G_2)$ satisfy one of* (5.2.1)–(5.2.5) *and $(H_1, H_2)$ is the corresponding pair below:*

(5.6.1) $(x^r p(x^n),\, x^n)$*;*
(5.6.2) $((x-1/x)p(x+1/x),\, x+1/x)$*;*
(5.6.3) $(D_n(x),\, D_m(x))$*;*

(5.6.4) $\big(x^2+2x+\frac{1}{x}-\frac{1}{4x^2},\, \frac{1}{3}\big((x+1-\frac{1}{2x})^3+4\big)\big)$;
(5.6.5) $(x^n+1/x^n,\, (\zeta x)^m+1/(\zeta x)^m)$ *where* $\zeta^{dmn}=-1$.

*Proof.* Since $g_1(x)-g_2(y)$ vanishes when $x=h_1(z)$ and $y=h_2(z)$, there is an irreducible factor $E(x,y)$ of $g_1(x)-g_2(y)$ such that $E(h_1(z),h_2(z))=0$. Here $E=0$ defines a genus-zero curve having at most two closed points lying over $x=\infty$. By Corollary 5.2, we have $g_1=G\circ G_1\circ\mu_1$ and $g_2=G\circ G_2\circ\mu_2$ where $G,\mu_1,\mu_2\in\mathbb{C}[x]$ with $\mu_i$ linear, and moreover (perhaps after switching $g_1$ and $g_2$) we may choose $(G_1,G_2)$ to have the form of one of (5.2.1)–(5.2.5). Furthermore, these choices can be made so that $E(x,y)$ divides $G_1\circ\mu_1(x)-G_2\circ\mu_2(y)$. As noted in Proposition 5.1, in cases (5.2.1)–(5.2.4) the polynomial $G_1(x)-G_2(y)$ is irreducible. Thus, for any $H_1,H_2\in\mathbb{C}(x)$ satisfying $G_1\circ H_1=G_2\circ H_2$ and $\gcd(\deg(H_1),\deg(H_2))=1$, there exists $H\in\mathbb{C}(x)$ such that $\mu_1\circ h_1=H_1\circ H$ and $\mu_2\circ h_2=H_2\circ H$. Hence in these cases it suffices to exhibit one such pair $(H_1,H_2)$, and visibly the pairs stated in the Theorem have the required properties.

Henceforth suppose that $G_1=D_{dm}$ and $G_2=-D_{dn}$ with $m,n$ coprime positive integers and $d>1$. Let $G_1=a_1\circ b_1$ and $G_2=a_2\circ b_2$ be the decompositions occurring in Proposition 5.4. Denoting by $\Omega$ the splitting field of $a_1(x)-z$ over $\mathbb{C}(z)$, we see that $\deg(a_1)$ is the ramification index in $\Omega/\mathbb{C}(z)$ of any place lying over $z=\infty$; but (5.4.2) implies the same description applies to $\deg(a_2)$, so $a_1$ and $a_2$ have the same degree. By Lemma 3.1, there exist linear $\nu_1,\nu_2\in\mathbb{C}[x]$, and a divisor $e$ of $d$, such that $a_1=D_e\circ\nu_1$ and $a_2=-D_e\circ\nu_2$ (and $b_1=\nu_1^{-1}\circ D_{md/e}$ and $b_2=\nu_2^{-1}\circ D_{nd/e}$). Since Proposition 5.4 holds for some linear $\nu_1,\nu_2$, it follows that Proposition 5.4 holds for any arbitrarily chosen linears $\nu_1,\nu_2$, so we may assume $\nu_1=\nu_2=x$. A factorization of $a_1(x)-a_2(y)$ is given in Proposition 5.5, in terms of the polynomials $A_{k,e}:=x^2-xy\cdot 2\cos(\pi k/e)+y^2-4\sin^2(\pi k/e)$ where $1\le k<e$ and $k$ is odd. Note that $A_{k,e}$ is irreducible (since its degree-2 part is a nonsquare, it has no degree-1 terms, and it has a nonzero constant term). Thus, by (5.4.3), every irreducible factor of $G_1(x)-G_2(y)$ has $x$-degree $2dm/e$, unless $e$ is odd when there is also one factor of $x$-degree $dm/e$. But Proposition 5.5 implies that $G_1(x)-G_2(y)$ is the product of several polynomials $A_{k,d}(D_m(x),D_n(y))$, as well as (if $d$ is odd) the polynomial $D_m(x)+D_n(y)$. Thus every irreducible factor of $G_1(x)-G_2(y)$ has $x$-degree at most $2m$, so either $e=d$ or $(d,e)=(2,1)$. In the latter case, $G_1(x)-G_2(y)$ is irreducible. Thus, in either case, the irreducible factors of $G_1(x)-G_2(y)$ consist just of the polynomials $A_{k,d}(D_m(x),D_n(y))$ with $1\le k<d$ and $k$ odd, unless $d$ is odd in which case $D_m(x)+D_n(y)$ is another irreducible factor. Now $E(\mu_1^{-1}(x),\mu_2^{-1}(y))$ must be a scalar multiple of one of these factors, and we may assume the scalar is 1 (since we are free to replace $E$ by a scalar multiple of itself). Since $E(h_1(x),h_2(y))=0$, we cannot have $E(\mu_1^{-1}(x),\mu_2^{-1}(y))=D_m(x)+D_n(y)$, so we must have $E(\mu_1^{-1}(x),\mu_2^{-1}(y))=A_{k,d}(D_m(x),D_n(y))$. Denote this polynomial as $R(x,y)$, and put $H_1:=x^n+1/x^n$ and $H_2:=(\zeta x)^m+1/(\zeta x)^m$,

where $\zeta = e^{\pi ik/(dmn)}$. Then $R(H_1(x), H_2(x)) = 0$, so (since $R(x, y)$ is irreducible) we have $H_1 = \widehat{H_1} \circ J$ and $H_2 = \widehat{H_2} \circ J$ for some $\widehat{H_1}, \widehat{H_2}, J \in \mathbb{C}(x)$ such that $R(\widehat{H_1}(x), \widehat{H_2}(x)) = 0$, where in addition $\mu_1 \circ h_1 = \widehat{H_1} \circ H$ and $\mu_2 \circ h_2 = \widehat{H_2} \circ H$ for some $H \in \mathbb{C}(x)$. If $\deg(J) = 1$ this gives (5.6.5), so assume $\deg(J) > 1$. Since $\deg(J)$ divides $\gcd(\deg(H_1), \deg(H_2)) = 2$, we must have $\deg(J) = 2$. If $J \in \mathbb{C}(x^2)$ then $H_1, H_2 \in \mathbb{C}(x^2)$ so both $n$ and $m$ are even, contradiction. Now Lemma 3.1 implies that $J = \lambda_1 \circ (x/\gamma + \gamma/x)$ and $J = \lambda_2 \circ (x/\delta + \delta/x) \circ \zeta x$, where $\gamma^{2n} = 1 = \delta^{2m}$ and $\lambda_1, \lambda_2 \in \mathbb{C}(x)$ have degree one. Comparing images of $x = 0$, we see that $\lambda_1(\infty) = \lambda_2(\infty)$, so $\lambda_2^{-1} \circ \lambda_1$ fixes $\infty$ and thus is a linear polynomial. Thus $J$ is a Laurent polynomial, and its constant term is $\lambda_1(0) = \lambda_2(0)$, so $\lambda_2^{-1} \circ \lambda_1 = \epsilon x$ for some $\epsilon \in \mathbb{C}^*$. Thus

$$\epsilon \left( \frac{x}{\gamma} + \frac{\gamma}{x} \right) = \frac{\zeta x}{\delta} + \frac{\delta}{\zeta x},$$

and equating coefficients of like terms yields $\epsilon\delta = \zeta\gamma$ and $\epsilon\gamma\zeta = \delta$, so $\epsilon = \zeta\gamma/\delta = \pm 1$. Raising to the $(2nm)^{\text{th}}$ power gives $\zeta^{2mn} = 1$, but $\zeta^{2mn} = e^{2\pi ik/d} \neq 1$ since $0 < k < d$, contradiction. □

## 6. Laurent polynomials with decompositions of both types

In this section we prove the following result:

**Theorem 6.1.** *Let $g_1 \in \mathbb{C}[x] \setminus \mathbb{C}$ and $g_2, h_1 \in \mathcal{L} \setminus \mathbb{C}$ satisfy $g_1 \circ h_1 = g_2 \circ x^n$ with $n \in \mathbb{Z}_{>0}$. Then either $h_1 = A \circ x^n$ (and $g_2 = g_1 \circ A$) for some $A \in \mathcal{L}$, or there exist $G, \mu \in \mathbb{C}[x]$ with $\mu$ linear such that $g_1 = G \circ G_1 \circ \mu$ and $h_1 = \mu^{-1} \circ H_1$ and $g_2 = G \circ G_2$, where one of the following holds (with $e \in \mathbb{Z}$ and $r = \gcd(n, e)$):*

(6.1.1) *$G_1 = x^{n/r}$, $H_1 = x^e p(x^n)$, and $G_2 = x^{e/r} p(x)^{n/r}$, where $p \in \mathbb{C}[x]$;*

(6.1.2) *$G_1 = D_{n/r}$, $H_1 = (x^e + 1/x^e) \circ \alpha x$, and $G_2 = (x^{e/r} + 1/x^{e/r}) \circ \alpha^n x$, where $\alpha \in \mathbb{C}^*$.*

We will use some results of Avanzi and Zannier [2, §4], which we state as follows.

**Proposition 6.2** (Avanzi–Zannier)**.** *Pick an indecomposable $g \in \mathbb{C}[x]$, and distinct nonconstant $h_1, h_2 \in \mathbb{C}(x)$, and suppose that $g \circ h_1 = g \circ h_2$. Then $g = \mu \circ G \circ \nu$ and $h_1 = \nu^{-1} \circ H_1 \circ H$ and $h_2 = \nu^{-1} \circ H_2 \circ H$, where $\mu, \nu \in \mathbb{C}[x]$ are linear, $H \in \mathbb{C}(x)$, and either $(G, H_1, H_2)$ or $(G, H_2, H_1)$ is in the following list:*

(6.2.1) *$(x^n, x, \zeta x)$, where $n$ is prime and $\zeta$ is a primitive $n^{\text{th}}$ root of unity;*

(6.2.2) *$\left(D_n, x + \frac{1}{x}, \zeta x + \frac{1}{\zeta x}\right)$, where $n$ is an odd prime and $\zeta$ is a primitive $n^{\text{th}}$ root of unity;*

(6.2.3) *$\left((x^r(x+1)^m, \frac{1-x^r}{x^{r+m}-1}, -1 + \frac{x^m-1}{x^{r+m}-1}\right)$, where $r, m$ are coprime positive integers with $r + m > 3$;*

(6.2.4) $\left(x(x+\alpha)^2(x+1)^2,\ -4\alpha\frac{x^2}{E},\ -\frac{\alpha}{E}\left(x^2-\frac{7x}{4}-\frac{15}{64}\right)^2\right)$, *where* $\alpha\in\mathbb{C}^*$ *satisfies* $9\alpha^2-2\alpha+9=0$ *and*

$$E=\alpha x^4+\frac{3}{8}(3-7\alpha)x^3+\frac{99}{64}(1+\alpha)x^2+\frac{45}{512}(7-3\alpha)x+\frac{225}{4096};$$

(6.2.5) $\left(x(x+\alpha)^3(x+1)^3,\ -4096\frac{x^3}{E},\ \frac{1}{E}(64-(x-\alpha)^2)^3\right)$, *where* $\alpha\in\mathbb{C}^*$ *satisfies* $\alpha^2-5\alpha+8=0$ *and*

$$\begin{aligned}E=x^6&+(32-10\alpha)x^5+(31\alpha-88)x^4+(68\alpha+1888)x^3\\&+(651\alpha-56)x^2+(11158\alpha-50288)x+41881\alpha-156520.\end{aligned}$$

*Remark.* The polynomials in [2] involve some parameters which we have removed by absorbing them into $\mu$ and $\nu$. Also, the assertion in [2, Prop. 4.7] about $g_1$ being reduced is false in case (3).

*Proof of Theorem 6.1.* Let $\zeta$ be a primitive $n^{\text{th}}$ root of unity, so for $h_2:=h_1\circ\zeta x$ we have $g_1\circ h_2=g_1\circ h_1$. If $h_2=h_1$ then $h_1=A\circ x^n$ with $A\in\mathcal{L}$, in which case $g_2=g_1\circ A$. Henceforth assume $h_2\neq h_1$. This implies $g_1$ is not linear, so we can write $g_1=f_1\circ\dots\circ f_v$ where every $f_i$ is indecomposable. Let $j$ be the largest integer for which

$$f_j\circ f_{j+1}\circ\dots\circ f_v\circ h_2=f_j\circ f_{j+1}\circ\dots\circ f_v\circ h_1,$$

and put $R=f_{j+1}\circ\dots\circ f_v$ and $A=f_1\circ\dots\circ f_{j-1}$, so $g_1=A\circ f_j\circ R$. Then $S_2:=R\circ h_2$ and $S_1:=R\circ h_1$ satisfy $S_2\neq S_1$ but $f_j\circ S_2=f_j\circ S_1$. After replacing $A$, $f_j$, and $R$ by $A\circ\mu$, $\mu^{-1}\circ f_j\circ\nu^{-1}$, and $\nu\circ R$, for suitable linear $\mu,\nu\in\mathbb{C}[x]$, Proposition 6.2 implies that there exist $s_1,s_2,T\in\mathbb{C}(x)\setminus\mathbb{C}$ such that $S_1=s_1\circ T$ and $S_2=s_2\circ T$ and either $(f_j,s_1,s_2)$ or $(f_j,s_2,s_1)$ is one of the triples (6.2.1)–(6.2.5). Since replacing $\zeta$ by $1/\zeta$ has the effect of exchanging $s_1$ and $s_2$, we may assume that $(f_j,s_1,s_2)$ is among (6.2.1)–(6.2.5). Moreover, since $h_i\in\mathcal{L}$ and $R\in\mathbb{C}[x]$, also $S_i=R\circ h_i$ is in $\mathcal{L}$, so $s_i$ has at most two poles. This rules out (6.2.3), (6.2.4) and (6.2.5).

If (6.2.1) holds then $f_j=x^\ell$ for some prime $\ell$, and moreover $S_2=\gamma S_1$ for some primitive $\ell^{\text{th}}$ root of unity $\gamma$. Thus $S_1(\zeta x)=\gamma S_1(x)$, so $S_1\in x^t\mathbb{C}[x^n]$ for some $t\in\mathbb{Z}$ with $\zeta^t=\gamma$. By Proposition 4.5, after replacing $R$ and $h_1$ by $R\circ\mu$ and $\mu^{-1}\circ h_1$ for a suitable linear $\mu\in\mathbb{C}[x]$, we may assume that $R$ and $h_1$ satisfy the conditions required of $g$ and $h$ in either (4.5.1) or (4.5.2). First suppose $R$ and $h_1$ satisfy (4.5.1), so $R\in x^d\mathbb{C}[x^m]$ and $h_1=x^e p(x^n)$ with $p\in\mathbb{C}[x]$ and $n\mid em$; then $\gamma=\zeta^{de}$, so $n\mid\ell de$. Putting $r=\gcd(n,e)$, we have $n\mid r\gcd(d\ell,m)$, so $f_j\circ R\in\mathbb{C}[x^{n/r}]$. Since $g_1=A\circ f_j\circ R$, we can write $g_1=G\circ x^{n/r}$. It follows that $g_2=x^{e/r}p(x)^{n/r}$, so we have (6.1.1). Now suppose $R$ and $h_1$ satisfy (4.5.2), so $n$ is even, and also $R=\widehat{R}\circ D_d$ and $h_1=(x^e+1/x^e)\circ\alpha x$, where $\widehat{R}\in x\mathbb{C}[x^2]$ and $ed\equiv t\equiv n/2\pmod{n}$; thus $\gamma=\zeta^t$ has order 2, so $\ell=2$. Now $f_j\circ R=x^2\circ\widehat{R}\circ D_d$; since $\widehat{R}\in x\mathbb{C}[x^2]$, we see that $x^2\circ\widehat{R}$ is in $\mathbb{C}[x^2]$, and thus can be written as $\widetilde{R}\circ D_2$ with $\widetilde{R}\in\mathbb{C}[x]$. Thus $f_j\circ R=\widetilde{R}\circ D_{2d}$, so since $n\mid 2ed$ we can write $g_1=G\circ D_{n/r}$ where

$r = \gcd(n, e)$ amd $G = A \circ \widetilde{R} \circ D_{2dr/n}$. This implies $g_2 = (x^{e/r} + x^{-e/r}) \circ \alpha^n x$, so we have (6.1.2).

Finally, suppose (6.2.2) holds. Then $f_j = D_\ell$ for some odd prime $\ell$, and moreover $s_1 = x + 1/x$ and $s_2 = \gamma x + 1/(\gamma x)$ for some primitive $\ell^{\text{th}}$ root of unity $\gamma$. Since $s_1 \circ T$ is a Laurent polynomial, and $s_1$ has poles at 0 and $\infty$, Lemma 2.1 implies that $T = \delta x^d$ for some $\delta \in \mathbb{C}^*$ and $d \in \mathbb{Z}$. Since we can replace $s_1$, $s_2$, and $T$ by $s_1 \circ 1/x$, $s_2 \circ 1/x$, and $1/x \circ T$, we may assume $d > 0$. Now we have $R \circ h_1 = \delta x^d + 1/(\delta x^d)$ and $R \circ h_1(\zeta x) = \gamma\delta x^d + 1/(\gamma\delta x^d)$, so $\zeta^d = \gamma$ and thus $n \mid d\ell$. Since $R$ is a polynomial, Lemma 3.1 implies that $R = \alpha^d D_{d/e} \circ \mu$ and $h_1 = \mu^{-1} \circ (x^e + 1/x^e) \circ \widehat{\delta} x/\alpha$ where $\mu \in \mathbb{C}[x]$ is linear, $\alpha^{2d} = 1$, and $\widehat{\delta}^d = \delta$. Likewise $R = \beta^d D_{d/e} \circ \nu$ and $h_1 \circ \zeta x = \nu^{-1} \circ (x^e + 1/x^e) \circ \widehat{\gamma} x/\beta$ where $\nu \in \mathbb{C}[x]$ is linear, $\beta^{2d} = 1$, and $\widehat{\gamma}^d = \gamma\delta$. Thus $(\alpha/\beta)^d D_{d/e} = D_{d/e} \circ \nu \circ \mu^{-1}$; equating coefficients of $x^{d/e-1}$ shows that $\nu \circ \mu^{-1} = \theta x$ with $\theta \in \mathbb{C}^*$, and equating coefficients of $x^{d/e}$ shows that $\theta^{d/e} = (\alpha/\beta)^d$. If $d = e$ it follows that $\theta \in \{1, -1\}$; if $d \neq e$ then we also obtain $\theta = \pm 1$ upon equating coefficients of $x^{d/e-2}$. Since $\epsilon := \alpha^d = \pm 1$, we have

$$\begin{aligned} g_1 &= A \circ D_\ell \circ \epsilon D_{d/e} \circ \mu \\ &= A \circ \epsilon^\ell D_\ell \circ D_{d/e} \circ \mu \quad \text{(by (5.3.3))} \\ &= A \circ \epsilon^\ell D_{\ell d/e} \circ \mu. \end{aligned}$$

Recall that $n \mid d\ell$, so with $r = \gcd(e, n)$ we have $en \mid \ell dr$, and thus $g_1 = G \circ D_{n/r} \circ \mu$ with $G = A \circ \epsilon^\ell D_{\ell dr/(en)}$. Since $h_1 = \mu^{-1} \circ (x^e + 1/x^e) \circ \widehat{\delta} x/\alpha$, we find $g_2 = G \circ (x^{e/r} + x^{-e/r}) \circ (\widehat{\delta}/\alpha)^n x$, so we have (6.1.2). □

## 7. Proofs of main results

In this section we prove the results stated in Section 1.

7.1. **Proof of Theorem 1.1.** Define an 'admissible sequence' to be a finite sequence of complete decompositions of a rational function $f$, such that consecutive decompositions in the sequence differ only in that two adjacent indecomposables $u, v$ in the first decomposition are replaced in the second decomposition by two other indecomposables $\widehat{u}, \widehat{v}$ such that $u \circ v = \widehat{u} \circ \widehat{v}$ and $\{\deg(u), \deg(v)\} = \{\deg(\widehat{u}), \deg(\widehat{v})\}$. It suffices to prove that, for any two complete decompositions of a Laurent polynomial $f$, there is an admissible sequence containing them both. We prove this by induction on $\deg(f)$. So assume it holds for all Laurent polynomials of degree less than $\deg(f)$, and consider two complete decompositions $f = p_1 \circ p_2 \circ \cdots \circ p_r = q_1 \circ q_2 \circ \cdots \circ q_s$ (so $p_i, q_j \in \mathbb{C}(x)$ are indecomposable). If $r = 1$ or $s = 1$ then these decompositions are identical, so trivially are contained in an admissible sequence. Henceforth assume $r, s > 1$.

By Lemma 2.1, after replacing $p_{r-1}$ and $p_r$ by $p_{r-1} \circ \mu$ and $\mu^{-1} \circ p_r$ for some $\mu \in \mathbb{C}(x)$ with $\deg(\mu) = 1$, we may assume that both $p_r$ and $\widehat{p} := p_1 \circ \cdots \circ p_{r-1}$

are Laurent polynomials, and moreover either $\widehat{p}\in\mathbb{C}[x]$ or $p_r=x^n$ with $n$ prime. Further, if $\widehat{p}\in\mathbb{C}[x]$ and $p_r\in\mathbb{C}(x^n)$ with $n>1$, then $n$ is prime and $p_r=\widehat{\mu}\circ x^n$ for some degree-one $\widehat{\mu}\in\mathbb{C}(x)$, so by replacing $p_{r-1}$ and $p_r$ by $p_{r-1}\circ\widehat{\mu}$ and $\widehat{\mu}^{-1}\circ p_r$ we may assume $p_r=x^n$; since $\widehat{p}\circ p_r=f\in\mathcal{L}$, we must have $\widehat{p}\in\mathcal{L}$. Thus we may assume that $\widehat{p},p_r\in\mathcal{L}$, and if there is no prime $n$ for which $p_r=x^n$, then $\widehat{p}\in\mathbb{C}[x]$ and $p_r\notin\mathbb{C}(x^n)$ for any $n>1$. We can make analogous assumptions about $q_s$ and $\widehat{q}:=q_1\circ\cdots\circ q_{s-1}$.

If there is a degree-one $\nu\in\mathbb{C}(x)$ for which $p_r=\nu\circ q_s$, then $\widehat{p}=\widehat{q}\circ\nu^{-1}$, so by induction there is an admissible sequence containing $p_1\circ\cdots\circ p_{r-1}$ and $q_1\circ\cdots\circ q_{s-2}\circ(q_{s-1}\circ\nu^{-1})$. Composing each complete decomposition in the sequence with $p_r$, we then get an admissible sequence containing $p_1\circ\cdots\circ p_r$ and $q_1\circ\cdots\circ q_s$. Henceforth assume there is no such $\nu$.

If $p_r=x^n$ and $q_s=x^m$ (with $n,m$ distinct primes), then Proposition 2.2 implies $\widehat{p}=G\circ x^m$ and $\widehat{q}=G\circ x^n$ for some $G\in\mathcal{L}$. Write $G=g_1\circ\cdots\circ g_t$ where every $g_i\in\mathbb{C}(x)$ is indecomposable. By induction, there is an admissible sequence containing $p_1\circ\cdots\circ p_{r-1}$ and $g_1\circ\cdots\circ g_t\circ x^m$, so composing with $p_r$ yields an admissible sequence containing $p_1\circ\cdots\circ p_{r-1}\circ p_r$ and $g_1\circ\cdots\circ g_t\circ x^m\circ x^n$. Likewise there is an admissible sequence containing $q_1\circ\cdots\circ q_s$ and $g_1\circ\cdots\circ g_t\circ x^n\circ x^m$. Since the sequence $(x^m\circ x^n, x^n\circ x^m)$ is admissible, there is an admissible sequence containing $p_1\circ\cdots\circ p_r$ and $q_1\circ\cdots\circ q_s$.

Now assume $q_s=x^n$ but $p_r\notin\mathbb{C}(x^m)$ for every $m>1$. Then $\widehat{p}\in\mathbb{C}[x]$. By Theorem 6.1, there exist $G,\mu\in\mathbb{C}[x]$ with $\deg(\mu)=1$ such that $\widehat{p}=G\circ G_1\circ\mu$ and $p_r=\mu^{-1}\circ H_1$ and $\widehat{q}=G\circ G_2$, where $G_1,G_2,H_1$ satisfy either (6.1.1) or (6.1.2). In (6.1.2) we have $H_1=(x^e+1/x^e)\circ\alpha x$ with $\alpha\in\mathbb{C}^*$ and $e>0$, and indecomposability of $p_r$ implies $e=1$. Thus $G_1=D_n$ and $G_2=(x+1/x)\circ\alpha^n x$, so $(G_1\circ H_1, G_2\circ q_s)$ is admissible, and the inductive argument of the previous paragraph produces an admissible sequence containing $p_1\circ\cdots\circ p_r$ and $q_1\circ\cdots\circ q_s$. In (6.1.1) we have $H_1=x^e h(x^n)$ with $h\in\mathbb{C}[x]$ and $e\in\mathbb{Z}$; since $p_r\notin\mathbb{C}(x^m)$ for $m>1$, we must have $\gcd(e,n)=1$, so $G_1=x^n$ and $G_2=x^e h(x)^n$. We will show that $G_2$ is indecomposable. This implies that $(G_1\circ H_1, G_2\circ x^n)$ is admissible, so as above there is an admissible sequence containing $p_1\circ\cdots\circ p_r$ and $q_1\circ\cdots\circ q_s$. So suppose $G_2$ is decomposable; then Lemma 2.1 implies that $G_2$ has a decomposition of either Type 1 or Type 2 in which both rational functions involved have degree $>1$. By Proposition 4.2, if there is a Type 1 decomposition with this property, then $G_2=u\circ v$ where $u=x^iA(x)^n$ and $v=x^jB(x)^n$, with $A,B\in\mathbb{C}[x]$ and $i,j\in\mathbb{Z}$ and $i>0$. But then $x^n\circ H_1=G_2(x^n)=u\circ v(x^n)=x^iA^n\circ x^n\circ x^jB(x^n)=x^n\circ x^iA(x^n)\circ x^jB(x^n)$, so $H_1=\zeta x^iA(x^n)\circ x^jB(x^n)$ for some $\zeta\in\mathbb{C}^*$ with $\zeta^n=1$, contradicting indecomposability of $p_r$. If $G_2$ has a Type 2 decomposition into rational functions of degree $>1$, say $G_2\in\mathbb{C}(x^m)$ with $m>1$, then $G_2(\zeta x)=G_2(x)$ where $\zeta$ is a primitive $m^{\text{th}}$ root of unity. Thus $\zeta^e h(\zeta x)^n=h(x)^n$, so $h(\zeta x)=\beta h(x)$ where $\zeta^e\beta^n=1$. Hence $h=x^dA(x^m)$ for some $A\in\mathbb{C}[x]$ and some $d\in\mathbb{Z}$ such that $\zeta^d=\beta$. Thus $1=\zeta^e\beta^n=\zeta^{e+nd}$, so $m\mid(e+nd)$. Now $H_1=x^eh(x^n)=x^{e+nd}A(x^{nm})$ is in $\mathbb{C}(x^m)$, and since $H_1$ is indecomposable we must have $H_1 = \lambda \circ x^m$ for some degree-one $\lambda \in \mathbb{C}(x)$. But $H_1 = x^e h(x^n)$ has no constant term (since $\gcd(e, n) = 1$), so $\lambda$ is a degree-one Laurent polynomial with no constant term, whence $\lambda$ is a monomial Laurent polynomial. Thus $h$ is a monomial polynomial, so $G_2 = x^e h(x)^n$ is a constant times $H_1 = x^e h(x^n)$, whence indecomposability of $H_1$ implies indecomposability of $G_2$.

Now assume $p_r, q_s \notin \mathbb{C}(x^n)$ for every $n > 1$. This implies $\widehat{p}, \widehat{q} \in \mathbb{C}[x]$, so Theorem 5.6 applies. After switching $(\widehat{p}, p_r)$ and $(\widehat{q}, q_s)$ if necessary, we obtain

$$\begin{aligned} \widehat{p} &= G \circ G_1 \circ \mu_1 \\ \widehat{q} &= G \circ G_2 \circ \mu_2 \\ p_r &= \mu_1^{-1} \circ H_1 \circ H \\ q_s &= \mu_2^{-1} \circ H_2 \circ H \end{aligned}$$

for some $H \in \mathbb{C}(x)$ and $G, \mu_1, \mu_2 \in \mathbb{C}[x]$ with $\mu_i$ linear, where $(G_1, G_2)$ is one of (5.2.1)–(5.2.5) and $(H_1, H_2)$ is the corresponding pair among (5.6.1)–(5.6.5). If $\deg(H) > 1$ then indecomposability of $p_r$ and $q_s$ implies $p_r = \nu \circ q_s$ for some degree-one $\nu \in \mathbb{C}(x)$, a case treated previously. So assume $\deg(H) = 1$, whence $H_1$ and $H_2$ are indecomposable. In case (5.6.1) we have $H_2 = x^n$ with $n > 0$ (where indecomposability implies $n$ is prime), and $H_1 = x^e h(x^n)$ with $h \in \mathbb{C}[x]$ and $e \in \mathbb{Z}_{>0}$ coprime to $n$. Moreover, $G_1 = x^n$ and $G_2 = x^e h(x)^n$. Here indecomposability of $H_1$ implies indecomposability of $G_2$ (by Ritt's first theorem), so our result follows by induction. In case (5.6.2) we have $H_2 = x + 1/x$ and $H_1 = (x - 1/x)p(x + 1/x)$ with $p \in \mathbb{C}[x]$, and moreover $G_1 = x^2$ and $G_2 = (x^2 - 4)p(x)^2$. Here we need only to prove that $G_2$ is indecomposable. If it were not, then by Proposition 4.6 there would be nonlinear $u, v \in \mathbb{C}[x]$ such that $u \circ v = G_2$ and $u, v$ satisfy the conditions required of $g, h$ in either (4.6.1) or (4.6.2). In (4.6.1) we have $u = xB^2$ and $v = (x^2 - 4)D^2$ with $B, D \in \mathbb{C}[x]$, so composing with $x + 1/x$ gives

$$\begin{aligned} x^2 \circ H_1 = G_2\left(x + \frac{1}{x}\right) &= u \circ v\left(x + \frac{1}{x}\right) = u \circ x^2 \circ \left(x - \frac{1}{x}\right) \cdot D\left(x + \frac{1}{x}\right) \\ &= x^2 \circ xB(x^2) \circ \left(x - \frac{1}{x}\right) \cdot D\left(x + \frac{1}{x}\right), \end{aligned}$$

whence $H_1 = \pm xB(x^2) \circ (x - 1/x)D(x + 1/x)$, contradicting indecomposability of $H_1$. In (4.6.2) we have $u = (x^2 - 4)B^2$ and $v = D_n$ where $B \in \mathbb{C}[x]$ and $n > 1$, so composing with $x + 1/x$ gives

$$\begin{aligned} x^2 \circ H_1 = G_2\left(x + \frac{1}{x}\right) &= u \circ v\left(x + \frac{1}{x}\right) = u \circ \left(x + \frac{1}{x}\right) \circ x^n \\ &= x^2 \circ \left(x - \frac{1}{x}\right) \cdot B\left(x + \frac{1}{x}\right) \circ x^n, \end{aligned}$$

whence $H_1 = \pm(x-1/x)B(x+1/x)\circ x^n$, again contradicting indecomposability. If (5.6.3) holds then $H_1 = G_2 = D_n$ and $H_2 = G_1 = D_m$ where $m, n$ are distinct primes, so the result follows by induction. If (5.6.4) holds then $H_2$ is decomposable, a contradiction. Suppose (5.6.5) holds. Then $H_1 = x^n + 1/x^n$ with $n \in \mathbb{Z}_{>0}$, and indecomposability implies $n = 1$. Likewise $H_2 = \zeta x + 1/(\zeta x)$, where $\zeta^d = -1$ for some $d \in \mathbb{Z}_{>1}$, and moreover $G_1 = D_d = -G_2$. Write $d = \prod_{i=1}^t \ell_i$ where the $\ell_i$ are primes which need not be distinct, and put $e = d/\ell_1$. Since $D_e\circ(x+1/x) = -D_e\circ(\zeta^{\ell_1}x+1/(\zeta^{\ell_1}x))$, by induction there is an admissible sequence containing both $D_{\ell_2}\circ\cdots\circ D_{\ell_t}\circ(x+1/x)$ and $-D_{\ell_2}\circ D_{\ell_3}\circ\cdots\circ D_{\ell_t}\circ(\zeta^{\ell_1}x+1/(\zeta^{\ell_1}x))$. Composing with $x^{\ell_1}$ gives an admissible sequence containing $D_{\ell_t}\circ\cdots\circ D_{\ell_2}\circ(x+1/x)\circ x^{\ell_1}$ and $-D_{\ell_t}\circ D_{\ell_{t-1}}\circ\cdots\circ D_{\ell_2}\circ(\zeta^{\ell_1}x+1/(\zeta^{\ell_1}x))\circ x^{\ell_1}$, and plainly $((x+1/x)\circ x^{\ell_1},\, D_{\ell_1}\circ(x+1/x))$ is admissible, as is $((\zeta^{\ell_1}x+1/(\zeta^{\ell_1}x))\circ x^{\ell_1},\, D_{\ell_1}\circ(\zeta x+1/(\zeta x)))$. Thus there is an admissible sequence containing $D_{\ell_t}\circ\cdots\circ D_{\ell_1}\circ H_1$ and $-D_{\ell_t}\circ D_{\ell_{t-1}}\circ\cdots\circ D_1\circ H_2$, so there is an admissible sequence containing $p_1\circ\cdots\circ p_r$ and $q_1\circ\cdots\circ q_s$. This concludes the proof of Theorem 1.1.

7.2. **Proof of Theorem 1.2.** We prove the result by induction on $\deg(f)$. So assume it holds for all Laurent polynomials of degree less than $\deg(f)$, and write $f = g_1\circ h_1 = g_2\circ h_2$ with $f\in\mathcal{L}$ and with indecomposable $g_1, g_2, h_1, h_2 \in \mathbb{C}(x)$. After replacing $g_1$ and $h_1$ by $g_1\circ\mu$ and $\mu^{-1}\circ h_1$ for some $\mu\in\mathbb{C}(x)$ with $\deg(\mu)=1$, we may assume that $g_1, h_1\in\mathcal{L}$ and either $g_1\in\mathbb{C}[x]$ or $h_1 = x^n$ with $n$ prime (by Lemma 2.1). Moreover, this argument shows that if $h_1\in\mathbb{C}(x^n)$ for some $n>1$ we may assume $h_1 = x^n$ (and indecomposability implies $n$ is prime). We can make analogous assumptions about $g_2$ and $h_2$. If $h_1 = \mu\circ h_2$ for some degree-one $\mu\in\mathbb{C}(x)$, then $g_1\circ\mu = g_2$, so we have (1.2.1). Henceforth assume $h_1\neq\mu\circ h_2$ for any degree-1 $\mu\in\mathbb{C}(x)$.

First suppose $h_1 = x^m$ and $h_2 = x^n$, where $m$ and $n$ are distinct primes. Proposition 2.2 implies $g_1 = G\circ x^n$ and $g_2 = G\circ x^m$ for some $G\in\mathcal{L}$, which must have degree 1 since $g_1$ and $h_2$ are indecomposable. This yields (1.2.2) with $r = m$ and $q = 1$.

Now suppose $h_2 = x^n$ but $h_1\notin\mathbb{C}(x^m)$ for any $m>1$. Then $g_1\in\mathbb{C}[x]$, so Theorem 6.1 applies. Since $h_1\notin\mathbb{C}(x^n)$, there exist $G,\mu\in\mathbb{C}[x]$ with $\deg(\mu)=1$ such that $g_1 = G\circ G_1\circ\mu$ and $h_1 = \mu^{-1}\circ H_1$ and $g_2 = G\circ G_2$, where either (6.1.1) or (6.1.2) holds. If $\deg(G)>1$ then indecomposability of $g_1$ implies $\deg(G_1)=1$, so in both (6.1.1) and (6.1.2) we have $n\mid e$ and thus $G_1\in\mathbb{C}(x^n)$, contradiction. Hence $\deg(G)=1$, so $G_1$ is indecomposable and thus $\gcd(n,e)=1$. In (6.1.1) we have $G_1 = x^n$ and $H_1 = x^e q(x^n)$ and $H_2 = x^e q(x)^n$, with $q\in\mathbb{C}[x]$ and $e\in\mathbb{Z}$ coprime to $n$; this gives (1.2.2). In (6.1.2) we have $G_1 = D_n$ and $H_1 = (\alpha x)^e + 1/(\alpha x)^e$ and $G_2 = (\alpha^n x)^e + 1/(\alpha^n x)^e$ with $\alpha\in\mathbb{C}^*$ and $e\in\mathbb{Z}$, and indecomposability implies $e=\pm 1$. After adjusting $G_1, G_2, H_1, H_2$ by composing with linears, this gives (1.2.4).

Henceforth assume $h_1, h_2\notin\mathbb{C}(x^m)$ for every $m>1$. Then $g_1, g_2\in\mathbb{C}[x]$, so Theorem 5.6 applies. Thus, after switching $(g_1, h_1)$ and $(g_2, h_2)$ if necessary, we have

$$\begin{aligned} g_1 &= G \circ G_1 \circ \mu_1 \\ g_2 &= G \circ G_2 \circ \mu_2 \\ h_1 &= \mu_1^{-1} \circ H_1 \circ H \\ h_2 &= \mu_2^{-1} \circ H_2 \circ H \end{aligned}$$

for some $G \in \mathbb{C}[x]$, some linear $\mu_1, \mu_2 \in \mathbb{C}[x]$, and some $H \in \mathbb{C}(x)$, where $(G_1, G_2)$ is one of the pairs (5.2.1)–(5.2.5) and $(H_1, H_2)$ is the corresponding pair among (5.6.1)–(5.6.5). If $\deg(G) > 1$ then indecomposability of $g_i$ implies $\deg(G_i) = 1$, so we must have either (5.2.1) or (5.6.3). Thus $(H_1, H_2)$ satisfy (5.6.1) and (5.6.3), and in either case $G_1 \circ H_1 = G_2 \circ H_2$ is a linear polynomial, so we have (1.2.1). Likewise if $\deg(H) > 1$ then $\deg(H_i) = 1$, so since $g_1 \circ \mu_1^{-1} \circ H_1 = g_2 \circ \mu_2^{-1} \circ H_2$ we again have (1.2.1). Now assume $\deg(G) = \deg(H) = 1$, so $G_i$ and $H_i$ are indecomposable. Since $H_2 \neq x^n$, we do not have (5.6.1). If (5.2.2) and (5.6.2) hold then, by (4.1.1)–(4.1.3), there are $\nu_1, \nu_2, q \in \mathbb{C}(x)$ with $\deg(\nu_i) = 1$ such that $H_1 \circ \nu_1 = xq(x^2)$ and $G_2 \circ \nu_2 = xq(x)^2$; here also $G_1 = x^2$ and $\nu_2^{-1} \circ H_2 \circ \nu_1 = x^2$, so we have (1.2.2). Note that in this case $q$ is not a Laurent polynomial, instead $q = Q(1/(x+1))$ for some $Q \in x\mathbb{C}[x]$. If (5.2.3) and (5.6.3) hold then (1.2.3) holds. Since $G_1$ is indecomposable, we do not have (5.2.4). Now suppose (5.2.5) and (5.6.5) hold. Thus $G_1 = D_{dm}$ and $G_2 = -D_{dn}$ with $d > 1$ and $m, n \geq 1$, so indecomposability implies $d$ is prime and $m = n = 1$. Here $H_1 = x + 1/x$ and $H_2 = H_1 \circ \zeta x$, where $\zeta^d = -1$. If $d$ is odd then, with $\mu = -x$, we have $G_2 = D_{dn} \circ \mu$ and $\mu^{-1} \circ H_2 = H_1 \circ (-\zeta x)$ where $(-\zeta)^d = 1$, which is (1.2.5). Finally, if $d = 2$ then with $\mu = 2 - x$ we see that $(\mu \circ G_2,\, \mu \circ G_1)$ satisfies (5.2.2) and $(H_2, H_1)$ satisfies (5.6.2) (both with $p(x) = \zeta$), a case we have already resolved. This concludes the proof of Theorem 1.2.

7.3. **Proof of Theorem 1.5.** Let $f \in \mathcal{L} \setminus \mathbb{C}$ and $g_1, g_2, h_1, h_2 \in \mathbb{C}(x)$ satisfy $f = g_1 \circ h_1 = g_2 \circ h_2$. By Lemma 2.1, after replacing $g_1$ and $h_1$ by $g_1 \circ \mu$ and $\mu^{-1} \circ h_1$ for some degree-one $\mu \in \mathbb{C}(x)$, we may assume $g_1, h_1 \in \mathcal{L}$ and either $g_1 \in \mathbb{C}[x]$ or $h_1 = x^n$ with $n \in \mathbb{Z}_{>0}$. We can make similar assumptions about $g_2$ and $h_2$.

If $h_1 = x^n$ and $h_2 = x^m$ with $n, m > 0$, then Proposition 2.2 implies $g_1 = G \circ x^{\operatorname{lcm}(n,m)/n}$ and $g_2 = G \circ x^{\operatorname{lcm}(n,m)/m}$ for some $G \in \mathcal{L}$. Thus (1.5.1) holds with $\mu_i = x$ and $H = x^{\gcd(n,m)}$ (and $p = 1$).

Now suppose precisely one of $h_1$ and $h_2$ has the form $x^n$ with $n > 0$; by switching $(g_1, h_1)$ and $(g_2, h_2)$ if necessary, we may assume $h_2 = x^n$ and $g_1 \in \mathbb{C}[x]$. If there exists $A \in \mathcal{L}$ such that $h_1 = A \circ x^n$ and $g_2 = g_1 \circ A$, then (1.5.1) holds with $G = g_1,\ \mu_i = x,\ H = x^n$, and $p = A$. So assume there is no such $A$. By Theorem 6.1, there exist $G, \mu \in \mathbb{C}[x]$ with $\mu$ linear such that $g_1 = G \circ G_1 \circ \mu$ and $h_1 = \mu^{-1} \circ H_1$ and $g_2 = G \circ G_2$, where either (6.1.1) or (6.1.2) holds. If (6.1.1) holds then (1.5.1) holds with $H = x^{\gcd(n,e)}$. If (6.1.2) holds then (1.5.6) holds with $H = (\alpha x)^{\gcd(n,e)}$.

Finally, suppose $g_1, g_2 \in \mathbb{C}[x]$, so Theorem 5.6 applies. Thus, perhaps after switching $(g_1, g_2)$ and $(h_1, h_2)$, we have

$$\begin{aligned} g_1 &= G \circ G_1 \circ \mu_1 \\ g_2 &= G \circ G_2 \circ \mu_2 \\ h_1 &= \mu_1^{-1} \circ H_1 \circ H \\ h_2 &= \mu_2^{-1} \circ H_2 \circ H \end{aligned}$$

for some $G \in \mathbb{C}[x]$, some $H \in \mathbb{C}(x)$, and some linear $\mu_1, \mu_2 \in \mathbb{C}[x]$, where $(G_1, G_2)$ satisfy one of (5.2.1)–(5.2.5) and $(H_1, H_2)$ is the corresponding pair among (5.6.1)–(5.6.5). In each case, this implies the corresponding condition among (1.5.1)–(1.5.5).

If $G_1 \circ H_1$ has poles at both 0 and $\infty$, then $H$ preserves $\{0, \infty\}$, so $H$ is a monomial. This occurs in (1.5.2) and (1.5.4)–(1.5.6).

Now we prove the final assertion in Theorem 1.5. Since $f = G \circ G_1 \circ H_1 \circ H$ is a nonconstant Laurent polynomial, and $G, G_1 \in \mathbb{C}[x]$, we see that $H_1 \circ H$ has no poles besides 0 and $\infty$. If any of (1.5.2) or (1.5.4)–(1.5.6) holds, then $H_1$ has poles at both 0 and $\infty$, so $H$ preserves $\{0, \infty\}$ and thus $H = \alpha x^s$ with $\alpha \in \mathbb{C}^*$ and $s \in \mathbb{Z}$. Here $s \neq 0$ (since $f$ is nonconstant). To show we can choose $s > 0$, it suffices to prove that, for some $\beta \in \mathbb{C}^*$ and some degree-one $\nu_1, \nu_2 \in \mathbb{C}(x)$, the decompositions $(G_1 \circ \nu_1) \circ (\nu_1^{-1} \circ H_1 \circ \beta/x) = (G_2 \circ \nu_2) \circ (\nu_2^{-1} \circ H_2 \circ \beta/x)$ satisfy the same one of (1.5.2) or (1.5.4)–(1.5.6) that is satisfies by the original decompositions. In case (1.5.2) this is true for $\beta = 1$ and $\nu_2 = x = -\nu_1$. In (1.5.4), we can take $\beta = -1/2$ and $\nu_2 = x = -\nu_1$. In (1.5.5), we can take $\beta = 1$ and $\nu_1 = x = \nu_2$ (provided we replace $\zeta$ by $1/\zeta$). In (1.5.6), we can take $\beta = 1$ and $\nu_1 = x = 1/\nu_2$. This concludes the proof of Theorem 1.5.

7.4. **Proof of Proposition 1.4.** Pick $f \in \mathcal{L} \setminus \mathbb{C}$, and suppose there are $g_1, g_2, h_1, h_2 \in \mathbb{C}(x)$ such that $f = g_1 \circ h_1 = g_2 \circ h_2$ and $\deg(g_1) = \deg(g_2)$. By Theorem 1.5, after possibly switching $(g_1, h_1)$ and $(g_2, h_2)$, we have

$$\begin{aligned} g_1 &= G \circ G_1 \circ \mu_1 \\ g_2 &= G \circ G_2 \circ \mu_2 \\ h_1 &= \mu_1^{-1} \circ H_1 \circ H \\ h_2 &= \mu_2^{-1} \circ H_2 \circ H \end{aligned}$$

for some $G \in \mathbb{C}[x]$, some $H \in \mathcal{L}$, and some degree-one $\mu_1, \mu_2 \in \mathbb{C}(x)$, where one of (1.5.1)–(1.5.6) holds. Since $\deg(g_1) = \deg(g_2)$, we have $\deg(G_1) = \deg(G_2)$, which greatly restricts the possibilities. In particular, (1.5.4) cannot happen. In case (1.5.3) we must have $m = n = 1$, so (1.4.1) holds. In case (1.5.5) we again have $m = n = 1$, so (1.4.3) holds. In case (1.5.6) we have $m = 2$ and $n = 1$, so (1.4.4) holds. In case (1.5.2) we have $p = \alpha x$ with

$\alpha \in \mathbb{C}^*$. Putting $\lambda = 2 + \frac{x}{\alpha^2}$ and $\nu = \alpha x/i$ we get

$$\begin{aligned} \lambda \circ G_1 \circ \nu &= -D_2(x) \\ \lambda \circ G_2 &= D_2(x) \\ \nu^{-1} \circ H_1 &= ix + \frac{1}{ix} \\ H_2 &= x + \frac{1}{x}, \end{aligned}$$

which is the $n = 2$ case of (1.4.3). Finally, suppose (1.5.1) holds, so $G_1 = H_2 = x^n$ for some $n > 0$, and $H_1 = x^r p(x^n)$ and $G_2 = x^r p(x)^n$ where $p \in \mathbb{C}[x] \setminus \{0\}$ and $r \in \mathbb{Z}$ is coprime to $n$. Write $p = x^e P$ where $P \in \mathbb{C}[x]$ satisfies $P(0) \neq 0$, so with $R = r - en$ we have $H_1 = x^R P(x^n)$ and $G_2 = x^R P(x)^n$; replacing $r$ by $R$ and $p$ by $P$, we may therefore assume $x \nmid p$. If $r \geq 0$ then $\deg(G_2) = r + n \cdot \deg(p)$, which must equal $n$, so $\deg(p) \leq 1$. In either case, coprimality of $r$ and $n$ implies $n = 1$: for, if $\deg(p) = 1$ then $r = 0$, and if $\deg(p) = 0$ then $r = n$. Thus $G_2$ and $H_1$ are linear, and $G_2 = H_1$, so by composing with linears we obtain (1.4.1). Now assume $r < 0$, and write $s = -r$. Then $\deg(G_2) = \max(s, n \deg(p))$, so $\deg(p) = 1$ and $1 \leq s \leq n$. We may assume $s < n$, since otherwise $s = n = 1$ so we obtain (1.4.1) as above. Now, composing with (scalar) linears gives (1.4.2).

Cases (1.4.3) and (1.4.4) are instances of (1.5.5) and (1.5.6), so by Theorem 1.5 we may assume $H = \alpha x^s$ with $\alpha \in \mathbb{C}^*$ and $s \in \mathbb{Z}_{>0}$. If (1.4.2) holds, then $f = G \circ G_1 \circ H_1 \circ H$ is a nonconstant Laurent polynomial, and $G, G_1 \in \mathbb{C}[x]$, so $H_1 \circ H$ has no poles besides 0 and $\infty$. But $H_1$ has poles at 0 and $\infty$, so $H$ preserves $\{0, \infty\}$, and thus $H = \alpha x^s$ with $\alpha \in \mathbb{C}^*$ and $s \in \mathbb{Z}$ (and $s \neq 0$). If $s < 0$ then, writing $\nu = 1/x$, we have $H_1 \circ \nu = (x^n + 1)/x^{n-r}$ and $\nu \circ H_2 \circ \nu = H_2$ and $G_2 \circ \nu = (x + 1)^n / x^{n-r}$, so by replacing $r$ by $n - r$ we again have (1.4.2), but now with $H$ replaced by $x^{-s}/\alpha$. Thus we may assume $s > 0$, so the proof of Proposition 1.4 is complete.

## References

[1] S. S. Abhyankar, S. D. Cohen and M. E. Zieve, *Bivariate factorizations connecting Dickson polynomials and Galois theory*, Trans. Amer. Math. Soc. **352** (2000), 2871–2887.

[2] R. M. Avanzi and U. M. Zannier, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$*, Compositio Math. **139** (2003), 263–295.

[3] R. M. Beals, J. L. Wetherell and M. E. Zieve, *Polynomials with a common composite*, submitted for publication. (arXiv:0707.1552 [math.AG])

[4] M. Bhargava and M. Zieve, *Factoring Dickson polynomials over finite fields*, Finite Fields Appl. **5** (1999), 103–111.

[5] Y. F. Bilu, *Quadratic factors of $f(x) - g(y)$*, Acta Arith. **90** (1999), 341–355.

[6] Y. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

[7] F. Binder, *Characterization of polynomial prime bidecompositions: a simplified proof*, in: Contributions to General Algebra, 9 61–72, Hölder-Pichler-Tempsky, Vienna, 1995.

[8] F. Dorey and G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.

[9] H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.

[10] M. D. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. **17** (1973), 128–146.

[11] M. D. Fried, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. **264** (1973), 40–55.

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

[13] D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math., to appear. (arXiv:0705.1954 [math.NT])

[14] D. Ghioca, T. J. Tucker and M. E. Zieve, *Algebraic relations between polynomial orbits*, in preparation.

[15] J. Gutierrez and D. Sevilla, *Building counterexamples to Ritt's decomposition theorem for rational functions*, J. Algebra **303** (2006), 655–667.

[16] H. Lausch and W. Nöbauer, Algebra of Polynomials, North-Holland, Amsterdam, 1973.

[17] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 389–400.

[18] R. Lidl, G. L. Mullen and G. Turnwald, Dickson Polynomials, Longman Sci. Tech., 1993.

[19] R. Lyons and M. E. Zieve, *The rational function analogues of Ritt's polynomial decomposition theorems*, in preparation.

[20] A. McConnell, *Polynomial subfields of $k(x)$*, J. Reine Angew. Math. **266** (1974), 136–139.

[21] J. McKay and D. Sevilla, *Application of univariate rational decomposition to Monstrous Moonshine*, in: Proceedings of Encuentro de Agebra Computacional y Aplicaciones pp. 289–294, 2004.

[22] P. Müller, *Primitive monodromy groups of polynomials*, in: Recent Developments in the Inverse Galois Problem 385–401, Amer. Math. Soc., Providence, RI, 1995.

[23] P. Müller and M. E. Zieve, *On Ritt's decomposition theorems for polynomials*, in preparation.

[24] M. Muzychuk and F. Pakovich, *Solution of the polynomial moment problem*, preprint, available at `http://www.math.bgu.ac.il/∼pakovich/Publications/s.pdf`

[25] F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, arXiv:math/0603452 [math.DS].

[26] F. Pakovich, *On the functional equation $F(A(z)) = G(B(z))$, where $A, B$ are polynomials and $F, G$ are continuous functions*, arXiv:math/0605016 [math.CV].

[27] F. Pakovich, N. Roytvarf and Y. Yomdin, *Cauchy-type integrals of algebraic functions*, Israel J. Math. **144** (2004), 221–291. (arXiv:math/0312353 [math.CA])

[28] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.

[29] J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 399–448.

[30] J. F. Ritt, *Equivalent rational substitutions*, Trans. Amer. Math. Soc. **26** (1924), 221–229.

[31] A. Schinzel, Selected Topics on Polynomials, University of Michigan Press, Ann Arbor, 1982.

[32] A. Schinzel, Polynomials with Special Regard to Reducibility, Cambridge University Press, 2000.

[33] P. Tortrat, *Sur la composition des polynômes*, *Colloq. Math.*, **55** (1988), 329–353.

[34] U. Zannier, *Ritt's second theorem in arbitrary characteristic*, J. Reine Angew. Math. **445** (1993), 175–203.

[35] U. Zannier, *On a functional equation relating a Laurent series $f(x)$ to $f(x^m)$*, Aequat. Math. **55** (1998), 15–43.

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540
*E-mail address*: `zieve@math.rutgers.edu`
*URL*: `www.math.rutgers.edu/∼zieve/`