On the structure of skew polynomial rings

Gil Alon and Elad Paran

January 3, 2020

Abstract

We study arithmetic in the ring $K[x, \sigma]$ of skew polynomials rings, where K is a field and σ is an automorphism of finite order. We show that every non-zero element of $K[x, \sigma]$ decomposes as a right least common multiple of products of similar primes. This generalizes the classical prime power decomposition in the commutative ring of polynomials $K[x]$.

1 Introduction

Skew polynomial rings were first introduced by Noether and Schmeidler in [NS20], and systematically studied by Ore in his classical paper [Ore33]. Let K be a skew field[1], let σ be an automorphism of K and let δ be a derivation on K. The **skew polynomial ring** $R = K[x, \sigma, \delta]$ is the set of polynomials over K, equipped with the usual addition and with multiplication determined by $ax = xa^\sigma + \delta(a)$ for any scalar $a \in K$.[2] These rings have been extensively studied in the literature, both from an abstract point of view (for example in [Jac37], [Coh63], [LL88], [GL94b], [Coh95], [SZ02], [BG12],[MPK19], [GTLN19]), as well as for their various applications (for example in [IM94],[GL94a], [Tae06], [BU09]).

If $R = K[x]$ is the usual ring of polynomials over a commutative field K, then R satisfies the classical unique factorization theorem:

> *Every $0 \neq f \in K[x]$ can be factored into a product of primes in R. The factorization is unique up to association and order of terms.*

[1] That is, a division ring.

[2] When no derivation is involved, i.e. when $\delta = 0$, we denote the ring by $K[x, \sigma]$.

By grouping together recurring primes, unique factorization can also be reformulated as the following "prime power decomposition":

> *Every* $0 \neq f \in K[x]$ *can be written in the form* $P_1 \cdot \ldots \cdot P_m = [P_1, \ldots, P_m]$ *, where* $P_1, \ldots, P_m$ *are associates of powers of primes, and the* P_i *are pairwise co-prime. The* P_i *are determined uniquely up to association and order of terms.*

Here $[P_1, \ldots, P_m]$ denotes the least common multiple of $P_1, \ldots, P_m$, which equals the product $P_1 \cdot \ldots \cdot P_m$ since the P_i are pairwise co-prime.

The central result of [Ore33] generalizes the factorization into products of primes, for skew polynomial rings.

Theorem 1.1. *[Ore33, Theorem 1, p. 494] Any polynomial* $0 \neq f \in K[x, \sigma, \delta]$ *can be written as a product of prime factors. This presentation is unique up to order and similarity.*

Here a polynomial p is called prime if it admits no right (or left) non-constant factors of smaller degree. Two polynomials f, g are called **similar** if R/Rf is isomorphic to R/Rg as left R-modules (a more explicit characterization is given in the next section). Note that if $R = K[x]$ is the usual ring of polynomials over a commutative field, then two polynomials in R are similar if and only if they are associates.

The purpose of this note is to give a "prime power decomposition" theorem for the ring $R = K[x, \sigma]$, where K is a commutative field and σ is an automorphism of finite order. Note that unlike the case of usual polynomial rings, here one cannot simply "group together" recurring primes, since the ring is generally non-commutative.

We call an element $f \in R$ a **skew power** of a polynomial $p \in R$, if f is a product of terms all similar to p (see Definition 3.6). For polynomials $f_1, \ldots, f_m \in R$, let $[f_1, \ldots, f_m]$ be the right least common multiple of $f_1, \ldots, f_m$. We prove the following result:

Theorem 1.2. *Every polynomial* $0 \neq f \in R$ *decomposes as* $f = [P_1, \ldots, P_m]$*, where* $P_1, \ldots, P_m$ *are skew powers of prime polynomials* $p_1, \ldots, p_m$*. The number of terms in each minimal such decomposition is uniquely determined by* f*, and the primes* p_i *are determined uniquely up to order and similarity.*

Note that in the case where $R = K[x]$ is the usual ring of commutative polynomials, a skew power of a polynomial p is simply an associate of a power of p.[3] Thus the decomposition given by Theorem 1.2 generalizes the usual prime power decomposition in $K[x]$ (see Remark 3.8).

[3]For example, if $R = \mathbb{Q}[x]$, then $2x^2$ is a skew power of x.

In section 2 we briefly recall the necessary results established in [Ore33]. Section 3 is then dedicated to the proof of Theorem 1.2.

In Section 4, we consider the special case where $K = \mathbb{C}$ if the field of complex numbers and σ is complex conjugation. In this case, we show that the skew powers that appear in the decomposition given by Theorem 1.2 can be uniquely[4] written as products of primes (Corollary 4.4), and we provide an explicit characterization of them (Theorem 4.11).

Finally, in Section 5 we observe that Theorem 1.2 does not hold for general skew polynomial rings: We show that the assertion of the theorem fails for the ring $K[x, \delta]$, where $K = \mathbb{C}(t)$ is the field of complex rational functions and δ is the standard derivation with respect to t.

2 Preliminaries

Let $R = K[x, \sigma, \delta]$ be a skew polynomial ring, where K is a skew field, σ is an automorphism of K, and δ a derivation of K.

A polynomial $f \in R$ is called **reduced** if its leading term is 1 (i.e. f is monic). A reduced polynomial $p \in R$ is said to be **prime** if it cannot be written as a product of two non-constant polynomials[5].

Two polynomials $f, g \in R$ are said to be **relatively prime** if they admit no common right-hand prime divisors.

Given non-zero elements $f, g \in R$ we denote by $[f, g]$ their right least common multiple. That is, $[f, g]$ is an element of minimal degree that is right-hand divisible by both f and g. The polynomial $[f, g]$ is determined uniquely up to association. Throughout this work, unless stated otherwise, we shall implicitly choose $[f, g]$ to be reduced[6].

Similarly, there is a unique (up to association) polynomial of minimal degree which is left-hand divisible by f and g, denoted by $[f, g]_l$. One similarly defines the right and left least common multiples $[f_1, \ldots, f_m]$ and $[f_1, \ldots, f_m]_l$, respectively, for any number of terms.

The ring R is left and right Euclidean [Ore33, p. 483], hence is a left and right principal ideal domain. It follows that if an element f is right-hand divisible by elements g and h, then f is right-hand divisible by $[g, h]$. Similarly, if f is left-hand divisible by g and h, then f is left-hand divisible

[4]Here the factorization is unique in the strictest possible sense, not even up to order or similarity.

[5]Ore does not consider non-reduced irreducible polynomials as "prime". We follow his convention.

[6]Here we slightly deviate from Ore's terminology in [Ore33], who calls $[f, g]$ the **union** of f and g, and only allows for it to be reduced.

by $[g,h]_l$

Given non-zero elements $f,g \in R$, there exists a unique element $f_g \in R$ with the same leading term as f such that $f_g \cdot g$ is an associate of $[f,g]$. The polynomial f_g is called the **transform** of f by g [Ore33, §4, p. 488][7]. If f and g are relatively prime, then f_g is called a **special transform**, and in this case one has $\deg(f_g) = \deg(f)$. Two elements $f,h \in R$ are called **left-hand similar** if $h = f_g$ is a special transform of f for some $g \in R$ relatively prime to f. In a similar fashion, the **left-transform** ${}_gf$ [Ore33, p. 491] is the unique element with the same leading term as f such that $g \cdot ({}_gf)$ is an associate of $[f,g]_l$, and ${}_gf$ is called **right-hand similar** to f if g is left-hand relatively prime to f (that is, if f,g admit no common left-hand prime divisors). If an element h is left-hand similar to f then h is also right-hand similar to f [Ore33, Theorem 18, p. 493], and we shall simply say that f and h are **similar**. Equivalently (see [Coh63, §2]), f,h are similar if and only if R/Rf is isomorphic to R/Rh as left R-modules.

If h is similar to f and f is prime, then so is h [Ore33, p. 493].

The following lemma [Ore33, Theorem 11, p. 489] is an especially useful property of the transform:

Lemma 2.1. *Let $f,g,h \in R$. If fg is right-hand divisible by h, then f is right-hand divisible by h_g.*

By symmetry, one has:

Lemma 2.2. *Let $f,g,h \in R$. If fg is left-hand divisible by h, then g is left-hand divisible by ${}_fh$.*

A reduced element $f \in R$ is called **non-distributive** if it cannot be written in the form $[g,h]$ for any $f,g \in R$ of degree smaller than $\deg(f)$. Equivalently [Ore33, Theorem 15, p. 506], f is non-distributive if and only if it admits a unique prime **left-hand** divisor p, and one says that f **belongs** to p.

An element $g \in R$ is called **completely reducible** if it is of the form $[p_1,\ldots,p_m]$, with $p_1,\ldots,p_m$ primes.

Ore shows that [Ore33, Theorem 18, p. 507][8]:

[7] Ore denotes the transform by $gf(x)g^{-1}$. We find the notation f_g more convenient.

[8] We note that there is a small error in the formulation of [Ore33, Theorem 18, p. 507]: Ore allows f to be an arbitrary element in R, but in fact his result can only apply to reduced elements, since he defines $[A_1,\ldots,A_m]$ to be reduced. However, allowing least common multiples to be non-reduced, as we have defined, Ore's theorem holds as stated here.

Theorem 2.3. *Let $f \in R$ and let $[p_1, \ldots, p_m]$ be a completely reducible left-hand divisor of f of maximal degree, with $p_1, \ldots, p_m$ distinct primes. Then f has a minimal decomposition of the form $[A_1, \ldots, A_m]$ with $A_1, \ldots, A_m$ non-distributive elements. The number of terms in every minimal such presentation is m. Moreover, the unique prime left-hand divisors of $A_1, \ldots, A_m$ are, up to order and similarity, $p_1, \ldots, p_m$.*

In the next section we show that in the case of $R = K[x, \sigma]$ with K a commutative field and σ and automorphism of finite order, the non-distributive elements in R are all skew powers of prime polynomials. This enables us to deduce Theorem 1.2 from Theorem 2.3.

3 Proof of Theorem 1.2

For this section, fix a (commutative) field K and let σ be an automorphism of K of finite order. Put $R = K[x, \sigma]$.

The proof of the following lemma is given in the first part of the proof of [BGSZ15, Theorem 3.1]. We note that in [BGSZ15] K is assumed to be algebraically closed, but the mentioned part of the proof of [BGSZ15, Theorem 3.1] does not rely on this assumption.

Lemma 3.1. *For each $f \in R$ there exists a non-zero polynomial $h \in R$ such that hf lies in the center $C(R)$ of R.*

Note that the condition $hf \in C(R)$ implies $hf = fh$. Indeed, $f(hf) = (hf)f$ implies $fh = hf$, since R has no zero-divisors.

Lemma 3.2. *Let p, q be primes in R. If pq is non-distributive, then pq has a unique presentation as a product of primes*[9]*.*

Proof. If pq is non-distributive, p is the only prime left-hand divisor of pq. By Theorem 1.1 any factorization of $p \cdot q$ into a product of primes includes precisely two terms, hence must be the given one. □

Lemma 3.3. *Let p, q be prime elements in R such that pq is non-distributive, and let $0 \neq h \in R$ satisfy $hp \in C(R)$. If q does not divide h from the left, then p, q are similar.*

Proof. We have $hpq = phq = qph$, hence by Lemma 2.2, the left-transform ${}_hq$ divides pq from the left. From the assumption it follows that the left-transform ${}_hq$ is special, hence ${}_hq$ is prime. Since pq has a unique presentation as a product of primes, we must have $p =_h q$. □

[9] Recall that we assume all our primes to be reduced.

Proposition 3.4. *Let p, q be prime elements in R such that pq is non-distributive. Then p and q are similar.*

Proof. Let $0 \neq h \in R$ be such that $hp \in C(R)$. If the condition of the preceding lemma is met, we are done. So suppose that $h \in qR$. Write $q^{-1}h$ in the form bp^l, where l is chosen to maximal, so that $b \notin Rp$. We have $qbp^{l+1} = hp = ph = pqbp^l$, hence $qbp = pqb$. Thus p divides pqb from the right, hence by Lemma 2.1 the transform p_b divides pq from the right. Since p does not divide b from the right, p_b is a special transform of p, hence p_b is a prime. By the unique presentation of pq we deduce that $q = p_b$. □

We now show that given non-similar elements in R, the order of the terms in the product pq may be swapped, up to similarity:

Proposition 3.5. *Suppose p, q are non-similar prime elements of R. Then there exist primes $r, s \in R$ such that r is similar to q, p is similar to s, and $pq = rs$.*

Proof. By the preceding proposition pq is distributive, hence there exist reduced polynomials $a, s \in R$ such that $pq = [a, s]$. Both a and s must be prime – otherwise pq could be presented as a product of more than two primes, in contradiction with Theorem 1.1. At least one of a and s, say s, must be relatively prime to q, otherwise $[a, s] = q$. Let $r \in R$ be such that $pq = [a, s] = rs$. Then by Theorem 1.1 r and s must be prime, and by Lemma 2.1 p is right-hand divisible by s_q, which is a prime, being a special transformation of s. Thus we must have $p = s_q$, hence p and s are similar. Since p, q are non-similar, by Theorem 1.1 q must be similar to r. □

Definition 3.6. Let f, g be elements in a skew polynomial ring. We say that f is a **skew power** of g if f can be written as $g_1 \cdot g_2 \cdot \ldots \cdot g_k$ with $g_1 = g, k \geq 1$, and g_i similar to g for all $1 \leq i \leq k$.

From Proposition 3.5 we get the following corollary:

Corollary 3.7. *Let f be a non-distributive element in R, and let p be the unique prime left-hand divisor of f. Then f is a skew power of p.*

Proof. Let n be the number of primes that appear in any factorization of f into a product of primes. For any $1 \leq k \leq n$, we show by induction that the k left most factors in any factorization of f into a product of primes are similar to p. Indeed, suppose we have shown this for $1 \leq k < n$, and consider a factorization $f = p_1 \cdot p_2 \cdot \ldots \cdot p_k \cdot p_{k+1} \cdot \ldots \cdot p_n$ into a product of primes (where p_1 is necessarily p). If p_{k+1} is not similar to p_k, then by the induction hypothesis p_{k+1} is not similar to p. By Proposition 3.5 there exist primes q_k, q_{k+1} such

that p_k is similar to q_{k+1}, p_{k+1} is similar to q_k and $p_k p_{k+1} = q_k q_{k+1}$. We thus have the factorization $f = p_1 \cdot p_2 \ldots \cdot p_{k-1} \cdot q_k \cdot q_{k+1} \cdot p_{k+2} \cdot \ldots \cdot p_n$, where the k-th left most factor q_k is not similar to p, a contraction. Thus p_{k+1} is similar to p_k, hence similar to p, which completes the induction.

For $k = n$ we obtain the desired result. □

Theorem 1.2 now follows from Theorem 2.3 and Corollary 3.7.

Remark 3.8. Consider the factorization $f = [P_1, \ldots, P_m]$ given by Theorem 1.2. In the case where $R = K[x]$ is the usual ring of polynomials, the skew powers P_i are simply associates of power of primes. Thus by the minimality of m, it follows that the P_i are pairwise relatively prime, and so the decomposition obtained is the usual prime power decomposition. However, it does not generally hold for $R = K[x, \sigma]$ that the P_i are relatively prime. Indeed, let $K = \mathbb{C}$ and let σ be complex conjugation. The elements $(x - i)(x - 1), (x + i)(x - 1)$ are both non-distributive (see Corollary 4.13 in the next section). Put $f = [(x - i)(x - 1), (x + i)(x - 1)]$. One checks directly that $f = (x^2 - 1)(x - 1) = (x - 1)(x^2 - 1)$. This element is distributive, as it admits both $(x - 1)$ and $(x + 1)$ as left-hand prime divisors. Thus the decomposition $f = [(x - i)(x - 1), (x + i)(x - 1)]$ is minimal, although $(x - i)(x - 1), (x + i)(x - 1)$ are not relatively prime.

Similarly, the element $g = [(x - 1)(x - i), (x - 1)(x + i)] = (x^2 - 1)^2$ demonstrates that the P_i also cannot be guaranteed to be left-hand relatively prime.

4 The ring $\mathbb{C}[x, \bar{\cdot}]$

In this section we focus on the ring $R = \mathbb{C}[x, \bar{\cdot}]$ of skew polynomials over the field of complex numbers $\mathbb{C}$, where $z \mapsto \bar{z}$ denotes complex conjugation. The following notion is particularly useful in the study of R.

Definition 4.1. For a polynomial $f = f_0 + f_1 x + \ldots + f_n x^n \in R$, we define its **dual** as the polynomial $f^* = \bar{f}_0 - f_1 x + \bar{f}_2 x^2 - f_3 x^3 + \ldots$. One verifies directly that $f + f^*$ and $f f^*$ belong to $\mathbb{R}[x^2]$, which is the center of R. Moreover, the map $f \mapsto f^*$ is an anti-automorphism of R, of order 2.

The next lemma shows that the product of two distinct but similar primes in R belongs to the center $\mathbb{R}[x^2]$.

Lemma 4.2. *If q and r are distinct similar primes in R, then $[q, r] = qq^* = rr^*$ if $\deg(q) = 2$, and $[q, r] = -qq^* = -rr^*$ if $\deg(r) = 1$. Moreover $[q, r]_l = [q, r]$.*

Proof. Since q and r are similar, there exists a reduced polynomial $s \in R$, relatively prime to r, such that $q = r_s$. We claim that rs and r are relatively prime. Indeed, if they are not, then r divides rs from the right, hence by Lemma 2.1, r is right-hand divisible by r_s, which implies that $r = r_s$, hence $q = r$, a contradiction.

Thus r, rs are relatively prime, hence $[r, rs]$ is of degree $\deg(r)+\deg(rs) = \deg(r^*rs)$. But $sr^*r = r^*rs$ is right-hand divisible by rs and r, hence $[r, rs]$ is an associate of r^*rs. If $\deg(r) = 2$ then r^*rs is reduced and hence $r^*rs = [r, rs]$ and if $\deg(r) = 1$ then $-r^*rs$ is reduced, hence $-r^*rs = [r, rs]$.

Next, note that $[q, r] = [[s, r]s^{-1}, r] = ([[s, r]s^{-1}, r]r^{-1})r$. By [Ore, Thm. 15, p. 490], this element equals $[r, rs]s^{-1}r^{-1}r = [r, rs]s^{-1}$. Thus $[q, r] = r^*rss^{-1} = r^*r$ if $\deg(r) = 2$ and $[q, r] = -r^*rss^{-1} = -r^*r$ if $\deg(r) = 1$. Since right-hand similarity coincides with left-hand similarity, by the symmetric argument we also have $[q, r]_l = r^*r$ if $\deg(q) = 2$ and $[q, r]_l = -r^*r$ if $\deg(q) = 1$. □

Proposition 4.3. *Suppose $f \in R$ is a non-distributive polynomial that belongs to the prime p. Write $f = pg$. Then g is non-distributive.*

Proof. Suppose g has two distinct left-hand prime divisors q and r. Since f is non-distributive, by Corollary 3.7 f is a skew-power of p, hence by Theorem 1.1 q and r are both similar to p. By the preceding lemma $[q, r]_l \in \mathbb{R}[x^2]$. Since g is left-hand divisible by q and r, g is left-hand divisible by $[q, r]_l$, and hence f is left-hand divisible by $[q, r]_l$. Thus f is left-hand divisible by the two distinct primes q, r, a contradiction. □

Corollary 4.4. *A reduced element $f \in R$ is non-distributive if and only if f has a unique[10] factorization into a product of primes.*

Proof. The "if" part of the claim already follows from the characterization of non-distributive elements as those that admit a unique left-hand prime divisor. The "only if" part follows from the preceding proposition by induction on the number of factors that appear in each factorization of f. □

It is unknown to the authors whether Corollary 4.4 holds for more general skew polynomial rings. This remains an intriguing open question.

In the present case of $R = \mathbb{C}[x, \bar{\cdot}]$, we shall now establish a concrete characterization of the non-distributive elements.

Remark 4.5. By [BGSZ15, Theorem 3.1], every prime in R is of degree 1 or 2. Let p be a prime in R. Then either p and p^* are relatively prime, or they are associates. In the latter case it follows that $p^* = -p$ if $p = x - a$ is linear, and $p^* = p$ if $p = x^2 + ax + b$ is quadratic.

[10] In the strict sense.

Lemma 4.6. *If p is a quadratic prime in R and $p = p^*$ then p^2 is non-distributive.*

Proof. The condition $p^* = p$ implies that $p = x^2 + a$ with $a \in \mathbb{R}$, and clearly $a > 0$ since p is prime. If p^2 factors as a product $p^2 = qr$ with q, r distinct primes, then $p^2 = (p^*)^2 = r^*q^*$. Thus r, q, r^*, q^* are all quadratic primes similar to p. If $r \neq q^*$ then by Lemma 4.2 we have $[q^*, r] = rr^* = q^*q$. Since p^2 is right-hand divisible by r and q^*, we deduce that $p^2 = [q^*, r] = qq^*$. If $r = q^*$ we also have $p^2 = qq^*$.

Write $q = x^2 + bx + c$. Then

$$x^4 + (\bar{c} + c - \bar{b}b)x^2 + \bar{c}c = qq^* = p^2 = x^4 + 2ax^2 + a^2$$

hence $|c| = a$ and $\bar{c} + c = 2a + |b|^2$. But then $2a + |b|^2 = |c + \bar{c}| \leq 2a$, hence $b = 0$. Thus $|c| = a$ and $\bar{c} + c = 2a$, from which it follows that $c = a$, hence $q = p = r$, a contradiction. □

Lemma 4.7. *The element x^2 is non-distributive.*

Proof. Obvisouly if $x^2 = (x - a)(x - b)$ then $a = b = 0$. □

Lemma 4.8. *If $p = x - a$ is a linear prime with $a \neq 0$, then $-pp^* = x^2 - |a|^2$ is distributive.*

Proof. We have $-p^* = x + \bar{a}$, hence $-pp^* = (x - a)(x + \bar{a}) = x^2 - |a|^2$. Then for any $b \in \mathbb{C}$ with $|b| = |a|$ we get $-pp^* = (x - b)(x + \bar{b})$, hence $-pp^*$ has infinitely many factorizations into products of primes. □

Definition 4.9. Let p, q be primes in R. We say that p and q are **amicable** if they are similar and any of the following conditions hold:

- $p = q = x$.
- $\deg(p) = 1$ and $p \neq -q^*$.
- $\deg(p) = 2$ and $p \neq q^*$.
- $\deg(p) = 2$ and $p = q = q^*$.

We note that the amicability relation is symmetric but not reflexive nor transitive.

Proposition 4.10. *Let p, q be similar primes. Then pq is non-distributive if and only if p and q are amicable.*

Proof. First, suppose pq is distributive. Then there exists a prime $r \neq q$ that divides pq from the right. By Lemma 2.1 and Theorem 1.1 we have $r_q = p$, hence $[r, q] = pq$. By Lemma 4.2 we have $[r, q] = q^*q$ if $\deg(p) = 2$ and $[r, q] = -q^*q$ if $\deg(p) = 1$. It follows that $p = q^*$ if $\deg(p) = 2$ and $p = -q^*$ if $\deg(p) = 1$. If $p = q = x$ then $pq = x^2$ is non-distributive by Lemma 4.7, a contradiction. If $\deg(p) = 2$ and $p = q = q^*$ then $pq = p^2$ is non-distributive by Lemma 4.6, a contradiction. Thus p, q are not amicable.

For the converse, first suppose that $\deg(p) = 1$ and $p = -q^*$ and $p \neq x$. Then by Lemma 4.8 pq is distributive.

Next, suppose that $\deg(p) = 2$, $p = q^*$ and $p \neq q$. Then $pq = q^*q = qq^* = qp$ admits p and q as distinct left-hand prime factors, hence pq is distributive. □

Theorem 4.11. *The non-distributive elements in R are precisely the elements of the form $p_1 \cdot \ldots \cdot p_k$, with $p_1, \ldots, p_k$ primes such that p_n, p_{n+1} are amicable for $n = 1, \ldots, k-1$.*

Proof. First, suppose $f \in R$ is non-distributive. By Corollary 4.4 f has a unique presentation $f = p_1 \cdot \ldots \cdot p_k$ as a product of primes. For each $1 \leq n < k$, the element $p_n \cdot p_{n+1}$ also has a unique presentation as a product of primes – otherwise we obtain a different factorization of f. Thus $p_n p_{n+1}$ is non-distributive, hence p_n, p_{n+1} are amicable by Proposition 4.10.

For the converse, we prove the claim by induction on k. For $k = 1$ the claim holds trivially. Suppose we have proven the claim for any element which is a product of k primes, and let f be an element of the form $p_1 \cdot \ldots \cdot p_k \cdot p_{k+1}$, with $p_1, \ldots, p_{k+1}$ primes such that p_n, p_{n+1} are amicable for $n = 1, \ldots, k$. If f is distributive, then it admits a left-hand prime factor $q \neq p_1$. Then by Lemma 2.2 ${}_{p_1}q$ is a left-hand prime divisor of $p_2 \cdot \ldots \cdot p_{k+1}$. By the induction hypothesis we have ${}_{p_1}q = p_2$, hence $[q, p_1]_l = p_1 p_2$. Thus $p_1 p_2$ is distributive, in contradiction with Proposition 4.10. □

Lemma 4.12. *The primes $x - a$ and $x - b$ in R are similar if and only if $|a| = |b|$.*

Proof. If $x - a, x - b$ are similar then by Lemma 4.2 we have $[x - a, x - b] = x^2 - |a|^2 = x^2 - |b|^2$, hence $|a| = |b|$.

Conversely, if $|a| = |b|$, then there exists $c \in \mathbb{C}$ such that $\bar{c}a = cb$ (writing $\frac{b}{a} = e^{-2i\theta}$, take $c = e^{i\theta}$). Let $f(x) = x - a + c$. Then one directly checks that $(x - b)f = (x - \frac{b(a-c)}{a})(x - a)$. Thus $[x - a, f] = (x - b)f$, hence $(x - a)_f = (x - b)$. □

By Lemma 4.12 and Definition 4.9, for non-distributive elements that belong to linear primes, Theorem 4.11 takes the following explicit form:

Corollary 4.13. *The non-distributive elements in R that belong to a linear prime are the elements of the form x^k, and those of the form $(x-a_1)\cdot\ldots\cdot(x-a_k)$ with $|a_n| = |a_{n+1}|$ and $a_n \neq -\overline{a_{n+1}}$ for $n = 1,\ldots,k-1$.*

5 A counter-example for differential skew polynomial rings

Let $K = \mathbb{C}(t)$ be the field of complex rational functions, and let $R = K[x, \frac{\partial}{\partial t}]$ be the skew polynomial ring over K with trivial automorphism and the usual derivation $\cdot' = \frac{\partial}{\partial t}$ on K. It is easy to see that the center of R is merely $\mathbb{C}$, hence no non-constant element can divide an element of the center. We now wish to give an example of a non-distributive element in R of the form pq with p, q **non-similar** primes.

Put $F(x) = (x+t)(x-t) = x^2 - (1+t^2)$. We first claim that F is non-distributive. Since $F(x)$ is a product of two primes in R, we must show that $(x+t)\cdot(x-t)$ is the only factorization of $F(x)$ into a product of primes. Indeed, if $F(x) = (x-h)(x-g) = x^2-(h+g)x-(g'+hg)$ for $h, g \in K$, then $h = -g$ and $-g'-g^2 = -g'+hg = -(1+t^2)$. The equation $y^2+y'-(1+t^2) = 0$ is a Ricatti equation, whose general solution is given by $y = u+t$, where u is a solution to the first order Bernoulli equation $u' + u^2 + 2tu = 0$. One checks that the latter equation has no non-zero rational solutions, hence the only function $g \in \mathbb{C}(t)$ satisfying $g^2 + g' - (1+t^2) = 0$ is $g = t$.

Next, we claim that $x+t, x-t$ are non-similar. This means that if $G \in R$ satisfies $[x+t, G] = (x-t)G$, then G is right-hand divisible by $x+t$. Indeed, if $[x+t, G] = (x-t)G$ then the evaluation $((x-t)G)(-t)$ of $(x-t)G$ at $-t$ is 0 (see [LL88, §2] for details on evaluation in skew polynomial rings). If $G(-t) \neq 0$ then by [LL88, Theorem 2.7] we have $(-t)^{G(-t)} \cdot G(-t) = 0$, where $(-t)^{G(-t)} = -t + \frac{G(-t)'}{G(-t)}$. Replacing t with $-t$ we obtain the linear ODE $t + \frac{y'}{y} = 0$, which clearly has no rational solutions: one gets $\ln(y) = -\frac{t^2}{2} + c$, hence $y = \exp(-\frac{t^2}{2} + c)$.

Thus the element F is non-distributive, but is not a skew power, demonstrating that Theorem 1.2 fails for $\mathbb{C}(t)[x, \frac{\partial}{\partial t}]$.

Bibliography

[BG12] J. Bergen and P. Grzeszczuk. Jacobson radicals of ring extensions. *Journal of Pure and Applied Algebra*, 216(12):2601–2607, 2012.

[BGSZ15] J. Bergen, M. Giesbrecht, P. Shivakumar, and Y. Zhang. Factorizations for difference operators. *Advances in difference equations*, 57(1):1–6, 2015.

[BU09] D. Boucher and F. Ulmer. Coding with skew polynomial rings. *Journal of Symbolic Computation*, 44(12):1644–1656, 2009.

[Coh63] P.M. Cohn. Non-commutative unique factorization domains. *Transactions of the American Mathematical Society*, 109:313–331, 1963.

[Coh95] P.M. Cohn. *Skew Fields: Theory of General Division Rings*. Cambridge University Press, 1995.

[GL94a] K. R. Goodearl and E. S. Letzter. Prime factor algebras of the coordinate ring of quantum matrices. *Proceedings of the American Mathematical Society*, 121:1017–1025, 1994.

[GL94b] K. R. Goodearl and E. S. Letzter. Prime ideals in skew and q-skew polynomial rings. *Memoirs of the American Mathematical Society*, 109(521), 1994.

[GTLN19] J. Gomez-Torrecillas, F.J. Lobillo, and G. Navarro. Computing the bound of an ore polynomial, applications to factorization. *Journal of Symbolic Computation*, 92(May-June):269–297, 2019.

[IM94] K. Ihora and F. Malikov. Rings of skew polynomials and gel'fand-kirillov conjecture for quantum groups. *Communications in Mathematical Physics*, 164(2):217–237, 1994.

[Jac37] N. Jacobson. Psuedo-linear transformations. *Annals of Mathematics*, 38(2):484–507, 1937.

[LL88] T. Y. Lam and A. Leroy. Vandermonde and wronsksian matrices over division rings. *Journal of Algebra*, 119:308–336, 1988.

[MPK19] U. Martinez-Penas and F.R. Kschischang. Evaluation and interpolation over multivariate skew polynomial rings. *Journal of algebra*, 525(1):111–139, 2019.

[NS20] E. Noether and W. Schmeidler. Moduln in nichtkommutativen bereichen, insbesondere aus differential und differenzenausdrcken. *Math. Z*, 8(1-2):1–35, 1920.

[Ore33] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.

[SZ02] S. P. Smith and J. J. Zhang. Fibers in ore extensions. *Algebras and Representation Theory*, 5(4):411–431, 2002.

[Tae06] L. Taelman. Dieudonne determinants for skew polynomial rings. *Journal of Algebra and its applications*, 05(01):89–93, 2006.