

Completely prime one-sided ideals in skew polynomial rings

Gil Alon and Elad Paran*

August 6, 2020

Abstract

Let $R = K[x, \sigma]$ be the skew polynomial ring over a field K , where σ is an automorphism of K of finite order. We show that prime elements in R correspond to completely prime one-sided ideals – a notion introduced by Reyes in 2010. This extends the natural correspondence between prime elements and prime ideals in commutative polynomial rings.

1 Introduction

Let K be a field, let σ be an automorphism of K , let δ be a derivation of K , and let $R = K[x, \sigma, \delta]$ be the skew polynomial ring, where multiplication is determined by the rule $xa = a^\sigma x + \delta(a)$ for any $a \in K$. This ring was first studied in Ore’s classical paper [Ore33], who showed that many of the fundamental properties of the commutative ring of polynomials $K[x]$ have natural analogues in R . Notably, the ring R is a left and right Euclidean domain, and is generally a noncommutative unique factorization domain. Since then, numerous works have studied these rings, and in particular their primes and prime ideal structure (for example in [Goo92], [GL94b], [GL94a]).

When attempting to define the notion of a “one-sided prime ideal” in noncommutative algebra, the common approach adapts Krull’s definition of a two-sided prime ideal: A left (right) ideal I in a ring R is called **of prime type** in [Koo71], or simply **prime** (for example in [Mic72],[Han75], [MS93], [HPT10]), if for any left (right) ideals A, B , the condition $AB \subseteq I$ implies

*Corresponding Author. Email: paran@openu.ac.il, Tel. 972-9-7781856, Fax. 972-9-7780856.

that $A \subseteq I$ or $B \subseteq I$. It is well-known that in skew polynomial rings there are generally “few” two-sided prime ideals, and even few one-sided prime ideals, in the above sense. For example, in $R = \mathbb{C}[x, \sigma]$, where σ denotes complex conjugation (and with the trivial derivation $\delta = 0$), the element $f = x^2 - 1$ is not prime, but the left ideal generated by f is (see Example 1 in §4 below). Thus here the analogy between $K[x]$ and $K[x, \sigma]$ fails, as in $K[x]$ prime elements stand in one-to-one correspondence with non-zero prime ideals.

In this note, we show that this aspect of the analogy between $K[x]$ and $K[x, \sigma]$ can be restored, if instead of one-sided prime ideals in the above sense, one works with completely prime one-sided ideals – a notion introduced by Reyes in [Rey10]. A left ideal I of a ring R is called **completely prime** if given $a, b \in I$ with $ab \in I$ and $Ib \subseteq I$, it follows that $a \in I$ or $b \in I$. We prove:

Theorem 1.1. *Let $R = K[x, \sigma]$, where σ is an automorphism of finite order of K , and let $0 \neq p \in R$. Then p is a prime element in R if and only if Rp is a completely prime left ideal.*

In [Rey10] and [Rey12] it is demonstrated that the notion of a completely prime one-sided ideal is, in some aspects, a “better” notion of a “one-sided prime ideal” in noncommutative algebra than the classical one mentioned above. Theorem 1.1 here gives further evidence of that.

We note that the forward direction of Theorem 1.1 holds in greater generality, for any skew polynomial ring $R = K[x, \sigma, \delta]$ (where σ is any automorphism and δ is any derivation), see Proposition 3.1 below. However, the converse generally fails: In section §4 we give examples demonstrating that the conditions that σ is of finite order and that $\delta = 0$ cannot be dropped.

The note is organized as follows. In §2 we recall some basic properties of skew polynomial rings. In §3 we prove Theorem 1.1. In §4 we give the counter-examples mentioned above.

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 . If $\delta = 0$ is trivial, we denote $R = K[x, \sigma]$, and if σ is the identity automorphism, we denote $R = K[x, \delta]$.

A polynomial $f \in R$ is called **reduced** if its leading term is 1 (i.e. f is monic). A reduced polynomial is said to be **prime** if it cannot be written

as a product of two non-constant polynomials¹. 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 $f, g \in R$, their **union** [Ore33, p. 485] is a reduced polynomial of minimal degree that is right-hand divisible by both f and g . The union $[f, g]$ is determined uniquely by f and g .

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]². 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 **similar** if $h = f_g$ is a special transform of f for some $g \in R$ relatively prime to f . If h is similar to f and f is prime, then so is h [Ore33, p. 493].

The following claim [Ore33, Theorem 11, p. 489] will be particularly useful for our needs:

Lemma 2.1. *Let $f, g, h \in R$. If $fg \in Rh$, then $f \in Rh_g$.*

The ring R is a unique factorization domain, in the following sense [Ore33, Theorem 1, p. 494]:

Theorem 2.2. *Every reduced element in R can be uniquely written as a product of primes, up to order of terms and similarity.*

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

Given an element $f \in R$ and $a \in K$, there exists a unique scalar $f(a) \in K$ (the **substitution** of a in f) such that $f - f(a) \in R(x - a)$. Substitution is generally not a homomorphism, however it satisfies the following product rule [LL88, Theorem 2.7]:

Proposition 2.3. *For $f, g \in R$ and $a \in K$ we have $(fg)(a) = 0$ if $g(a) = 0$, and $(fg)(a) = f(a^{g(a)})g(a)$ if $g(a) \neq 0$, where $a^b = b^\sigma ab^{-1} + \delta(b)$ for any $a, b \in K$ with $b \neq 0$.*

3 Proof of Theorem 1.1

We begin by proving the forward direction of Theorem 1.1.

¹Ore does not consider non-reduced irreducible polynomials as “prime”. We follow the same convention.

²Ore denotes the transform by $gf(x)g^{-1}$. We prefer the compact notation f_g .

Proposition 3.1. *Let $R = K[x, \sigma, \delta]$ be a skew polynomial ring, where K is field, σ an automorphism of K , and δ a derivation on K . Let p be a prime element in R . Then Rp is a completely prime left ideal.*

Proof. Suppose $a, b \in R$ satisfy $ab \in Rp$, $b \notin Rp$, and $Rpb \subseteq Rp$. In particular, $pb \in Rp$, hence by Lemma 2.1 p is right-hand divisible by p_b . But since p and b are relatively prime, the transform p_b is special, thus $\deg(p_b) = \deg(p)$ and hence $p_b = p$. Since $ab \in Rp$, by Lemma 2.1 a is right-hand divisible by $p_b = p$, as needed. \square

For the rest of this section fix a field K , let σ be an automorphism of K of finite order n , and let R be the skew polynomial ring $K[x, \sigma]$. Let L be the fixed field of σ in K , and let R' be the center R . One checks directly that $R' = L[x^n]$.

For an element $g \in R$, we denote by Rg the left ideal generated by g (as we have done in the preceding section), and by RgR the two-sided ideal generated by g . Recall that g is called **invariant** if $Rg \subseteq gR$, equivalently if $Rg = gR = RgR$. Note that $RxR = Rx$ is the ideal of polynomials g whose constant term $g(0)$ is 0.

Lemma 3.2. *Let g be a reduced polynomial in R with $g \notin Rx$. If g is invariant then $g \in R'$.*

Proof. We have $gx \in RgR = Rg$, hence $gx = pg$ for a necessarily linear polynomial $p = \alpha x + \beta$, $\alpha, \beta \in K$. By comparing leading coefficients, we get $\alpha = 1$. Then $\beta g = pg - xg = gx - xg \in RxR = Rx$, hence $\beta = 0$ since $g \notin Rx$. Thus $p = x$, hence g commutes with x .

Similarly, given a scalar $\alpha \in K$, we have $g\alpha = \beta g$ for some $\beta \in K$. Then $g(0)\alpha = \beta g(0)$, hence $\alpha = \beta$. Thus g commutes with all scalars. Since R is generated by x and K , we have $g \in R'$. \square

Definition 3.3. We say that a polynomial $f \in R$ is **center-free** if there exists no non-constant polynomial $c \in R'$ that divides f from the left (or from the right).

Clearly, every nonzero element of R can be written in the form cf with c a reduced polynomial in R' and f center-free.

Corollary 3.4. *Let $f \in R$ be center-free with $f \notin Rx$. Then $RfR = R$.*

Proof. Since the two-sided ideal RfR is also a left ideal, we may write $RfR = Rg$ for some reduced polynomial $g \in R$. Then $RgR = (RfR)R = RfR = Rg$. Since $f \notin Rx$, we also have $g \notin Rx$. By the preceding lemma, $g \in R'$. Since $f \in RfR = gR = Rg$ and f is center-free, g must be a (non-zero) constant, hence $RfR = R$. \square

Lemma 3.5. *If a, b, c, d are reduced elements of R , with a and c center-free, $b, d \in R'$, and $ab = cd$, then $a = c$.*

Proof. Let m be the maximal integer such that $a \in Rx^m$. Since a is center-free and $R' = L[x^n]$, we have $m < n$. Similarly, if k is the maximal integer such that $c \in Rx^k$, then $k < n$. Since $b, d \in L[x^n]$, by comparing the lowest degree monomials in ab and cd , we must have $k = m$. Replace a, c with $x^{-m}a, x^{-m}c$ to assume that $a, b \notin RxR$. Since $b \in R'$, we have $RabR = bRaR$. By the preceding corollary, $RaR = R$, hence $RabR = bR$. Similarly, $RcdR = dR$. Thus $bR = dR$, hence $b = d$, hence $a = c$. \square

The proof of the following lemma is 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 3.6. *For each $0 \neq f \in R$ there exists a polynomial $h \in R$ such that hf is a reduced polynomial in R' .*

Lemma 3.7. *For each $0 \neq f \in R$ there exists a unique polynomial $f^* \in R$ of minimal degree such that f^*f is a reduced polynomial in R' .*

Proof. The existence part of the claim follows from Lemma 3.6. To prove the uniqueness, write $f = f_n x^n + \dots + f_0$ and suppose that g, h are both of minimal degree k such that $gf, hf \in R'$. If $k = 0$, then we must have $gf_n = hf_n = 1$, hence $g = h$. If $k > 0$ and $g \neq h$, then $g - h = \sum_{i=0}^m (g_i - h_i)x^i$ for some $m < n$ with $g_m \neq h_m$. Then $(g - h)f = gf - hf \in R' = L[x^n]$. The leading coefficient $\alpha = (g_m - h_m)(f_n^{\sigma^m})$ of $gf - hf$ thus belongs to L , hence $(\alpha^{-1}(g - h))f$ is a reduced polynomial in R' , and $\deg(\alpha^{-1}(g - h)) < k$, a contradiction. \square

Definition 3.8. We call the element f^* given by Lemma 3.7 the **dual** of f .

Note that since $f^*f \in R'$, we have $ff^* = f^*f$. (Indeed, $(f^*f)f = f(f^*f) = (ff^*)f$, hence $ff^* = f^*f$.)

Lemma 3.9. *If $f \in R$ and $\alpha \in K^\times$ is a constant, then $(\alpha f)^* = f^* \alpha^{-1}$.*

Proof. We have $(f^* \alpha^{-1})(\alpha f) = f^* \alpha \cdot \alpha^{-1} f = f^* f$. If $g \in R$ is such that $c = g(\alpha f)$ is a reduced element in R' , then also $c = \alpha fg$, hence $fg = c \alpha^{-1}$, hence $f(g\alpha) = ((g\alpha)f) = c$, hence $\deg(g) = \deg(g\alpha) \geq \deg(f^*) = \deg(f^* \alpha^{-1})$. Thus $(\alpha f)^* = f^* \alpha^{-1}$. Note that if f is a non-zero constant, then $f^* = f^{-1}$. \square

Corollary 3.10. *If $f \in R$ is center-free then $f^{**} = f$.*

Proof. By Lemma 3.9 may divide f from the left by its leading coefficient to assume that f is reduced, hence also f^* is reduced.

We have $f^*f = ff^* \in R'$. Suppose that $g \in R$ is a polynomial such that $c = gf^*$ is a reduced polynomial in R' . Necessarily, g is reduced. Write $g = hd$ with h center-free and $d \in R'$ reduced. Then also h is reduced. We have $cf = gf^*f = h(df^*f)$, hence by Lemma 3.5 we get $f = h$, which implies that $\deg(f) \leq \deg(g)$. Thus we have $(f^*)^* = f$. □

Proposition 3.11. *Let $f, g \in R$ with fg center-free. Then $(fg)^* = g^*f^*$.*

Proof. By Lemma 3.9 may divide f and g from the left by their leading coefficients to assume that both are reduced, hence also f^*, g^* are reduced. The polynomial

$$(g^*f^*)(fg) = g^*(f^*f)g = (g^*g)(f^*f)$$

is a reduced element in R' . As in the proof of Corollary 3.10, suppose that $d \in R'$ and $h \in R$ are reduced elements with h center-free such that $c = (dh)(fg) \in R'$ is reduced. Then $c(g^*f^*) = (dh)(fg)(g^*f^*) = h(dgg^*ff^*)$, hence by Lemma 3.5 we have $g^*f^* = h$, therefore $\deg(dh) \geq \deg(g^*f^*)$. Thus $(fg)^* = g^*f^*$. □

Lemma 3.12. *Let h be an arbitrary non-zero element of R . Then h^* is center-free.*

Proof. We may assume, without loss of generality, that h is reduced. Write $h^* = fc$ with f, c reduced, $c \in R'$ and f center-free. Let g be an arbitrary polynomial in R . We have

$$(h^*h)fg = fg(hh^*) = fghfc = fcghf = h^*ghf$$

Cancelling h^* from the left, we get that $(hf)g = g(hf)$. Thus $hf \in R'$. By the definition of the dual, we must have $\deg(f) \geq \deg(h^*)$, hence c must be a constant. □

Corollary 3.13. *If $p \in R$ is prime and $p \notin R'$, then p^* is also prime.*

Proof. Suppose that $p^* = fg$ with both $f, g \in R$ non-constants. By Corollary 3.10 we have $p = (p^*)^*$. By the preceding lemma, p^* is center-free, hence by Proposition 3.11, $(p^*)^* = g^*f^*$. Thus $p = g^*f^*$, hence either $g^* \in K$ or $f^* \in K$. Then by the definition of the dual, either f or g is an associate of an element of R' , hence p is divisible by a non-constant element of R' , a contradiction. □

Proof of Theorem 1.1. The forward direction of the theorem is given by Proposition 3.1. For the converse, suppose p is composite and that Rp is completely prime. Write $p = cf$ with $c \in R'$ and f center-free. Then $pc = cp \in Rp$ hence $Rpc \subseteq Rp$. Then, since Rp is completely prime, either $f \in Rp$ or $c \in Rp$, which implies that either f or c is a constant. First suppose that f is a constant. Then c is an associate of p , and since p is composite we may write $c = ab$ with a, b non-constants. Then $cb = bc \in Rc$, hence $Rcb \subseteq Rc = Rp$ and hence $a \in Rc$ or $b \in Rc$, a contradiction.

Next suppose that c is a constant. Then f is center-free and composite. Let q be a left-hand prime divisor of f , and write $f = qh$ with h non-constant. Then $h(q^*q) = q^*qh = q^*f \in Rf$. Since $q^*q \in R'$ and since $Rf = Rp$ is completely prime, it follows that $h \in Rf$ or $q^*q \in Rf$. The first option cannot be since $\deg(h) < \deg(f)$, hence $q^*q = df = dqh$ for some $d \in R$. Since f is center-free, so is q , hence by Corollary 3.13, q^* is prime. Since h is a non-constant, by the unique factorization in R it follows that d must be a non-zero constant. Thus $f = (q^*q)d^{-1}$ is left-hand divisible by $q^*q \in R'$, in contradiction with f being center-free. \square

4 Some counter-examples

One might initially expect a correspondence between prime ideals and prime elements in skew polynomial rings. In Example 1 below we give a counter-example to this, which motivated this paper. We first prove the following:

Proposition 4.1. *Let K be a field, σ an automorphism of K and δ a derivation on K . Let $R = K[x, \sigma, \delta]$ and let $z \in K$. Then the left ideal $R(x - z)$ in R is prime, in the sense of [Mic72] or [Han75].*

Proof. Write $g = x - z$, and suppose $a, b \in R$ are such that $(Ra)(Rb) \subseteq Rg$. That is, $afb \in Rg$ for all $f \in R$. Suppose $b \notin Rg$, that is, $b(z) \neq 0$, and put $\beta = b(z)$. Take $f = x - z^\beta + \beta^{-1}$. Then by the product formula (Proposition 2.3), $(fb)(z) = f(z^\beta)\beta = \beta^{-1}\beta = 1$. Again by the product formula, we have $(afb)(z) = a(z^1) \cdot 1 = a(z)$. Thus $a(z) = 0$, hence $a \in R(x - z)$. \square

Lemma 4.2. *Let $R = \mathbb{C}[x, \sigma]$, where σ denotes complex conjugation, and let $z, w \in \mathbb{C}$ with $|z| = |w| = 1$ and $z \neq w$. If $f \in R(x - z)$ and $f \in R(x - w)$, then $x \in R(x^2 - 1)$.*

Proof. By [AP20, Lemma 4.12], the primes $x - z$ and $x - w$ in R are similar, and by [AP20, Lemma 4.2] the union $[x - z, x - w]$ is $x^2 - 1$, hence $f \in R(x^2 - 1)$. \square

Example 1. Let $R = \mathbb{C}[x, \sigma]$, where σ denotes complex conjugation. Consider the non-prime element $g = x^2 - 1 = (x - 1)(x + 1)$, which belongs to the center $\mathbb{R}[x^2]$ of R . The ideal $Rg = gR$ in R is prime. Indeed, suppose $a, b \in R$ are such that $(Ra)(Rb) \subseteq Rg$. That is, $afb \in Rg$ for all $f \in R$. Note that for any $z \in \mathbb{C}$ with $|z| = 1$ we have $g = (x + z^\sigma)(x - z)$, hence $afb \in R(x - z)$ for all $f \in R$. Since $R(x - z)$ is prime by Proposition 4.1, this implies that for such z we have $a \in R(x - z)$ or $b \in R(x - z)$. Thus at least one of a and b belongs to infinitely many such ideals $R(x - z)$, which implies that it belongs to $R(x^2 - 1)$, by the preceding lemma.

We now wish to show that the assertion of Theorem 1.1 fails for the rings $K[x, \sigma]$ and $K[x, \delta]$, where $K = \mathbb{C}(t)$ is the field of complex rational functions in the variable t , δ is the differentiation map on K , and σ is the \mathbb{C} -automorphism given by $t \rightarrow t + 1$. Clearly, σ is of infinite order. Note that if $f \in \mathbb{C}(t)$ is fixed by σ , then f is a scalar in \mathbb{C} .

Lemma 4.3. Let $R = K[x, \sigma]$ or $R = K[x, \delta]$. The polynomials $x - t$ and $x + t$ are not similar in R .

Proof. If $R = K[x, \delta]$, then the lemma is proven in [AP20, §5]. If $R = K[x, \sigma]$ and $x - t$ is similar to $x + t$ in R , then there exists a reduced polynomial $f \in R$ with $f(t) \neq 0$ such that $[x - t, f] = (x + t)f$. Then $((x + t)f)(t) = 0$, hence by Proposition 2.3 we have $0 = t^{f(t)} + t = f(t + 1)tf(t)^{-1} + t = t(f(t + 1)f(t)^{-1} + 1)$, hence $f(t + 1) = -f(t)$. Then $f(t + 2) = -f(t + 1) = f(t)$, which implies that $f(t)$ is a scalar in \mathbb{C} . Since f is reduced, we have $f = 1$ and $[x - t, f] = x - t$, a contradiction. \square

The following proposition is proven in [AP20, §5] in the case where $R = K[x, \delta]$. The proof in the case $R = K[x, \sigma]$ is technical, and we postpone it to the appendix below.

Proposition 4.4. Let $R = K[x, \sigma]$ or $R = K[x, \delta]$. The polynomial $g = (x + t)(x - t)$ has a unique presentation³ as a product of primes in R . That is, $x - t$ is the only right-hand prime divisor of g .

Even though $(x + t)(x - t)$ is obviously not a prime in $K[x, \sigma]$ or $K[x, \delta]$, we have:

Proposition 4.5. Let $R = K[x, \sigma]$ or $R = K[x, \delta]$ and let $g = (x + t)(x - t)$ in R . The left ideal Rg is completely prime.

³Not even up to order or similarity.

Proof. Suppose that $a, b \in R$ satisfy $ab \in Rg, Rgb \subseteq Rg$. In particular, $gb \in Rg \subseteq R(x-t)$. First, suppose that $b \in R(x-t)$ and write $b = c(x-t)$ for some $c \in R$. Then $gc \in R(x+t)$. If $c \in R(x+t)$ then $b \in Rg$ and we are done. Suppose that $c \notin R(x+t)$. By Lemma 2.1 we have $g \in R((x+t)_c)$. By Proposition 4.4 we have $(x-t) = (x+t)_c$, hence $x-t$ and $x+t$ are similar, in contradiction with Lemma 4.3.

Next, suppose that $b \notin R(x-t)$. Then $(x-t)_b$ is prime. By Lemma 2.1, since $gb \in R(x-t)$, we have $g \in R((x-t)_b)$. By the unique factorization of g , we have $(x-t)_b = x-t$. That is, $[x-t, b] = (x-t)b$, which implies by Proposition 2.3 that $t^{b(t)} = t$. If $R = K[x, \delta]$, then this implies that $b(t)'b(t)^{-1} = 0$, hence $b(t)$ is a scalar $\beta \in \mathbb{C}^\times$. Similarly, if $R = K[x, \sigma]$, we get $b(t+1)tb(t)^{-1} = t$, hence $b(t+1) = b(t)$, which again implies that $b(t)$ is a scalar $\beta \in \mathbb{C}^\times$.

By left division with remainder in the ring R , we have $b = h(x-t) + b(t) = h(x-t) + \beta$ for some $h \in R$. Since $gb = gh(x-t) + g\beta = gh(x-t) + \beta g \in Rg$, we have $gh(x-t) \in Rg$, hence $gh \in R(x+t)$. If $h \notin R(x+t)$, then by Lemma 2.1, $g \in R((x+t)_h)$, which by the unique factorization of g implies that $(x-t) = (x+t)_h$, in contradiction with Lemma 4.3. Thus $h = f(x+t)$ for some $f \in R$. Then since $ab = a(fg + \beta) = afg + a\beta \in Rg$ we have $a\beta = \beta a \in Rg$, hence $a \in Rg$, as needed. \square

Appendix: Proof of Proposition 4.4

With the notation of §4, let $R = K[x, \sigma]$ and let $g = (x+t)(x-t) = x^2 - x - t^2$. To prove Proposition 4.4, we must show that the only zero of g in K is t . Suppose $a \in K$ satisfies $g(a) = 0$. Then⁴ we have $aa^\sigma - a = t^2$. Write $a = \frac{p(t)}{q(t)}$ with $p(t), q(t) \in \mathbb{C}[t]$, $q(t) \neq 0$. We may assume without loss of generality that p and q are coprime. We now have $p(t)p(t+1) - p(t)q(t+1) = t^2q(t)q(t+1)$, hence

$$p(t)(p(t+1) - q(t+1)) = t^2q(t)q(t+1)$$

If $\deg(p) \leq \deg(q)$, then the degree of the left-hand side is at most $\deg(p) + \deg(q)$, while the degree of the right-hand side is $2 + 2\deg(q)$, a contradiction. Thus $\deg(p) > \deg(q)$ and we get $2\deg(p) = 2 + 2\deg(q)$, hence $\deg(p) = \deg(q) + 1$.

Suppose $p(0) \neq 0$. Then, since p and q are coprime, p must divide $q(t)^\sigma = q(t+1)$. Write $q^\sigma = ph$ for $h \in \mathbb{C}[t]$. Then $p(p^\sigma - ph) = t^2p^{\sigma-1}h^{\sigma-1}ph$, hence $p^\sigma - ph = t^2p^{\sigma-1}h^{\sigma-1}h$, which implies that h divides p^σ . Since p and

⁴Substitution of a in x^2 gives $a^\sigma a$.

q are coprime, so are p^σ, q^σ , hence h must be a (non-zero) constant. Then $\deg(q) = \deg(q^\sigma) = \deg(p)$, a contradiction.

Thus $p(0) = 0$, and we may write $p = t^m r$ with $m \geq 1$ and $r \in \mathbb{C}[t]$ coprime to q and t . Then $t^m r((t+1)^m r^\sigma - q^\sigma) = t^2 q q^\sigma$, and since r is coprime to q and t , r must divide q^σ . Write $q^\sigma = hr$ for $h \in \mathbb{C}[t]$. We then get $t^m r((t+1)^m r^\sigma - hr) = t^2 h^{\sigma^{-1}} r^{\sigma^{-1}} hr$, hence $t^m((t+1)^m r^\sigma - hr) = t^2 h^{\sigma^{-1}} r^{\sigma^{-1}} h$, hence h must divide $t^m(t+1)^m r^\sigma = t^m p^\sigma$. Since p^σ, q^σ are coprime, h must divide t^m . Write $h = \alpha t^k$ with $\alpha \in \mathbb{C}^\times$ and $0 \leq k \leq m$. Then $p = t^m r, q^\sigma = \alpha t^k r$. Since $\deg(p) = \deg(q) + 1 = \deg(q^\sigma) + 1$, we must have $m = 1 + k$. We then have $t^{k+1}((t+1)^{k+1} r^\sigma - \alpha t^k r) = \alpha^2 t^2 (t-1)^k r^{\sigma^{-1}} t^k$. Dividing by t^{k+1} , we get

$$(t+1)^{k+1} r^\sigma - \alpha t^k r = \alpha^2 t (t-1)^k r^{\sigma^{-1}}$$

Suppose that $k > 0$. Substituting $t = 0$ in the last equation we get that $r^\sigma(0) = 0$, hence $r(1) = 0$. Substituting $t = 1$ in the same equation, we get that $r^\sigma(1) = 0$, hence $r(2) = 0$. We claim that $r(i) = 0$ for all $i \in \mathbb{N}$. Indeed, suppose we have proven the claim for all $i = 1, \dots, n$, with $n > 1$. In particular, $r(n-1) = 0$, hence $r^{\sigma^{-1}}(n) = 0$. Putting $t = n$, we get that $r^\sigma(n) = 0$, hence $r(n+1) = 0$, as claimed. It follows that $r = 0$, hence $q = 0$, a contradiction.

Thus $k = 0$, and we have

$$(t+1)r^\sigma - \alpha r = \alpha^2 t r^{\sigma^{-1}}$$

Putting $t = 0$ in this equation, we get $r(1) = \alpha r(0)$. Note that since r is coprime to t , $r(0) \neq 0$. Putting $t = 1$, we get that $2r(2) - \alpha^2 r(0) = \alpha^2 r(0)$, hence $r(2) = \alpha^2 r(0)$. We prove by induction that $r(n) = \alpha^n r(0)$ for all $n \in \mathbb{N}$. Indeed, assume the claim holds up to a given $n > 1$, then putting $t = n$ in the last presented equation we get $(n+1)r(n+1) - \alpha \cdot \alpha^n r(0) = \alpha^2 n \cdot \alpha^{n-1} r(0)$, hence $(n+1)r(n+1) = \alpha^{n+1}(n+1)r(0)$, hence $r(n+1) = \alpha^{n+1} r(0)$, which completes the induction.

Thus the polynomial $r(t)r(0)^{-1}$ coincides with the function $t \mapsto \alpha^t$ at infinitely many points, which can only happen for $\alpha = 1$. Thus $r(n) = r(0)$ for all $n \in \mathbb{N}$, hence r must be a constant. We thus have $p = tr, q^\sigma = r$, hence also $q = r$. Then $\frac{p}{q} = t$, as claimed.

References

- [AP20] G. Alon and E. Paran. On the structure of skew polynomial rings. (preprint), 2020.

- [BGSZ15] J. Bergen, M. Giesbrecht, P. Shivakumar, and Y. Zhang. Factorizations for difference operators. *Advances in difference equations*, 57(1):1–6, 2015.
- [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.
- [Goo92] K. R. Goodearl. Prime ideals in skew polynomial rings and quantized weyl algebras. *Journal of algebra*, 150(2):324–377, 1992.
- [Han75] F. Hansen. On one-sided prime ideals. *Pacific Journal of mathematics*, 58(1):79–85, 1975.
- [HPT10] Y. Hirano, E. Poon, and H. Tsutsui. On rings in which every ideal is weakly prime. *Bulletin of the Korean mathematical society*, 47(5):1077–1087, 2010.
- [Koo71] K. Koo. On one sided ideals of a prime type. *Proceedings of the American Mathematical Society*, 28(2):321–329, 1971.
- [LL88] T. Y. Lam and A. Leroy. Vandermonde and wronskian matrices over division rings. *Journal of Algebra*, 119:308–336, 1988.
- [Mic72] G. O. Michler. Prime right ideals and right noetherian rings. *Ring Theory, proceedings of a Conference on Ring Theory Held in Park City, Utah, March 26, 1971*, pages 251–255, 1972.
- [MS93] R. L. McCasland and P. F. Smith. Prime submodules of noetherian modules. *Rocky mountain journal of mathematics*, 23(3):1041–1062, 1993.
- [Ore33] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.
- [Rey10] M. L. Reyes. A one-sided prime ideal principle for noncommutative rings. *Journal of algebra and its applications*, 9(6):877–919, 2010.
- [Rey12] M. L. Reyes. Noncommutative generalizations of theorems of cohen and kaplansky. *Algebras and Representation theory*, 15(5):933–975, 2012.