PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 11, November 2012, Pages 3739–3747
S 0002-9939(2012)11268-7
Article electronically published on March 12, 2012

# INVARIANT POLYNOMIALS OF ORE EXTENSIONS BY $q$-SKEW DERIVATIONS

CHEN-LIAN CHUANG, TSIU-KWEN LEE, AND CHENG-KAI LIU

(Communicated by Harm Derksen)

Abstract. Let $R$ be a prime ring with the symmetric Martindale quotient ring $Q$. Suppose that $\delta$ is a quasi-algebraic $q$-skew $\sigma$-derivation of $R$. For a minimal monic semi-invariant polynomial $\pi(t)$ of $Q[t;\sigma,\delta]$, we show that $\pi(t)$ is also invariant if $\operatorname{char} R = 0$ and that either $\pi(t) - c$ for some $c \in Q$ or $\pi(t)^p$ is a minimal monic invariant polynomial if $\operatorname{char} R = p \geq 2$. As an application, we prove that any $R$-disjoint prime ideal of $R[t;\sigma,\delta]$ is the principal ideal $\langle p(t)\rangle$ for an irreducible monic invariant polynomial $p(t)$ unless $\sigma$ or $\delta$ is X-inner.

## 1. Introduction

It will be assumed throughout that $R$ is an associative prime ring in the sense that for any $a, b \in R$, $aRb = 0$ implies $a = 0$ or $b = 0$. Let $\sigma$ be an automorphism of $R$. By a $\sigma$-derivation of $R$, we mean a map $\delta\colon R \to R$ satisfying

$$\delta(x+y) = \delta(x) + \delta(y) \quad \text{and} \quad \delta(xy) = \delta(x)y + \sigma(x)\delta(y)$$

for all $x, y \in R$. Given $b \in R$, the map $\mathrm{ad}_{b,\sigma}\colon x \in R \mapsto bx - \sigma(x)b$ defines a $\sigma$-derivation of $R$, called the inner $\sigma$-derivation defined by $b$. Analogously, for a unit $u \in R$, the map $\mathrm{I}_u\colon x \in R \mapsto uxu^{-1}$ defines an automorphism of $R$, called the inner automorphism defined by the unit element $u$.

Let $Q$ be the symmetric Martindale quotient ring of $R$. The center of $Q$, denoted by $C$, is called the extended centroid of $R$. (See [1, Chapter 2] for details.) The $\sigma$-derivation $\delta$ of $R$, together with its automorphism $\sigma$, can be uniquely extended to a $\sigma$-derivation of $Q$ [15, Lemma 1]. A $\sigma$-derivation of $R$ is called X-inner if its extension to $Q$ is equal to $\mathrm{ad}_{b,\sigma}$ for some $b \in Q$. An automorphism of $R$ is called X-inner if its extension to $Q$ is equal to $\mathrm{I}_u$ for some unit $u \in Q$. Following [14], define for each integer $j$ the $C$-space

$$\Phi(j) \stackrel{\text{def.}}{=} \{u \in Q \mid ur = \sigma^j(r)u \text{ for all } r \in Q\}.$$

By [22, Chapter 3, Lemma 12.1], any $0 \neq u \in \Phi(j)$ is a unit such that $\sigma^j = \mathrm{I}_u$. We recall a very useful property due to Kharchenko and Popov [15].

**Lemma 1.1.** *If $\delta$ is an X-outer $\sigma$-derivation, then $\sigma(\alpha) = \alpha$ and either $\delta(\alpha) = 0$ or $\sigma = I_{\delta(\alpha)}$ for each $\alpha \in C$.*

---

Received by the editors June 29, 2010 and, in revised form, April 28, 2011.
2010 *Mathematics Subject Classification.* Primary 16S36, 16N60, 16W25, 16R50.
*Key words and phrases.* Prime ring, (semi-)invariant polynomial, $q$-skew $\sigma$-derivation.
The first two authors are members of the Mathematics Division, NCTS (Taipei Office).

*Proof.* Given $\alpha \in C$ and $x \in R$, $\delta(\alpha x) = \delta(\alpha)x + \sigma(\alpha)\delta(x)$ and $\delta(x\alpha) = \delta(x)\alpha + \sigma(x)\delta(\alpha)$ yield $(\sigma(\alpha) - \alpha)\delta(x) = \sigma(x)\delta(\alpha) - \delta(\alpha)x$. So $\sigma(\alpha) = \alpha$ and $\sigma(x)\delta(\alpha) - \delta(\alpha)x = 0$ by the outerness of $\delta$. Since $x \in R$ is arbitrary, $\delta(\alpha) \neq 0$ implies $\sigma = \mathrm{I}_{\delta(\alpha)}$ by [22, Chapter 3, Lemma 12.1]. □

We shall need the following generalization of Lemma 1.1.

**Lemma 1.2.** *Let $\delta$ be an X-outer $\sigma$-derivation. For a unit $u \in Q$, if $\delta\, I_u = \gamma\, I_u \delta$, where $\gamma \in C$, then $\sigma(u) = \gamma u$ and either $\delta(u) = 0$ or $\sigma = I_{u^{-1}\delta(u)}$.*

*Proof.* Expand $0 = \delta(1) = \delta(uu^{-1}) = \delta(u)u^{-1} + \sigma(u)\delta(u^{-1})$. We see that $\delta(u^{-1}) = -\sigma(u)^{-1}\delta(u)u^{-1}$. With this, we compute for $x \in R$

$$\begin{aligned}\delta\mathrm{I}_u(x) &= \delta(uxu^{-1}) = \delta(u)xu^{-1} + \sigma(u)\delta(x)u^{-1} + \sigma(u)\sigma(x)\delta(u^{-1})\\ &= \delta(u)xu^{-1} + \sigma(u)\delta(x)u^{-1} - \sigma(u)\sigma(x)\sigma(u)^{-1}\delta(u)u^{-1}.\end{aligned}$$

The assumption $\delta\mathrm{I}_u(x) = \gamma\mathrm{I}_u\delta(x) = \gamma u\delta(x)u^{-1}$ gives the identity

$$\delta(u)xu^{-1} + \big(\sigma(u) - \gamma u\big)\delta(x)u^{-1} - \sigma(u)\sigma(x)\sigma(u)^{-1}\delta(u)u^{-1} = 0.$$

But $\delta$ is X-outer. By [15, Theorem 1], $\sigma(u) = \gamma u$ and for $x \in R$,

$$\begin{aligned}0 &= \delta(u)xu^{-1} - \sigma(u)\sigma(x)\sigma(u)^{-1}\delta(u)u^{-1}\\ &= \delta(u)xu^{-1} - (\gamma u)\sigma(x)(\gamma u)^{-1}\delta(u)u^{-1}\\ &= \delta(u)xu^{-1} - u\sigma(x)u^{-1}\delta(u)u^{-1} = u(u^{-1}\delta(u)x - \sigma(x)u^{-1}\delta(u))u^{-1}.\end{aligned}$$

So $u^{-1}\delta(u) \in \mathrm{I}_\sigma$. If $\delta(u) \neq 0$, then $\sigma = \mathrm{I}_{u^{-1}\delta(u)}$, as asserted. □

The Ore extension of $R$ by a $\sigma$-derivation $\delta$, denoted by $R[t;\sigma,\delta]$, is the set of polynomial expressions $a_0 + a_1t + \cdots + a_nt^n$, where $a_0, \ldots, a_n \in R$, with componentwise addition and multiplication subjected to the rule $tr = \sigma(r)t + \delta(r)$ for all $r \in R$. We form $Q[t;\sigma,\delta]$ analogously. Ore extensions have been extensively investigated in various directions. In the study of $R[t;\sigma,\delta]$, two crucially important notions are the notion of a right invariant polynomial and that of a semi-invariant polynomial. We omit "right" here for brevity and recall the definition below.

**Definition 1** ([16, 17, 18, 20])**.** We call $f(t) \in Q[t;\sigma,\delta]$ a cv-polynomial if it is associated to an automorphism $\tau$ of $Q$ such that $f(t)r - \tau(r)f(t) \in Q$ for any $r \in R$. A cv-polynomial $f(t)$ is called *semi-invariant* if $f(t)r - \tau(r)f(t) = 0$ for all $r \in R$. A semi-invariant polynomial $f(t)$ is called *invariant* if additionally $f(t)t = (at + b)f(t)$ for some $a, b \in Q$. A (semi-)invariant polynomial is called *minimal* if it is nonconstant and its degree is minimal among all nonconstant (semi-)invariant polynomials.

The importance of these polynomials is based on the following: cv-polynomials determine $R$-stable homomorphisms from other Ore extensions of $R$ into $R[t;\sigma,\delta]$ ([18] or [8, Theorem 12]). Semi-invariant polynomials determine the algebraic dependency of $\delta$ ([5]). Invariant polynomials determine the ideal structure of $R[t;\sigma,\delta]$ ([17, 20]). In particular, $R[t;\sigma,\delta]$ has nontrivial $R$-disjoint ideals iff $R[t;\sigma,\delta]$ has nonconstant (semi-)invariant polynomials ([20, Theorem 2.6]). For a simple ring $R$, $R[t;\sigma,\delta]$ is simple iff $R[t;\sigma,\delta]$ has no nonconstant (semi-)invariant polynomials. (Semi-)invariant polynomials for X-inner skew derivations can be found easily as follows.

**Lemma 1.3.** *If $\delta = ad_{b,\sigma}$, where $b \in Q$, then $\pi(t) \overset{\text{def.}}{=} t-b$ is the minimal invariant polynomial.*

*Proof.* Clearly, $\pi(t)r = \sigma(r)\pi(t)$ for $r \in R$. Also,

$$\begin{aligned}(t-b)t &= (t-b)(t-b+b) = (t-b)^2 + (t-b)b \\ &= (t-b)^2 + \sigma(b)(t-b) = (t-b+\sigma(b))(t-b).\end{aligned}$$

So $t-b$ is invariant. □

Let $\pi(t)$ be a minimal monic semi-invariant polynomial of $R[t;\sigma,\delta]$. It is shown in [20] that a factor of $\pi(t)^{\deg \pi(t)}$ forms a minimal monic invariant polynomial. But for an ordinary derivation $\delta$ (namely for $\delta$ with $\sigma = 1$), $\pi(t)$ is also invariant when $\operatorname{char} R = 0$ and either $\pi(t) - c$ for some $c \in Q$ or $\pi(t)^p$ is a minimal invariant polynomial when $\operatorname{char} R = p \geq 2$. Our aim here is to show that this is also true if $\delta$ is $q$-skew in a sense we now make clear. For any subset $S$ of $Q$, define

$$S^{(\sigma)} \overset{\text{def.}}{=} \{r \in S \mid \sigma(r) = r\},\ S^{(\delta)} \overset{\text{def.}}{=} \{r \in S \mid \delta(r) = 0\} \text{ and } S^{(\sigma,\delta)} \overset{\text{def.}}{=} S^{(\sigma)} \cap S^{(\delta)}.$$

**Definition.** A $\sigma$-derivation $\delta$ is called $q$-skew, where $0 \neq q \in C^{(\sigma,\delta)}$, if $\sigma^{-1}\delta\sigma = q\delta$.

## 2. Results

Throughout the sequel, let $\delta$ be a $q$-skew $\sigma$-derivation and let $\pi(t)$ be a minimal monic semi-invariant polynomial. In order for $\pi(t)$ to exist, we assume that $\delta$ is quasi-algebraic [20, p. 147]. We aim to describe the minimal monic invariant polynomial in terms of $\pi(t)$. By Lemma 1.3, we may consider X-outer $\delta$. For X-outer $\delta$, $\pi(t)$ is given as follows.

**Theorem 2.1** ([4, Theorem 1] and [9, Theorem 15])**.** *Let $\delta$ be an X-outer quasi-algebraic $q$-skew $\sigma$-derivation of $R$. Then there exists the least integer $\nu \geq 1$ such that $q^\nu = 1$ and any minimal monic semi-invariant polynomial $\pi(t) \in Q[t;\sigma,\delta]$ is given by*

$$\pi(t) = \begin{cases} t^\nu + b & \text{if } \operatorname{char} R = 0, \\ t^{\nu p^s} + \displaystyle\sum_{j=0}^{s-1} b_j t^{\nu p^j} + b & \text{if } \operatorname{char} R = p \geq 2, \end{cases}$$

*where $b \in Q$ and $b_j \in \Phi(\nu(p^s - p^j))$ for $0 \leq j \leq s-1$.*

We shall retain the notation above throughout. For brevity, we treat all characteristics simultaneously. If $\operatorname{char} R = 0$, then all $b_j$ are interpreted as 0. For any $u \in \Phi(\deg \pi(t))$, $\pi(t) + u$ is also semi-invariant. Clearly, all minimal monic semi-invariant polynomials of $Q[t;\sigma,\delta]$ are so obtained. Moreover, if $\sigma^{\deg \pi(t)}$ is X-outer, viz. $\Phi(\deg \pi(t)) = 0$, then $\pi(t)$ is the unique minimal monic semi-invariant polynomial of $Q[t;\sigma,\delta]$. The following is important.

**Lemma 2.2.** *If $0 \neq u \in \Phi(i)$, then $\nu | i^2$ and $\sigma(u) = q^i u$.*

*Proof.* Since $0 \neq u \in \Phi(i)$, we have $\sigma^i = \mathrm{I}_u$. Since $\delta$ is $q$-skew,

$$\delta \mathrm{I}_u = \delta\sigma^i = q^i \sigma^i \delta = q^i \mathrm{I}_u \delta.$$

By Lemma 1.2, $\sigma(u) = q^i u$. Inductively, $\sigma^\ell(u) = q^{\ell i} u$ for any $\ell \geq 0$. Setting $\ell = i$, $q^{i^2} u = \sigma^i(u) = \mathrm{I}_u(u) = u$. So $q^{i^2} = 1$ and hence $\nu | i^2$ by the minimality of $\nu$. □

As a direct application, if $\sigma$ is X-inner, then $q = 1$. For if $\sigma = \mathrm{I}_v$, then $\sigma(v) = qv$ by Lemma 2.2, implying $q = 1$ since $\sigma(v) = \mathrm{I}_v(v) = v$. To find minimal monic invariant polynomials, we need more information on $\sigma(b_j), \delta(b_j), \sigma(b)$ and $\delta(b)$.

**Lemma 2.3.** *For* $1 \le j < s$, $b_j \in Q^{(\sigma,\delta)}$. *If* $\nu > 1$, *then* $b, b_0 \in Q^{(\sigma,\delta)}$ *also. If* $\nu = 1$, *then* $\operatorname{char} R = p \ge 2$, $b_0 \in Q^{(\sigma)}$, $\delta(b_0) = b - \sigma(b) \in \Phi(p^s)$ *and* $\delta(b) \in \Phi(p^s + 1)$.

*Proof.* Set $n \stackrel{\text{def.}}{=} \deg \pi(t)$ for simplicity. So $n = \nu$ if $\operatorname{char} R = 0$ and $n = \nu p^s$ if $\operatorname{char} R = p \ge 2$. For $0 \le j < s$, since $b_j \in \Phi\big(\nu(p^s - p^j)\big)$, we have $b_j \in Q^{(\sigma)}$ by Lemma 2.2. Since the coefficient of $t^{n-1}$ of $\pi(t)$ is zero, $[t, \pi(t)]$ is also semi-invariant by [17, Proposition 2.4] or [20, Lemma 2.5, (2)]. By the monicity of $\pi(t)$ and with $b_j \in Q^{(\sigma)}$ for $0 \le j < s$,

$$[t, \pi(t)] = \sum_{j=0}^{s-1} \delta(b_j) t^{\nu p^j} + (\sigma(b) - b)t + \delta(b).$$

Since $\deg[t, \pi(t)] < \deg \pi(t)$, we have $[t, \pi(t)] \in \Phi(n + 1)$ by the minimality of $\pi(t)$. If $\nu > 1$, then $\delta(b_j) = 0$ for $0 \le j < s$, $\sigma(b) = b$ and $\delta(b) \in \Phi(n + 1)$. Since $\nu | n$, $\nu \nmid (n + 1)^2$. So $\delta(b) = 0$ by Lemma 2.2. If $\nu = 1$, then $\operatorname{char} R = p \ge 2$ and $n = p^s$ by the outerness of $\delta$. So

$$[t, \pi(t)] = \sum_{j=1}^{s-1} \delta(b_j) t^{p^j} + (\delta(b_0) + \sigma(b) - b)t + \delta(b) \in \Phi(p^s + 1).$$

Comparing coefficients of this yields $\delta(b_j) = 0$ for $1 \le j < s$, $\delta(b_0) = b - \sigma(b)$ and $\delta(b) \in \Phi(p^s + 1)$. Extend $\sigma$ to an automorphism of $Q[t; \sigma, \delta]$ by setting $\sigma(t) \stackrel{\text{def.}}{=} \frac{t}{q}$. Then $\sigma(\pi(t))$ is also semi-invariant. Since $\sigma(\pi(t))$ is also monic and has degree $n$, the difference $\pi(t) - \sigma(\pi(t))$ is also semi-invariant. We have seen $b_j \in Q^{(\sigma)}$ for $0 \le j < s$ by Lemma 2.2. So $\pi(t) - \sigma(\pi(t)) = b - \sigma(b) \in \Phi(p^s)$. □

**Lemma 2.4.** $[t, \pi(t)^k] = k\delta(b)\pi(t)^{k-1}$ *for* $k \ge 1$ *and* $[\pi(t), \delta(b)] = 0$.

*Proof.* By the Leibniz rule, $[t, \pi(t)^k] = \sum_{i=0}^{k-1} \pi(t)^i [t, \pi(t)] \pi(t)^{k-i-1}$. By Lemma 2.3 (or its proof), $[t, \pi(t)] = \delta(b)$. It suffices to show $[\delta(b), \pi(t)] = 0$. If $\nu > 1$, then $\delta(b) = 0$ by Lemma 2.3 and there is nothing to prove. So assume $\nu = 1$ and $\operatorname{char} R = p \ge 2$. By Lemma 2.3, $u \stackrel{\text{def.}}{=} b - \sigma(b) = \delta(b_0) \in \Phi(p^s)$. So $\sigma(u) = q^{p^s} u = u$ by Lemma 2.2. With this, we obtain inductively $\sigma^k(b) = b - ku$ for $k \ge 0$. In particular, $\sigma^{p^s}(b) = b - p^s u = b$. So $\delta(b) = \delta\sigma^{p^s}(b) = \sigma^{p^s}\delta(b)$. By the semi-invariance of $\pi(t)$, we have $\pi(t)\delta(b) = \sigma^{p^s}(\delta(b))\pi(t) = \delta(b)\pi(t)$, as wanted. □

**Corollary 2.5.** *In the notation of Theorem 2.1, the following are equivalent: (1)* $\pi(t)$ *is invariant; (2)* $\pi(t)t = t\pi(t)$*; (3)* $\delta(b) = 0$.

*Proof.* (2) ⇒ (1) is trivial. For (1) ⇒ (3), let $\pi(t)$ be invariant. So $\pi(t)t = (t - c)\pi(t)$ for some $c \in Q$. Then $c\pi(t) = t\pi(t) - \pi(t)t = \delta(b)$ by Lemma 2.4. Comparing degrees gives $c = 0$ and $\delta(b) = 0$. (3) ⇒ (2) holds since $[t, \pi(t)] = \delta(b)$ by Lemma 2.4. □

We are ready for our main result.

**Theorem 2.6.** *Let $\delta$ be X-outer. (1) If* $\operatorname{char} R = 0$ *or* $q \neq 1$, *then* $\pi(t)$ *is also invariant. (2) Suppose that* $\operatorname{char} R = p \geq 2$ *and* $q = 1$. *If* $\delta(b) = \delta(c)$ *for some* $c \in \Phi(p^s)$, *then* $\pi(t) - c$ *is invariant. Otherwise,* $\pi(t)^p$ *is a minimal monic invariant polynomial.*

*Proof.* If $\operatorname{char} R = 0$ or $q \neq 1$, then $\nu > 1$ and so $\delta(b) = 0$ by Lemma 2.3. By Corollary 2.5, $\pi(t)$ is invariant. So suppose that $\operatorname{char} R = p \geq 2$ and $q = 1$. Then $\nu = 1$ and $\deg \pi(t) = p^s$. For any $c \in \Phi(p^s)$, $\pi(t) - c$ is also monic and semi-invariant. If $\delta(b - c) = 0$, then $\pi(t) - c$ is invariant by Corollary 2.5. So we suppose that $\delta(b - c) \neq 0$ for any $c \in \Phi(p^s)$. By Lemma 2.4, $t\pi(t)^p - \pi(t)^p t = [t, \pi(t)^p] = p\delta(b)\pi(t)^{p-1} = 0$. So $\pi(t)^p$ is invariant. We show its minimality as an invariant polynomial. Let $f(t) \in Q[t; \sigma, \delta]$ be a monic invariant polynomial. Then $f(t)t = (t-c)f(t)$ for some $c \in Q$. So $cf(t) = tf(t) - f(t)t = [t, f(t)]$, implying $c = 0$, since $\deg[t, f(t)] < \deg f(t)$ by the monicity of $f(t)$. So $[t, f(t)] = 0$. By (1) of [20, Proposition 2.8], write $f(t) = \sum_{i=0}^{\ell} u_i \pi(t)^{\ell - i}$, where $u_0 \overset{\text{def.}}{=} 1$ and $u_i \in \Phi(ip^s)$. Since $q = 1$, $\sigma(u_i) = q^{ip^s} u_i = u_i$ by Lemma 2.2. So $[t, u_i] = \sigma(u_i)t + \delta(u_i) - u_i t = \delta(u_i)$. With this and Lemma 2.4, we compute

$$
\begin{aligned}
0 = [t, f(t)] &= [t, \sum_{i=0}^{\ell} u_i \pi(t)^{\ell-i}] = \sum_{i=0}^{\ell} [t, u_i]\pi(t)^{\ell-i} + \sum_{i=0}^{\ell} u_i [t, \pi(t)^{\ell-i}] \\
&= \sum_{i=1}^{\ell} \delta(u_i)\pi(t)^{\ell-i} + \sum_{i=0}^{\ell-1} (\ell - i) u_i \delta(b) \pi(t)^{\ell-i-1} \\
&= \sum_{i=0}^{\ell-1} \delta(u_{i+1})\pi(t)^{\ell-i-1} + \sum_{i=0}^{\ell-1} (\ell - i) u_i \delta(b) \pi(t)^{\ell-i-1} \\
&= \sum_{i=0}^{\ell-1} \Big( (\ell - i) u_i \delta(b) + \delta(u_{i+1}) \Big) \pi(t)^{\ell-i-1}.
\end{aligned}
$$

In the last expression above, the term of degree $\geq (\ell - 1)p^s$ is contributed by

$$\Big(\ell u_0 \delta(b) + \delta(u_1)\Big)\pi(t)^{\ell-1} = \Big(\ell \delta(b) + \delta(u_1)\Big)\pi(t)^{\ell-1}.$$

The coefficient of $t^{p^s(\ell-1)}$ in $[t, f(t)]$ yields the equality $\ell\delta(b) + \delta(u_1) = 0$. If $p \nmid \ell$, then $\ell$ is a unit and $\delta(b + \frac{u_1}{\ell}) = 0$, contradicting our assumption that $\delta(b - c) \neq 0$ for any $c \in \Phi(p^s)$. So $p | \ell$. Then $\ell \geq p$ and $\deg f(t) = \deg \pi(t)^\ell \geq \deg \pi(t)^p$. Since $f(t)$ is arbitrary, the minimality of $\pi(t)^p$ as a monic invariant polynomial is proved. $\square$

The second assertion of Theorem 2.6 can be simplified if $\sigma$ is also X-outer.

**Theorem 2.7.** *Assume that $\delta, \sigma$ are X-outer,* $\operatorname{char} R = p \geq 2$ *and* $q = 1$. *Then* $\pi(t)$ *or* $\pi(t)^p$ *is a minimal monic invariant polynomial according as* $\delta(b) = 0$ *or* $\delta(b) \neq 0$ *respectively. In the former case,* $\pi(t) = t^{p^s} + \sum_{j=0}^{s-1} b_j t^{p^j} + b \in Q^{(\sigma,\delta)}[t; \sigma, \delta]$. *In the latter case,* $\pi(t)^p = t^{p^{s+1}} + \sum_{j=0}^{s-1} b_j^p t^{p^{j+1}} + b^p \in Q^{(\sigma,\delta)}[t; \sigma, \delta]$.

*Proof.* Since $q = 1$, $\delta\sigma = \sigma\delta$. So $\delta\sigma^s = \sigma^s\delta$ for any $s$. Given $0 \neq u \in \Phi(s)$, $\mathrm{I}_u = \sigma^s$ and so $\delta \mathrm{I}_u = \mathrm{I}_u \delta$, implying $\delta(u) = 0$ by Lemma 1.2, since $\sigma$ is X-outer. So $\delta(\Phi(s)) = 0$. Now, if $\delta(b) = 0$, then $\pi(t)$ is also invariant by Corollary 2.5. If

$\delta(b) \neq 0$, then $\delta(b-c) = \delta(b) \neq 0$ for any $c \in \Phi(p^s)$, since $\delta(\Phi(p^s)) = 0$. By Theorem 2.6, $\pi(t)^p$ is a minimal monic invariant polynomial.

For the rest, since $\sigma$ is X-outer, we have $\delta(u) = 0$ for any $u \in \Phi(j)$ by Lemma 1.2. By Theorem 2.1, $b_0 \in \Phi(p^s - 1)$, implying $\delta(b_0) = 0$. So $b - \sigma(b) = \delta(b_0) = 0$ by Lemma 2.3. Together with Lemma 2.3, we have thus shown

$$(*) \qquad b \in Q^{(\sigma)} \quad \text{and} \quad b_j \in Q^{(\sigma,\delta)} \quad \text{for } 0 \leq j < s.$$

If $\delta(b) = 0$, then $\pi(t) \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$, as asserted. So suppose $\delta(b) \neq 0$. Write $\pi(t) = g(t) + b$, where $g(t) \stackrel{\text{def.}}{=} t^{p^s} + b_{s-1}t^{p^{s-1}} + \cdots + b_0 t$. By the semi-invariance of $\pi(t)$, $\pi(t)b = \sigma^{p^s}(b)\pi(t) = b\pi(t)$. So $[g(t), b] = [g(t)+b, b] = [\pi(t), b] = 0$. With this, $\pi(t)^p = (g(t)+b)^p = g(t)^p + b^p$. We show $g(t)^p = t^{p^{s+1}} + b_{s-1}^p t^{p^s} + \cdots + b_0^p t^p$. It suffices to observe that all $b_j$ commute with $t$ and with each other. The former holds by $(*)$. For the latter, if all positive powers of $\sigma$ are X-outer, then all $b_j \in \Phi(\nu(p^s - p^j)) = 0$ and there is nothing to prove. So assume that $\ell$ is the least positive integer such that $\sigma^\ell = \mathrm{I}_u$ for a unit $u \in Q$. Then for nonzero $b_j$, $\ell$ divides $\nu(p^s - p^j)$ and $b_j = \beta_j u^{\frac{\nu(p^s - p^j)}{\ell}}$ for some $\beta_j \in C$. So all $b_j$ commute. We have thus shown

$$\pi(t)^p = t^{p^{s+1}} + b_{s-1}^p t^{p^s} + \cdots + b_0^p t^p + b^p.$$

Since $\sigma(b) = b$ by $(*)$, $[b, \Phi(j)] = 0$ for any $j$. By Lemma 2.3, $\delta(b) \in \Phi(p^s + 1)$. So $[b, \delta(b)] = 0$. With this, $\delta(b^p) = pb^{p-1}\delta(b) = 0$. So $\pi(t)^p \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$. □

The case that $\sigma$ is X-inner can be reduced to ordinary derivations as follows. Let $u \in Q$ be a unit such that $\sigma = \mathrm{I}_u$. The map $d\colon x \in R \mapsto u^{-1}\delta(x)$ defines a derivation of $Q$. Form the Ore extension $Q[\tilde{t}; d]$. The map $t \in Q[t;\sigma,\delta] \mapsto u^{-1}\tilde{t} \in Q[\tilde{t}; d]$ induces a ring isomorphism $Q[t;\sigma,\delta] \cong Q[\tilde{t}; d]$ fixing all $r \in R$. Under this automorphism, (semi-)invariant polynomials of $Q[t;\sigma,\delta]$ and of $Q[t;d]$ correspond bijectively. So it suffices to consider the case when $\delta$ is an ordinary derivation. This is a special instance of Theorem 2.6. We quote it below for easy reference.

**Theorem 2.8** ([21, 6])**.** *Assume that* $\operatorname{char} R = p \geq 2$ *and* $\delta$ *is an ordinary derivation. If* $\delta(b) = \delta(\gamma)$ *for some* $\gamma \in C$*, then* $\pi(t) - \gamma$ *is a minimal monic invariant polynomial. Otherwise,* $\pi(t)^p$ *is a minimal monic invariant polynomial.*

If $R$ is a finite-dimensional central division algebra, Jacobson ([13, Lemma 1.5.3]) proved that there must exist $\gamma \in C$ such that $\pi(t) - \gamma$ is the minimal invariant polynomial. This was generalized to prime GPI-rings in [7, Lemma 2.5].

## 3. An application

For an invariant polynomial $f(t) \in Q[t;\sigma,\delta]$, $Q[t;\sigma,\delta]f(t) = f(t)Q[t;\sigma,\delta]$ ([20, Proposition 2.1]). We recall

**Lemma 3.1** ([20, Proposition 2.1])**.** *For any ideal* $\mathcal{I} \neq 0$ *of* $R[t;\sigma,\delta]$*, there exists a unique monic invariant polynomial* $f(t)$*, called the invariant generator of* $\mathcal{I}$*, such that* $If(t) \subseteq \mathcal{I} \subseteq R[t;\sigma,\delta] \cap Q[t;\sigma,\delta]f(t)$ *for some ideal* $I \neq 0$ *of* $R$*.*

**Definition** ([12])**.** An ideal $\mathcal{I}$ of $R[t;\sigma,\delta]$ is called $R$-disjoint if $\mathcal{I} \cap R = 0$. Given a monic invariant polynomial $f(t) \in Q[t;\sigma,\delta]$, define $\langle f(t) \rangle \stackrel{\text{def.}}{=} R[t;\sigma,\delta] \cap Q[t;\sigma,\delta]f(t)$, called the principal ideal generated by $f(t)$. We call an invariant polynomial $f(t)$ *irreducible* if it is nonconstant and it is *not* a product of two nonconstant invariant polynomials.

An ideal of $R[t;\sigma,\delta]$ is $R$-disjoint if and only if its invariant generator is not 1. By definition, $\langle f(t)\rangle$ is maximal among ideals with the invariant generator $f(t)$. We are interested in $R$-disjoint prime ideals of $R[t;\sigma,\delta]$. It is not hard to see that $\langle p(t)\rangle$ is prime for any irreducible invariant $p(t)$. Our aim here is the following converse.

**Theorem 3.2.** *Let $\delta$ be an X-outer $\sigma$-derivation. Unless* $\operatorname{char} R = p \geq 2$ *and $\sigma$ is X-inner (necessarily $q = 1$), any $R$-disjoint prime ideal of $R[t;\sigma,\delta]$ is of the form $\langle p(t)\rangle$ for an irreducible monic invariant polynomial $p(t)$.*

The above says that $R$-disjoint prime ideals of $R[t;\sigma,\delta]$ are maximal. This problem has been considered for Ore extensions of derivation type in [2, 11, 23] and of automorphism type in [3, 10]. Leroy and Matczuk [19] proved the same result under the assumption $\sigma\delta = \delta\sigma$ plus some mild conditions. We need the following generalization of [19, Lemma 1.8].

**Theorem 3.3.** *Assume that $\delta$ is X-outer. Unless* $\operatorname{char} R = p \geq 2$ *and $\sigma$ is X-inner (necessarily $q = 1$), monic invariant polynomials have all their coefficients in $Q^{(\sigma,\delta)}$ and hence commute with $t$.*

*Proof.* Let

$$M(t) \overset{\text{def.}}{=} \begin{cases} \pi(t) & \text{if } \operatorname{char} R = 0 \text{ or } q \neq 1; \\ \pi(t) & \text{if } \operatorname{char} R = p \geq 2, q = 1 \text{ and } \sigma \text{ is X-outer with } \delta(b) = 0; \\ \pi(t)^p & \text{if } \operatorname{char} R = p \geq 2, q = 1 \text{ and } \sigma \text{ is X-outer with } \delta(b) \neq 0. \end{cases}$$

By Theorems 2.6 and 2.7, $M(t)$ is a minimal monic invariant polynomial. If $\operatorname{char} R = 0$ or $q \neq 1$, then $M(t) = \pi(t) \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$ by Lemma 2.3. If $\operatorname{char} R = p \geq 2$, $q = 1$ and $\sigma$ is X-outer, then $M(t) \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$ by Theorem 2.7. So $M(t) \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$ always. By [20, Proposition 3.4], any monic invariant polynomial can be written in the form $u\omega(t)M(t)^l$, where $l \geq 0$ is an integer, $u \in Q$ is a unit and $\omega(t)$ is a nonzero central polynomial. By (iii) of [20, Theorem 3.7], there exist an integer $\ell > 0$ and a unit $v \in Q$ such that $\zeta \overset{\text{def.}}{=} vM(t)^\ell$ is a nonzero central polynomial of minimal degree and the central polynomial $\omega(t)$ can be written in the form

$$\omega(t) = \alpha_n\zeta^n + \alpha_{n-1}\zeta^{n-1} + \cdots$$

with $\alpha_i \in C^{(\sigma,\delta)}$. Since $[M(t), t] = 0$, we have $0 = [\zeta, t] = [v, t]M(t)^\ell$, implying $0 = [v, t] = (v - \sigma(v))t - \delta(v)$. So $\sigma(v) = v$ and $\delta(v) = 0$, that is, $v \in Q^{(\sigma,\delta)}$. So $\zeta \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$ and $\omega(t) \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$. Since $u\omega(t)M(t)^l$ and $M(t)^l$ are monic, so is $u\omega(t)$. Hence $u$ is the inverse of the leading coefficient of $\omega(t)$, implying $u \in Q^{(\sigma,\delta)}$. Whence $u\omega(t)M(t)^l \in Q^{(\sigma,\delta)}[t;\sigma,\delta]$, as asserted. □

We are now ready for

*Proof of Theorem* 3.2. Let $\Im$ be the set of ideals $I$ of $R$ such that $\sigma(I) \subseteq I$ and $\delta(I) \subseteq I$. For $I \in \Im$, $R[t;\sigma,\delta]I \subseteq I[t;\sigma,\delta]$, where $I[t;\sigma,\delta]$ is the set of polynomials $\sum_i a_it^i$ with $a_i \in I$. If $I, J \in \Im$, then $IJ \in \Im$. Define

$$Q_0 \overset{\text{def.}}{=} \{a \in Q \mid aI \subseteq R \text{ for some } 0 \neq I \in \Im\}.$$

Then $Q_0$ forms a subring of $Q$. Given $a \in Q^{(\sigma,\delta)}$ arbitrarily, let $I \neq 0$ be an ideal of $R$ such that $aI \subseteq R$. Set $J \overset{\text{def.}}{=} I + \sum_\theta \theta(I)$, where the summation ranges over all products $\theta$ of $\sigma$ and $\delta$. Clearly, $0 \neq J \in \Im$ and $aJ \subseteq R$, implying $a \in Q_0$. So

$Q_0 \supseteq Q^{(\sigma,\delta)}$. Clearly, $Q_0 \supseteq R$. Given an $R$-disjoint prime ideal $\mathcal{P}$ of $R[t;\sigma,\delta]$, let $p(t)$ be its monic invariant generator. Given $f(t) \in \langle p(t)\rangle$, write $f(t) = g(t)p(t)$, where $g(t) \in Q[t;\sigma,\delta]$. By Theorem 3.3, $p(t) \in Q^{(\sigma,\delta)}[t;\sigma,\delta] \subseteq Q_0[t;\sigma,\delta]$. With the left division algorithm in $Q_0[t;\sigma,\delta]$, we see $g(t) \in Q_0[t;\sigma,\delta]$. Let $0 \neq I \in \Im$ be such that $g(t)I \subseteq R[t;\sigma,\delta]$. Let $J$ be a nonzero ideal of $R$ such that $p(t)J \subseteq \mathcal{P}$. Since $[p(t),t] = 0$, $p(t)R[t;\sigma,\delta] = R[t;\sigma,\delta]p(t)$. With this, we compute

$$\begin{aligned} f(t)R[t;\sigma,\delta]IJ &= g(t)p(t)R[t;\sigma,\delta]IJ \\ &= g(t)R[t;\sigma,\delta]p(t)IJ = g(t)R[t;\sigma,\delta]\sigma^{\deg p}(I)p(t)J \\ &\subseteq\ g(t)R[t;\sigma,\delta]I\mathcal{P} \subseteq g(t)I[t;\sigma,\delta]\mathcal{P} \subseteq R[t;\sigma,\delta]\mathcal{P} \subseteq \mathcal{P}. \end{aligned}$$

Since $\mathcal{P}$ is $R$-disjoint, we have $IJ \nsubseteq \mathcal{P}$. The primeness of $\mathcal{P}$ implies $f(t) \in \mathcal{P}$. But $f(t) \in \langle p(t)\rangle$ is arbitrary. This proves $\mathcal{P} = \langle p(t)\rangle$. For the irreduciblility of $p(t)$, suppose that $p(t) = g(t)h(t)$, where $g(t)$ and $h(t)$ are monic invariant. Pick a nonzero ideal $I$ of $R$ such that $Ig(t) \cup Ih(t) \subseteq R[t;\sigma,\delta]$. Then $Ig(t)R[t;\sigma,\delta]Ih(t) = IR[t;\sigma,\delta]I^{\deg g(t)}g(t)h(t) \subseteq \langle p(t)\rangle$, implying $Ig(t) \subseteq \langle p(t)\rangle$ or $Ih(t) \subseteq \langle p(t)\rangle$. That is, $g(t) = 1$ or $h(t) = 1$. So $p(t)$ is irreducible. □

In the case $\operatorname{char} R = p \geq 2$, our $\delta$ and $\sigma$ above are both X-outer. The problem remains open if one of $\delta, \sigma$ is X-inner, as was raised in [19].

## Acknowledgments

The authors would like to thank the referees for the valuable suggestions which have served to simplify and clarify the paper greatly. This research was supported by the NSC and NCTS/TPE of Taiwan.

## References

[1] K. I. Beidar, W. S. Martindale III and A. V. Mikhalev, "Rings with Generalized Identities", Marcel Dekker, Inc., New York-Basel-Hong Kong, 1996. MR1368853 (97g:16035)

[2] A. D. Bell, *When are all prime ideals in an Ore extension Goldie?*, Comm. Algebra **13**(8) (1985), 1743–1762. MR792560 (86j:16003)

[3] W. Chin, *Prime ideals in differential operator rings and crossed products of infinite groups*, J. Algebra **106** (1987), 78–104. MR878469 (88c:16039)

[4] C.-L. Chuang and T.-K. Lee, *Algebraic q-skew derivations*, J. Algebra **282** (2004), 1–22. MR2095569 (2005g:16068)

[5] C.-L. Chuang and T.-K. Lee, *Identities with a single skew derivation*, J. Algebra **288** (2005), 59–77. MR2138371 (2006c:16059)

[6] C.-L. Chuang and T.-K. Lee, *Derivations and skew polynomial rings*, Comm. Algebra **35** (2007), 527–539. MR2294614 (2007k:16063)

[7] C.-L. Chuang and T.-K. Lee, *Ore extensions which are GPI-rings*, Manuscripta Math. **124** (2007), 45–58. MR2336054 (2009a:16048)

[8] C.-L. Chuang and Y.-T. Tsai, *On the structure of semi-invariant polynomials in Ore extensions*, J. Algebra **322**(7) (2009), 2464–2491. MR2553690 (2010m:16039)

[9] C.-L. Chuang and Y.-T. Tsai, *Higher derivations of Ore extensions by q-skew derivations*, J. Pure and Applied Algebra **214**(10) (2010), 1778-1786. MR2608105 (2011e:16050)

[10] E. Cisneros, M. Ferrero and M. I. Gonzalez, *Prime ideals of skew polynomial rings and skew Laurent polynomial rings*, Math. J. Okayama Univ. **32** (1990), 61–72. MR1112011 (92g:16041)

[11] M. Ferrero and J. Matczuk, *Prime ideals in skew polynomial rings of derivation type*, Comm. Algebra **18**(3) (1990), 689–710. MR1052761 (91h:16007)

[12] M. Ferrero, *Prime and principal closed ideals of polynomial rings*, J. Algebra **134**(1) (1990), 45–59. MR1068414 (91h:16008)

[13] N. Jacobson, Finite-Dimensional Division Algebras over Fields, Springer-Verlag, Berlin, 1996. MR1439248 (98a:16024)

[14] V. K. Kharchenko, *Generalized identities with automorphisms*, Algebra i Logika **14** (1975), 132–148. MR0399153 (53:3004)

[15] V. K. Kharchenko and A. Z. Popov, *Skew derivations of prime rings*, Comm. Algebra **20**(11) (1992), 3321–3345. MR1186710 (93k:16071)

[16] T. Y. Lam and A. Leroy, *Algebraic conjugacy classes and skew polynomial rings*, "Proceedings of the NATO Advanced Research Workshop on Perspectives in Ring Theory, Antwerp, Belgium, July 19-29, 1987", Kluwer, Dordrecht, 1988. MR1048406 (91c:16015)

[17] T. Y. Lam, A. Leroy, K. H. Leung and J. Matczuk, *Invariant and semi-invariant polynomials in skew polynomial rings*, Israel Mathematics Conference Proceedings **1** (1989), 247–261. MR1029317 (90k:16004)

[18] T. Y. Lam and A. Leroy, *Homomorphisms between Ore extensions*, Contemporary Math. 124, Amer. Math. Soc., Providence, RI, 1992, 83–110. MR1144030 (93b:16052)

[19] A. Leroy and J. Matczuk, *Prime ideals of Ore extensions*, Comm. Algebra **19**(7) (1991), 1893–1907. MR1121112 (92h:16029)

[20] A. Leroy and J. Matczuk, *The extended centroid and X-inner automorphisms of Ore extensions*, J. Algebra **145** (1992), 143–177. MR1144664 (93b:16053)

[21] J. Matczuk, *Extended centroid of skew polynomial rings*, Math. J. Okayama Univ. **30** (1988), 13–20. MR976726 (89m:16006)

[22] D. S. Passman, "Infinite Crossed Product", Pure and Applied Mathematics, 135. Academic Press, Inc., Boston, MA, 1989. MR979094 (90g:16002)

[23] D. S. Passman, *Prime ideals in enveloping rings*, Trans. Amer. Math. Soc. **302**(2) (1987), 535–560. MR891634 (88f:17015)

Department of Mathematics, National Taiwan University, Taipei 106, Taiwan
*E-mail address*: chuang@math.ntu.edu.tw

Department of Mathematics, National Taiwan University, Taipei 106, Taiwan
*E-mail address*: tklee@math.ntu.edu.tw

Department of Mathematics, National Changhua University of Education, Changhua 500, Taiwan
*E-mail address*: ckliu@cc.ncue.edu.tw