Canad. Math. Bull.Vol. **35** (1), 1992 pp. 126–132

# AUTOMORPHISMS AND DERIVATIONS OF SKEW POLYNOMIAL RINGS

MARY P. ROSEN AND JERRY D. ROSEN

ABSTRACT. For a prime ring $R$ and $\sigma \in \mathrm{Aut}(R)$, we determine the group of $R$-stabilizing automorphisms of the skew polynomial ring $R[x;\sigma]$. In the case where $R$ is simple, we characterize the $X$-inner automorphisms of $R[x;\sigma]$. We also provide necessary and sufficient conditions for a $\sigma$-commuting derivation of a prime ring $R$ to extend to a derivation of $R[x;\sigma]$.

Skew polynomial rings have played an increasingly important role in noncommutative algebra during the past twenty years. They provide an abundant source of examples and counter-examples and are a good testing ground for various concepts. For instance, the Jacobson radical, ideal structure, extended centroid, and Krull dimension have all been determined for skew polynomial rings. Recently, in [4], they were used to illustrate that the Martindale quotient rings $Q_\ell$, $Q_r$, and $Q_s$ are not closed (i.e., the repetition of the construction may produce a properly larger ring). Note that skew polynomial rings figure prominently in two recent texts [1,3] on noncommutative noetherian rings.

In this paper, we determine the group $G$ of $R$-stabilizing automorphisms of the skew polynomial ring $R[x;\sigma]$ where $R$ is prime and $\sigma$ is an $X$-outer automorphism of $R$. We characterize these automorphisms in terms of units of $R$ and certain subgroups of $\mathrm{Aut}(R)$. Specifically, we prove that $G/ZU \cong H$ where $ZU$ is the group of central units of $R$ and $H$ is the preimage of the centralizer of $\bar{\sigma}$ under the canonical epimorphism $\mathrm{Aut}(R) \longrightarrow \mathrm{Aut}(R)/\mathrm{Inn}(R)$. Furthermore, if every unit of $R$ is central, then $G$ is isomorphic to the semidirect product of $ZU$ with $H$ where, in this case, $H$ is the centralizer of $\sigma$ in $\mathrm{Aut}(R)$.

If $R$ is a simple ring, we determine the normalizing elements and hence the $X$-inner automorphisms of $R[x;\sigma]$. We use our results to construct an example of a prime ring $R$ having the property that for any integer $n > 1$, there exists an $X$-outer automorphism $\varphi$ of $R$ such that $\varphi^n$ is $X$-inner. As another application, we compute certain Galois groups of the type $\mathrm{Gal}(R/R^G)$ where $R = F[x;\sigma]$, $F$ a field. We prove that if $\sigma$ has finite period and $G = \mathrm{Xinn}(R)$, then $\mathrm{Gal}(R/R^G) = G$.

Finally, we determine the $R$-stabilizing derivations of $R[x;\sigma]$ where $R$ is prime. We prove that if $\delta$ is a derivation of $R$ such that $\delta\sigma = \sigma\delta$ then $\delta$ can be extended to a derivation (also denoted $\delta$) of $R[x;\sigma]$ if and only if $\delta(x) = g(x)x$ with $g(x) \in C[bx^m] \cap R[x;\sigma]$, where $C$ is the extended centroid of $R$, $b$ an $R$-normalizing element, and $m$ a nonnegative integer.

We now provide some background material. Let $R$ be a prime ring and let $Q = Q(R)$ denote its (left) Martindale ring of quotients. The construction of $Q$ has become standard

Received by the editors December 13, 1990; revised February 5, 1991.
AMS subject classification: 16A05.

and we refer the reader to [4, Chapter 3] for the details. The following lemma summarizes the main properties of $Q$ and characterizes $Q$ up to isomorphism.

LEMMA 1. *Let $R$ be a prime ring. Then $Q$ satisfies*
*(1) $R \subseteq Q$ with the same 1,*
*(2) if $q \in Q$, then there exists $0 \neq A \lhd R$ with $Aq \subseteq R$,*
*(3) if $q \in Q$ and $0 \neq A \lhd R$ with $Aq = 0$, then $q = 0$,*
*(4) if $\phi : {}_RA \longrightarrow {}_RR$ is given with $0 \neq A \lhd R$, then there exists $q \in Q$ with $aq = a\phi$ for all $a \in A$.*
*Furthermore, $Q$ is uniquely determined by these properties.*

The extended centroid of $R$, denoted $C(R)$, is the center of $Q$. $C(R)$ is a field containing $Z(R)$, the center of $R$. Any $\phi \in \mathrm{Aut}(R)$ has a unique extension to $Q$. $\phi$ is said to be $X$-inner if there exists a unit $q \in Q$ such that $\phi(r) = I_q(r) = qrq^{-1}$ for all $r \in R$. Otherwise $\phi$ is $X$-outer. Let Xinn($R$) be the group of $X$-inner automorphisms of $R$. Note that $\mathrm{Inn}(R) \leq \mathrm{Xinn}(R) \lhd \mathrm{Aut}(R)$. $I_q$ is $X$-inner if and only if $q \in N(R)$, the subgroup of $Q$ consisting of $R$-normalizing elements. Let $U(R)$ denote the group of units of $R$.

For a ring $R$ with $\sigma \in \mathrm{End}(R)$, let $R[x;\sigma]$ denote the ring freely generated by $R$ and $x$ subject to the relation $xr = \sigma(r)x$ for all $r \in R$. $R[x;\sigma]$ is called the *skew polynomial ring* over $R$ with respect to $\sigma$. If $\sigma \in \mathrm{Aut}(R)$ and $R$ is prime, then so is $R[x;\sigma]$. For $i \in Z^+$ and $a \in R$, let $N_i(a) = a\sigma(a)\cdots\sigma^{i-1}(a)$. A derivation of any ring $R$ is an additive mapping $\delta : R \longrightarrow R$ satisfying $\delta(rs) = r\delta(s) + \delta(r)s$ for all $r, s \in R$.

LEMMA 2. *(1) Let $R$ be any ring with $\phi$, $\sigma \in \mathrm{End}(R)$. Then $\phi$ extends to an endomorphism (also denoted $\phi$) of $R[x;\sigma]$ if and only if $\phi(x) = \sum_{i=0}^n a_ix^i$ where $a_i\sigma^i\big(\phi(r)\big) = \phi\big(\sigma(r)\big)a_i$ for all $r \in R$ and all $i$.*

*(2) Let $R$ be a prime ring with $\phi, \sigma \in \mathrm{Aut}(R)$. Then $\phi$ extends to an automorphism of $R[x;\sigma]$ if and only if $\phi(x) = ax + b$ for some $a \in U(R)$, $b \in R$ satisfying*
*(i) $a\sigma\big(\phi(r)\big) = \phi\big(\sigma(r)\big)a$,*
*(ii) $b\phi(r) = \phi\big(\sigma(r)\big)b$*
*for all $r \in R$. Furthermore, if $\sigma$ is $X$-outer, then $b = 0$.*

PROOF. (1) $R[x;\sigma]$ is freely generated by $R$ and $x$ subject to $xr = \sigma(r)x$ for all $r \in R$. Thus if $S$ is any ring and $\phi : R \longrightarrow S$ is a homomorphism, then $\phi$ extends to a homomorphism $\phi : R[x;\sigma] \longrightarrow S$ with $\phi(x) = y$ if and only if $y\phi(r) = \phi\big(\sigma(r)\big)y$ for all $r \in R$. Suppose $\phi \in \mathrm{End}(R)$ and $a_i \in R$ $(i = 0, 1, \ldots, n)$ satisfy $a_i\sigma^i\big(\phi(r)\big) = \phi\big(\sigma(r)\big)a_i$ for all $r \in R$. Setting $\phi(x) = \sum_{i=0}^n a_ix^i$, we have

$$\phi(x)\phi(r) = \sum_{i=0}^{n} a_i\sigma^i\big(\phi(r)\big)x^i = \phi\big(\sigma(r)\big)\phi(x) \text{ for all } r \in R.$$

Hence $\phi$ defines an $R$-stabilizing endomorphism of $R[x;\sigma]$. The converse is clear.

(2) Suppose $\phi$ is an $R$-stabilizing automorphism of $R[x;\sigma]$ with $\phi(x) = ax^n + \cdots$ By (1), $a\sigma^n\big(\phi(r)\big) = \phi\big(\sigma(r)\big)a$ for all $r \in R$ which implies $a \in N(R)$. Now $\phi$ onto gives

$$x = \phi(cx^m + \cdots) = \phi(c)\sigma^n(a)\sigma^{2n}(a)\cdots\sigma^{(m-1)n}(a)x^{mn} + \cdots$$

If $mn > 1$, then $\phi(c)\sigma^n(a)\cdots\sigma^{(m-1)n}(a) = 0$ and $a \in N(R)$ implies $\phi(c) = 0$ yielding $c = 0$, a contradiction. Thus $m = n = 1$ and so $\phi(x) = ax + b$ with $a \in U(R)$. Furthermore, (i) and (ii) follow from (1). If $b \neq 0$, by (ii) we have $b \in N(R)$ and $\sigma$ is the $X$-inner automorphism determined by $\phi^{-1}(b^{-1})$. The converse can be easily checked. ∎

Let $R$ be prime and $\sigma$ $X$-outer. Let $G$ denote the group of $R$-stabilizing automorphisms of $R[x;\sigma]$. Every element of $G$ may be expressed as $\phi_a$ where $\phi_a(x) = ax$ and $\phi \in \mathrm{Aut}(R)$, $a \in U(R)$ satisfy $\phi\big(\sigma(r)\big)a = a\sigma\big(\phi(r)\big)$ for all $r \in R$. This last equation implies $\phi\sigma = I_a\sigma\phi$ and hence $\bar{\phi} \in \mathbf{C}(\bar{\sigma})$ (the centralizer of $\bar{\sigma}$) in $\mathrm{Aut}(R)/\mathrm{Inn}(R)$. Consequently, $\phi \in H$ = the preimage of $\mathbf{C}(\bar{\sigma})$ under the canonical homomorphism.

THEOREM 3. *Let $R$ be a prime ring and $\sigma$ $X$-outer with $G$, $H$ as above. Let $ZU$ denote the group of central units of $R$.*

*(1) Then $G/ZU \cong H$.*

*(2) If every unit of $R$ is central, then $G$ is isomorphic to the semidirect product of $ZU$ with $H$. In this case, $H = \mathbf{C}(\sigma)$ in* $\mathrm{Aut}(R)$.

PROOF. (1) If $a \in ZU$, then $1_a \in H$ (where $1_a(r) = r$, $1_a(x) = ax$). The mapping given by $a \longrightarrow 1_a$ is an embedding of $ZU$ into $G$. Now the restriction map (to $R$) determines an epimorphism $G \longrightarrow H$ given by $\phi_a \longrightarrow \phi$ with kernel $ZU$. Hence $G/ZU \cong H$.

(2) If all units of $R$ are central, then $H = \mathbf{C}(\sigma)$ in $\mathrm{Aut}(R)$ and $\phi \longrightarrow \phi_1$ embeds $H$ in $G$. Furthermore, $H \cap ZU = 1$ and $G = H \cdot ZU$ (since $\phi_a = \phi_1 \circ 1_{\phi^{-1}(a)}$), completing the proof. ∎

We now determine $\mathrm{Xinn}(R[x;\sigma])$ when $R$ is simple. If, in addition, $R$ is a simple domain, we show every $X$-inner automorphism of $R[x;\sigma]$ stabilizes $R$. In this case, we will find necessary and sufficient conditions on $\phi$ and a which guarantee $\phi_a \in \mathrm{Xinn}(R[x;\sigma])$. The results in the following lemma are well-known and their respective proofs can be found in [2] and [5, p. 144, Exercise 12].

LEMMA 4. *(1) If $R$ is prime and $\sigma \in$ $\mathrm{Aut}(R)$, then $C(R[x;\sigma])$ is isomorphic to the field of fractions of $Z(R[x;\sigma])$.*

*(2) If $R$ is simple and $A \lhd R[x;\sigma]$, then $A = R[x;\sigma]x^n g$ where $g$ is central and $n \geq 0$.*

THEOREM 5. *If $R$ is a simple ring, then*

$$N(R[x;\sigma]) = \{\, ux^m z \mid u \in U(R[x;\sigma]), z \in C(R[x;\sigma]), m \in Z\}.$$

*If $R$ is a simple domain with $\sigma$ $X$-outer, then*

$$\mathrm{Xinn}(R[x;\sigma]) = \{\, \phi_a \mid a = u\sigma(u^{-1}), \phi = I_u\sigma^m \text{ where } u \in U(R) \text{ and } m \in Z\}.$$

PROOF. Set $S = R[x;\sigma]$ and let $0 \neq \alpha \in S \cap N(S)$. Then $S\alpha$ is an ideal of $S$; so by Lemma 4 (2), there exists $\beta = x^n g$, $g$ central, with $S\alpha = S\beta$. Thus $\alpha = u\beta = uv\alpha$ and $\alpha$ regular implies $uv = 1$. Similarly $\beta = v\alpha = vu\beta$ and thus $vu = 1$ which gives $\alpha = ux^n g$ where $u \in U(S)$.

Choose $0 \neq \gamma \in N(S)$ and let $0 \neq A \lhd S$ with $A\gamma \subseteq S$. Then $A = S\eta$ where $\eta = x^{\ell}h$, $h$ central. Now $0 \neq \eta\gamma \in S \cap N(S)$ and thus $\eta\gamma$ can be described as above; say $\eta\gamma = ux^n g$. Solving we get $\gamma = ux^{n-\ell}gh^{-1}$, the desired result. From this it is clear that any $X$-inner automorphism of $S$ is of the form $I_u\sigma^m$ where $u \in U(S)$ and $m \in Z$.

If $R$ is a domain, then $U(S) = U(R)$ and hence any $X$-inner automorphism of $S$ stabilizes $R$. Thus, if $\sigma$ is $X$-outer and $I_{ux^m} \in \mathrm{Xinn}(S)$, then $I_{ux^m} = \phi_a$. Now for all $r \in R$,

$$\phi(r) = \phi_a(r) = I_{ux^m}(r) = (I_u\sigma^m)(r), \text{ showing } \phi = I_u\sigma^m.$$

Furthermore, $ax = \phi_a(x) = I_{ux^m}(x) = u\sigma(u^{-1})x$, which gives $a = u\sigma(u^{-1})$. Conversely, consider $\phi_a$ with $a = u\sigma(u^{-1})$ and $\phi = I_u\sigma^m$. Thus for all $r \in R$,

$$\begin{aligned}\phi_a(rx^i) &= \phi(r)N_i(a)x^i = I_u\big(\sigma^m(r)\big)u\sigma^i(u^{-1})x^i = u\sigma^m(r)\sigma^i(u^{-1})x^i \\ &= u\sigma^m(r)x^iu^{-1} = u\sigma^m(r)x^m x^i x^{-m}u^{-1} = (ux^m)rx^i(ux^m)^{-1} \\ &= I_{ux^m}(rx^i),\end{aligned}$$

proving $\phi_a = I_{ux^m} \in \mathrm{Xinn}(S)$. ■

We provide an example of a prime ring having the property that for any $n > 1$, there exists an $X$-outer automorphism $\varphi$ such that $\varphi^n$ is $X$-inner.

EXAMPLE (1). Let $Q(t)$ be the field of rational functions over $Q$. Let $\sigma: Q(t) \longrightarrow Q(t)$ be the $Q$-automorphism given by $t \longrightarrow t + 1$. Set $R = Q(t)[x;\sigma]$. By Theorem 5,

$$\mathrm{Xinn}(R) = \{\phi_a \mid a = u\sigma(u^{-1}), u \in Q(t)^*, \phi \in \langle\sigma\rangle\}.$$

Note that $\sigma_1 = I_x \in \mathrm{Xinn}(R)$. For any $n > 1$, define $\tau: Q(t) \longrightarrow Q(t)$ to be the $Q$-automorphism given by $t \longrightarrow t + (1/n)$. Since $\tau\sigma = \sigma\tau$, it follows that $\tau_1 \in \mathrm{Aut}(R)$ by Theorem 3 (2). Also $\tau \notin \langle\sigma\rangle$ implies $\tau_1$ is $X$-outer. Since $(\tau_1)^n = \sigma_1$, we have $(\tau_1)^n$ is $X$-inner.

If $R$ is a ring and $S$ is a subring of $R$, let

$$\mathrm{Gal}(R/S) = \{\sigma \in \mathrm{Aut}(R) \mid \sigma(s) = s \text{ for all } s \in S\}.$$

Montgomery and Passman prove that if $R$ is a prime ring and $G$ is a subgroup of $\mathrm{Aut}(R)$ satisfying certain technical conditions (i.e., $G$ is an $N$-group), then $\mathrm{Gal}(R/R^G) = G$. We refer the reader to [4, Chapter 7]. In Theorem 6 and Example (2), we determine $\mathrm{Gal}(R/R^G)$ for $R = F[x;\sigma]$, $F$ a field, and various subgroups $G$ of $\mathrm{Aut}(R)$. We remark that these groups are not $N$-groups. Suppose $\sigma \in \mathrm{Aut}(F)$ is of finite period $m$. Recall that for any $j \in Z^+$ and $a \in F$, $N_j(a) = a\sigma(a)\cdots\sigma^{j-1}(a)$. The norm of $a$ is defined to be $N_m(a)$. $a$ has norm 1 if and only if $a = b\sigma(b^{-1})$ for some $b \in F^*$. Let $\mathbf{N}$ denote the subgroup of $F^*$ consisting of those elements of norm 1.

THEOREM 6. *Let $F$ be a field with $1 \neq \sigma \in \mathrm{Aut}(F)$ of finite period and let $J$ be a finite subgroup of* $\mathrm{C}(\sigma)$. *Set $R = F[x;\sigma]$ and $G = \{\phi_a \mid a \in \mathbf{N}, \phi \in J\}$. Then* $\mathrm{Gal}(R/R^G) = G$.

PROOF. Let $\sigma$ have finite period $m$. We first claim that for any $j$ not divisible by $m$, there exists $b \in \mathbf{N}$ such that $N_j(b) \neq 1$. Let $a \in F^*$ satisfy $\sigma^j(a) \neq a$ and let $b = a\sigma(a^{-1})$.

Then $N_j(b) = a\sigma^j(a^{-1}) \neq 1$. We now show $R^G = F^J[x^m]$. Note that if $c \in \mathbf{N}$, then $N_{im}(c) = 1$ for all $i \in Z^+$ and hence the inclusion $\supseteq$ follows. Let $\sum a_i x^i \in R^G$. Then for any $b \in \mathbf{N}$ and $\phi \in J$, we have

$$\sum a_i x^i = \phi_b(\sum a_i x^i) = \sum \phi(a_i) N_i(b) x^i,$$

showing $a_i = \phi(a_i)N_i(b)$. Thus if $a_i \neq 0$, $N_i(b) = N_i(c)$ for all $b, c \in \mathbf{N}$. We claim that $m | i$. Otherwise $i = km + \ell$ where $0 < \ell < m$ which implies $N_i(b) = N_{km}(b)\sigma^{km}\big(N_\ell(b)\big) = N_\ell(b)$ and hence $N_\ell(b) = N_\ell(c)$. Thus we can choose $N_\ell(b) \neq 1$ and taking $c = 1$, we obtain a contradiction. Therefore $m \mid i$, $a_i = \phi(a_i)$, and $\sum a_i x^i \in F^J[x^m]$ as desired.

Let $\phi_a \in \mathrm{Gal}(R/R^G)$. In particular, $x^m = \phi_a(x^m) = N_m(a)x^m$ implies $a \in \mathbf{N}$. Also for all $b \in F^J$, $b = \phi_a(b) = \phi(b)$. Thus $\phi \in \mathrm{Gal}(F/F^J) = J$ (since $J$ is a finite subgroup of Aut($F$), we may apply Artin's Theorem) and $\mathrm{Gal}(R/R^G) \leq G$. The other inclusion is clear. ∎

Note that if $J = \langle \sigma \rangle$ in the preceding theorem, then $\mathrm{Gal}(R/R^G) = G$ for $G = \mathrm{Xinn}(R)$. We give an example to show this result may fail if $\sigma$ has infinite period.

EXAMPLE (2). Let $R = Q(t)[x;\sigma]$ as in Example (1) with $G = \mathrm{Xinn}(R)$. We claim that $R^G = Q$. If $\sum h_i x^i \in R^G$, then for all $u \in Q(t)^*$, we have

$$\sum h_i x^i = \sigma_{u\sigma(u^{-1})}(\sum h_i x^i) = \sum \sigma(h_i) N_i\big(u\sigma(u^{-1})\big) x^i.$$

Taking $u = 1$, we get $\sigma(h_i) = h_i$ and hence, if there exists $i \neq 0$ such that $h_i \neq 0$, then $N_i\big(u\sigma(u^{-1})\big) = u\sigma^i(u^{-1}) = 1$ for all $u \in Q(t)^*$. This implies $\sigma^i$ is the identity on $Q(t)$, a contradiction. Hence $\sum h_i x^i = h_0 \in Q(t)^\sigma = Q$, proving $R^G \subseteq Q$. The other inclusion is clear. By Theorem 3 (2), $\mathrm{Aut}(R) = \{\phi_q \mid q \in Q(t)^*, \phi \in \mathbf{C}(\sigma)\}$. Since every automorphism of $Q(t)$ fixes $Q$, we have $\mathrm{Gal}(R/R^G) = \mathrm{Aut}(R) \neq G$.

The next two results characterize the derivations of $R[x;\sigma]$ when $R$ is prime.

THEOREM 7. *Let $R$ be any ring with $\sigma \in \mathrm{End}(R)$. Suppose $\delta$ is a derivation of $R$ satisfying $\delta\sigma = \sigma\delta$. Then $\delta$ can be extended to a derivation (also denoted $\delta$) of $R[x;\sigma]$ if and only if $\delta(x)r = \sigma(r)\delta(x)$ for all $r \in R$.*

PROOF. If $\delta$ extends to a derivation of $R[x;\sigma]$, then

$$\delta(x)r + \sigma\big(\delta(r)\big)x = \delta(x)r + x\delta(r) = \delta(xr) = \delta\big(\sigma(r)x\big) = \sigma(r)\delta(x) + \sigma\big(\delta(r)\big)x,$$

giving the desired result.

Now let $\delta(x) \in R[x;\sigma]$ satisfy $\delta(x)r = \sigma(r)\delta(x)$ for all $r \in R$ and define $\delta(x^m)$ recursively by $\delta(x^m) = x\delta(x^{m-1}) + \delta(x)x^{m-1}$ for $m \geq 1$. For all $r \in R$ and $m \geq 0$, define $\delta(rx^m) = r\delta(x^m) + \delta(r)x^m$. It is easy to verify by induction that

(i) $\delta(x^\ell)r = \sigma^\ell(r)\delta(x^\ell)$

(ii) $\delta(x^{\ell+m}) = x^\ell\delta(x^m) + \delta(x^\ell)x^m$

for all $r \in R$ and $\ell, m \geq 0$. We first check $\delta$ on monomials. For all $r, s \in R$ and $\ell, m \geq 0$,

$$\begin{aligned}\delta(rx^\ell sx^m) &= \delta\left(r\sigma^\ell(s)x^{\ell+m}\right) = r\sigma^\ell(s)\delta(x^{\ell+m}) + \delta\left(r\sigma^\ell(s)\right)x^{\ell+m} \\ &= r\sigma^\ell(s)\left(x^\ell\delta(x^m) + \delta(x^\ell)x^m\right) + r\delta\left(\sigma^\ell(s)\right)x^{\ell+m} + \delta(r)\sigma^\ell(s)x^{\ell+m} \\ &= rx^\ell s\delta(x^m) + r\sigma^\ell\left(\delta(s)\right)x^{\ell+m} + r\sigma^\ell(s)\delta(x^\ell)x^m + \delta(r)\sigma^\ell(s)x^{\ell+m} \\ &= rx^\ell\left(s\delta(x^m) + \delta(s)x^m\right) + \left(r\delta(x^\ell) + \delta(r)x^\ell\right)sx^m \\ &= rx^\ell\delta(sx^m) + \delta(rx^\ell)sx^m.\end{aligned}$$

Now $\delta(\sum_i b_ix^i \sum_j c_jx^j) = \sum_{i,j}\delta\left(b_ix^ic_jx^j\right) = \sum_{i,j}\left(b_ix^i\delta(c_jx^j) + \delta(b_ix^i)c_jx^j\right)$

$$\begin{aligned}&= (\sum_i b_ix^i)\left(\sum_j \delta(c_jx^j)\right) + \left(\sum_i \delta(b_ix^i)\right)(\sum_j c_jx^j) \\ &= (\sum_i b_ix^i)\delta(\sum_j c_jx^j) + \delta(\sum_i b_ix^i)(\sum_j c_jx^j),\end{aligned}$$

which proves $\delta$ is a derivation. ∎

Theorem 7 reduces the question of determining the derivations of $R[x;\sigma]$ to finding those $f \in R[x;\sigma]$ which satisfy $f(x)r = \sigma(r)f(x)$ for all $r \in R$. In the following result, we determine these polynomials when $R$ is prime and $\sigma \in \mathrm{Aut}(R)$.

THEOREM 8. *Let $R$ be a prime ring with $\sigma \in \mathrm{Aut}(R)$ and $f(x) \in R[x;\sigma]$. Then $f(x)r = \sigma(r)f(x)$ for all $r \in R$ if and only if $f(x) = g(x)x$ with $g(x) \in C[bx^m] \cap R[x;\sigma]$ where $C$ is the extended centroid of $R$, $b \in N(R)$, and $bx^m$ centralizes $R$.*

PROOF. Let $f(x) = \sum_{i=0}^n a_ix^i$. Then $f(x)r = \sigma(r)f(x)$ for all $r \in R$ implies $a_i\sigma^i(r) = \sigma(r)a_i$. If $a_i \neq 0$, then $a_i \in N(R)$ and hence $\sigma^{i-1}$ is $X$-inner. There are three cases to consider:

(1) $\langle\sigma\rangle$ $X$-outer and infinite: Thus $i = 1$ and $f(x) = ax$ with $a \in Z(R)$.

(2) $\langle\sigma\rangle$ $X$-outer of finite order $m$: Thus $m|(i-1)$ and so $i = mt_i + 1$, $a_i \in Z(R)$, and $f(x) = \left(\sum_i a_i(x^m)^{t_i}\right)x$.

(3) Some power of $\sigma$ is $X$-inner: Let $m$ be the smallest positive integer such that $\sigma^m = I_{b^{-1}}$ for some $b^{-1} \in N(R)$. Then $i = mt_i + 1$ and $\sigma^{i-1} = I_{a_i^{-1}} = I_{b^{-t_i}}$ which implies $a_i = \lambda_ib^{t_i}$ for $\lambda_i \in C$. Hence $f(x) = \left(\sum_i \lambda_ib^{t_i}(x^m)^{t_i}\right)x = (\sum_i \lambda_i(bx^m)^{t_i}\right)x$, as desired. The converse is clear. ∎

## REFERENCES


**1.** K. R. Goodearl and R. B. Warfield, Jr., *An Introduction to Noncommutative Noetherian Rings*, LMS Student Texts **16**, Cambridge University Press, Cambridge, 1989.

**2.** J. Matczuk, *Extended centroids of skew polynomials rings*, Math. J. Okayama Univ. **30**(1988), 13–20.

**3.** J. C. McConnell and J. C. Robson, *Noncommutative Noetherian Rings*, Wiley Series in Pure and Applied Mathematics, Wiley, Chichester, 1987.


https://doi.org/10.4153/CMB-1992-018-6 Published online by Cambridge University Press

4. D. S. Passman, *Infinite Crossed Products*, Pure and Applied Mathematics, **135**, Academic Press, Inc., San Diego, 1989.
5. L. Rowen, *Ring Theory, Volume I*, Pure and Applied Mathematics, **127**, Academic Press, Inc., San Diego, 1988.

*Department of Mathematics*
*California State University, Northridge*
*Northridge, California 91330*
*U.S.A.*

https://doi.org/10.4153/CMB-1992-018-6 Published online by Cambridge University Press