Canad. Math. Bull. Vol. 28 (1), 1985

EXTENDED CENTROIDS OF SKEW POLYNOMIAL RINGS

BY
JERRY D. ROSEN AND MARY PELES ROSEN

ABSTRACT. Let R be a prime ring with $\sigma \in \text{Aut}(R)$. We determine the extended centroid of the skew polynomial ring $R[x, \sigma]$ when (i) $\langle\sigma\rangle$ is X-outer of finite order, (ii) $\langle\sigma\rangle$ is X-outer and infinite, (iii) σ^m is X-inner and no smaller power of σ fixes the extended centroid of R.

Suppose $R \subseteq S$ are prime rings with extended centroids C and D respectively. A natural question to consider is the relationship between C and D. In this paper we investigate the situation where R is a prime ring and S is the skew polynomial ring over R with respect to $\sigma \in \text{Aut}(R)$, i.e., $S = R[x, \sigma]$. We use the notions of X-inner and X-outer automorphisms due to Kharchenko. In sections 2 and 3, the following cases are considered: (i) $\langle\sigma\rangle$ is X-outer of finite order m; (ii) $\langle\sigma\rangle$ is X-outer and infinite; (iii) m is the least positive integer such that σ^m is X-inner and no smaller power of σ fixes C.

We prove the extended centroid of $R[x, \sigma]$ is isomorphic to: (i) $C_0(x^m)$, the field of fractions of $C_0[x^m]$ (where C_0 denotes the fixed field of C under σ when extended to RC); (ii) C_0; (iii) $C_0(y)$ where $y = nx^m$ is central and n is in the set of R-normalizing elements of the Martindale ring of quotients.

1. **Preliminaries**. Let R be a ring and σ an automorphism of R. $R[x, \sigma]$ is the set of all polynomials in x where addition is as usual and multiplication is defined according to the rule $xr = r^\sigma x$, $r \in R$. These operations make $R[x, \sigma]$ into a ring. If R is a prime ring, it is easy to see that $R[x, \sigma]$ is prime. Cohn has determined the center of $R[x, \sigma]$ when R is a division ring.

PROPOSITION 1.1. [1, p. 61] *Let D be a division ring and $\sigma \in \text{Aut}(D)$. If no power of σ is inner on D, then the center of $D[x, \sigma]$ is Z_0, the subset of the center of D fixed by σ. If σ^m is inner but no lower power fixes the center of D, then the center of $D[x, \sigma]$ is $Z_0[y]$ where $y = dx^m$ is central.*

To generalize this result to prime rings, we need the notions of X-inner and X-outer automorphisms due to Kharchenko. We begin by summarizing the definition and main properties of the extended centroid and central closure of a prime ring R with 1.

Let $\mu = \{U\}$ be the collection of all nonzero two-sided ideals of R and consider the totality T of all left module homomorphisms ϕ: ${}_RU \to {}_RR$, where $U \in \mu$ and U and R are regarded as left R-modules. We write (ϕ, U) for an element of T and define an

Received by the editors June 3, 1983 and, in revised form, March 28, 1984.
AMS Subject Classification (1980): 16A12.

equivalence relation $\sim$ on T as follows: $(\phi, U) \sim (\psi, V)$ if $\phi = \psi$ on some $W \in \mu$ where $W \subseteq U \cap V$. Let $\overline{(\phi, U)}$ denote the equivalence class of (ϕ, U). The Martindale ring of quotients Q is defined to be the set of these equivalence classes. We make Q into a ring as follows:

$$\overline{(\phi, U)} + \overline{(\psi, V)} = \overline{(\phi + \psi, U \cap V)}$$

$$\overline{(\phi, U)}\,\overline{(\psi, V)} = \overline{(\phi \circ \psi, VU)} \text{ (composition acting on the right).}$$

R may be considered a subring of Q via the mapping $a \to \overline{(a_r, R)}$ where a_r is the right multiplication by a acting on R. We state some well-known properties of Q. The proofs can be found in [3].

LEMMA 1.2. *Let Q be as above with center C. Then*
(1) *Q is a prime ring, C is a field and C is the centralizer of R in Q.*
(2) *For any $0 \neq q \in Q$, there exists $U \in \mu$ such that $0 \neq Uq \subseteq R$.*
(3) *Any nonzero left R-submodule of Q intersects R nontrivially.*
(4) *If $\sigma \in \operatorname{Aut}(R)$, then σ extends uniquely to an automorphism of Q.*

C is called the extended centroid of R. The pair (ϕ, U) is permissible if ϕ: ${}_RU_R \to {}_RR_R$ is an (R,R)-bimodule homomorphism. C may also be characterized as the set $\{\overline{(\phi, U)} \in Q \mid (\phi, U)$ is permissible$\}$. We may now form the central closure RC of R. RC is a prime ring with center C. A prime algebra over a field F is said to be closed if F is already its extended centroid. We remark that RC is closed over C.

DEFINITION. $\sigma \in \operatorname{Aut}(R)$ is X-inner if there exists a unit $q \in Q$ such that $r^\sigma = q^{-1}rq$ for all $r \in R$. In other words, σ is X-inner if its extension to Q is an inner automorphism. Otherwise, σ is X-outer. For any group $G \subseteq \operatorname{Aut}(R)$, G is said to be X-outer if the only X-inner automorphism in G is the identity.

LEMMA 1.3. *Suppose G is a subgroup of* Aut (R) *which is X-outer. If $0 \neq a_1, a_2, b_1, b_2 \in R$ and $\sigma_1, \sigma_2 \in G$ such that*

$$a_1 r^{\sigma_1} b_1 + a_2 r^{\sigma_2} b_2 = 0 \text{ for all } r \in R,$$

then $a_1 = \lambda a_2$ for some $\lambda \in C$ and $\sigma_1 = \sigma_2$.

PROOF. Applying σ_1^{-1} to the above equation and then Lemma 2 of [4], there exists a unit $q \in Q$ with $a_1^{\sigma_1^{-1}} q = a_2^{\sigma_1^{-1}}$ and $q^{-1}rq = r^{\sigma_2\sigma_1^{-1}}$ for all $r \in R$. Since G is X-outer, $\sigma_1 = \sigma_2$ and hence $q \in C$, proving the lemma. $\square$

In this article we will be concerned with characterizing the extended centroids of related prime rings. The following lemmas will be useful for this purpose.

LEMMA 1.4. *Let R be a prime ring with center Z and extended centroid C. Suppose for any $0 \neq \overline{(\phi, U)} \in C$, there exists $0 \neq u \in U$ such that $u = az_1$ and $u\phi = az_2$ where $z_1, z_2 \in Z$, $a \in R$. Then C is isomorphic to the field of fractions of Z.*

PROOF. Set $\lambda = \overline{(\phi, U)} \in C$. Then $u = az_1$ and $u\phi = u\lambda = az_2$. Thus $u =$

$\lambda^{-1}az_2 = az_1$ implying $(\lambda^{-1}z_2 - z_1)a = 0$. Viewing this equation in RC, $\lambda^{-1}z_2 - z_1 = 0$. Hence $\lambda = z_1^{-1}z_2$ is in the field of fractions of Z. $\square$

LEMMA 1.5. *Let $R \subseteq S$ be prime rings with extended centroids C and D respectively. Suppose for any $0 \neq \overline{(\phi, U)} \in C$, there exists $0 \neq u \in U$ such that $u = a\lambda$ and $u\phi = a\beta$ where $\lambda, \beta \in D$, $a \in R$. Then C is embedded in D. Furthermore, if any nonzero left R-submodule of S intersects R nontrivially, then $C \cong D$.*

PROOF. Let $0 \neq \overline{(\phi, U)} \in C$ and $u \in U$ be as above. Define Φ: $SuS \to S$ by $\sum_i s_iut_i \to \sum_i s_i(u\phi)t_i$. We check Φ is well-defined: Suppose $\sum s_iut_i = 0$. Then $0 = \sum s_ia\lambda t_i = (\sum s_iat_i)\lambda$ (an equation in SD). Hence $\sum s_iat_i = 0$ which implies $0 = \sum s_ia\beta t_i = \sum s_i(u\phi)t_i$. Clearly $\overline{(\Phi, SuS)} \in D$. Note $\overline{(\phi, U)} = \overline{(\phi, RuR)}$ and define T: $C \to D$ by $\overline{(\phi, RuR)} \to \overline{(\Phi, SuS)}$. T is easily seen to be a ring homomorphism and C a field implies T is one-to-one.

Suppose any nonzero left R-submodule of S intersects R nontrivially. Let $0 \neq \overline{(\psi, V)} \in D$ and set $W = V \cap R$. By the assumption, W is a nonzero ideal of R. Since $W\psi$ is a nonzero R-submodule of S, $W\psi \cap R \neq 0$. Hence $U = \{w \in W | w\psi \in R\}$ is a nonzero ideal of R. Setting $\phi = \psi|_U$ we have $\overline{(\phi, U)}T = \overline{(\psi, V)}$. $\square$

We are also concerned with the prime ring $(RC)[x, \sigma]$ where σ denotes the extension to RC. An easy application of part (2) of Lemma 1.2 gives

LEMMA 1.6. *Any nonzero left $R[x, \sigma]$-submodule of $(RC)[x, \sigma]$ intersects $R[x, \sigma]$ nontrivially.*

2. $\langle \boldsymbol{\sigma} \rangle$ ***X*-outer**. In this section we assume $\langle \sigma \rangle$ is X-outer. Let Z denote the center of R and set $Z_o = \{z \in Z | z^\sigma = z\}$.

LEMMA 2.1. *If σ has finite period m, then the center of $R[x, \sigma]$ is $Z_o[x^m]$. If σ has infinite period, the center of $R[x, \sigma]$ is Z_o.*

PROOF. Suppose $f(x) = \sum_i r_ix^i \in$ center $(R[x, \sigma])$. Commuting $f(x)$ with x, we obtain $r_i^\sigma = r_i$ for all i. Commuting $f(x)$ with any $a \in R$, we have $ar_i = r_ia^{\sigma^i}$ for all i. If $r_i \neq 0$, then r_i is a unit in Q and hence σ^i is X-inner. If σ has finite period m, then $m | i$ and $r_i \in Z_o$. If σ has infinite period, then $i = 0$ and $f(x) = r_0 \in Z_o$. $\square$

In the next two theorems we determine the extended centroid of $R[x, \sigma]$ in the cases where $\langle \sigma \rangle$ is finite and infinite.

THEOREM 2.2. *Let R be a prime ring with extended centroid C and $\langle \sigma \rangle$ X-outer of finite order m. Let C_o denote the fixed field of C under σ when extended to RC. Then the extended centroid of $R[x, \sigma]$ is isomorphic to $C_o(x^m)$, the field of fractions of $C_o[x^m]$.*

PROOF. We first assume R is closed prime over C and show $R[x, \sigma]$ satisfies the hypotheses of Lemma 1.4. σ extends to an automorphism $\hat{\sigma}$ of $R[x, \sigma]$ as follows: $\sum_i r_ix^i \to \sum_i r_i^\sigma x^i$. To see $\hat{\sigma}$ is multiplicative, we check its effect on monomials:

$$[(rx^j)(sx^k)]^{\hat{\sigma}} = (rs^{\sigma^j}x^{j+k})^{\hat{\sigma}} = r^\sigma s^{\sigma^{j+1}}x^{j+k} = (r^\sigma x^j)(s^\sigma x^k) = (rx^j)^{\hat{\sigma}}(sx^k)^{\hat{\sigma}}.$$

$\hat{\sigma}$ is also of period m. From now on, we write σ for $\hat{\sigma}$.

Let $0 \neq \overline{(\phi, U)} \in$ extended centroid of $R[x, \sigma]$. By considering $0 \neq \bigcap_{i=0}^{m-1} U^{\sigma^i}$, we may assume U is σ-invariant. Let n be the minimal degree of elements of U and set $S = \{f \in U \mid \deg f = n\}$. We claim S contains an element whose coefficients are fixed by σ. Let $V = \{a \in R \mid a$ is the leading coefficient of some $f \in S\}$. Set $V' = V \cup \{0\}$. V' is clearly an ideal of R. Suppose $a \in V$ and $f \in S$ with leading coefficient a. Since U is σ-invariant, $f^\sigma \in S$ with leading coefficient a^σ, showing V' is σ-invariant. By Theorem 3.17 of [3], $\mathrm{tr}_\sigma(V') \neq 0$ where tr denotes the trace relative to $\langle\sigma\rangle$. So there exists $a \in V$ such that $\mathrm{tr}_\sigma(a) \neq 0$. Let

$$f(x) = \sum_{i=k}^{n} a_i x^i$$

with $a_n = a$. Now

$$\mathrm{tr}_\sigma(f(x)) = \sum_{i=k}^{n} (\mathrm{tr}_\sigma(a_i))x^i.$$

Since $f \in U = U^\sigma$, $\mathrm{tr}_\sigma(f(x)) \in U$ and $\mathrm{tr}_\sigma(a) \neq 0$ implies $\mathrm{tr}_\sigma(f(x)) \in S$. Furthermore, the coefficients of $\mathrm{tr}_\sigma(f(x))$ are fixed by σ, proving the claim.

Hence we may choose

$$f(x) = \sum_{i=k}^{n} a_i x^i \in U$$

with $a_n = a$ and $a_i^\sigma = a_i$ for all i. For any $r \in R$,

$$f(x)ra - ar^{\sigma^n} f(x) = \sum_{i=k}^{n-1} (a_i r^{\sigma^i} a - ar^{\sigma^n} a_i)x^i \in U.$$

By minimality, $a_i r^{\sigma^i} a - ar^{\sigma^n} a_i = 0$, $i = k, \ldots, n-1$. By Lemma 1.3, $a_i = \lambda_i a$, $\lambda_i \in C$ and $\sigma^i = \sigma^n$ for all i. Since σ fixes a_i and a, $\lambda_i \in C_0$. Also $\sigma^k = \ldots = \sigma^n$ implies the indices are all congruent to k mod m, i.e., $i = k + q_i m$, $q_i \in Z^+ \cup \{0\}$. Therefore $f(x) = (ax^k)g(x)$ where

$$g(x) = \sum_{i=k}^{n} \lambda_i x^{q_i m} \in C_0[x^m],$$

the center of $R[x, \sigma]$.

Suppose

$$(f(x))\phi = \sum_{j=\ell}^{p} b_j x^j.$$

Using the fact that each $a_i^\sigma = a_i$ and ϕ is bimodule, we obtain $x[(f(x))\phi] = [(f(x))\phi]x$. It follows that $b_j^\sigma = b_j$ for all j. For any $r \in R$, we have

$$0 = (f(x)ra - ar^{\sigma^n} f(x))\phi = [(f(x))\phi]ra - ar^{\sigma^n}[(f(x))\phi]$$
$$= \sum_{j=\ell}^{p} (b_j r^{\sigma^j} a - ar^{\sigma^n} b_j)x^j.$$

Thus we have $b_j r^{\sigma^j} a - ar^{\sigma^n} b_j = 0, j = \ell, \ldots, p$. As before, $b_j = \alpha_j a$ where $\alpha_j \in C_0$, $\sigma^j = \sigma^n$ and $j = \ell + w_j m$, $w_j \in Z^+ \cup \{0\}$. Hence $(f(x))\phi = (ax^\ell)h(x)$ where

$$h(x) = \sum_{j=\ell}^{p} \alpha_j x^{w_j m} \in C_0[x^m].$$

Since $\sigma^k = \sigma^n = \sigma^\ell$, we have $k \equiv \ell \pmod{m}$. If $k > \ell$, then $k = \ell + tm$, $t \in Z^+$. In this case, $f(x) = (ax^\ell)q(x)$ for some $q(x) \in C_0[x^m]$. Similarly, if $\ell > k$, $(f(x))\phi = (ax^k)p(x)$ for some $p(x) \in C_0[x^m]$. By Lemma 1.4, the extended centroid of $R[x,\sigma]$ is isomorphic to $C_0(x^m)$.

Now suppose R is a prime ring and let σ denote the extension to RC. One can show $\langle\sigma\rangle$ is X-outer on RC of order m. Since RC is closed prime over C, the extended centroid of $(RC)[x,\sigma]$ is isomorphic to $C_0(x^m)$. Let $0 \neq \overline{(\phi, U)} \in$ extended centroid of $R[x,\sigma]$. By the above argument, there exists $0 \neq f(x) \in U$ such that $f(x) = a(x)z_1(x)$ and $(f(x))\phi = a(x)z_2(x)$ where $z_1(x)$, $z_2(x) \in C_0[x^m]$ (the center of $(RC)[x,\sigma]$), $a(x) \in R[x,\sigma]$. By Lemmas 1.5 and 1.6, we may conclude $R[x,\sigma]$ and $(RC)[x,\sigma]$ have isomorphic extended centroids, completing the proof of the theorem. $\square$

THEOREM 2.3. *Let R be a prime ring with extended centroid C. If $\langle\sigma\rangle$ is X-outer and infinite, then the extended centroid of $R[x,\sigma]$ is isomorphic to C_0.*

PROOF. Assume R is closed prime. Let $0 \neq \overline{(\phi, U)} \in$ extended centroid of $R[x,\sigma]$. Choose

$$0 \neq f(x) = \sum_{i=k}^{n} a_i x^i \in U, \qquad a_n = a,$$

of minimal degree. We claim $a_i = 0$ for $i = k, \ldots, n-1$. Suppose $a_j \neq 0$ for some j such that $k \leq j \leq n-1$. There exists $b \in R$ such that $b^{\sigma^n} = a$. For any $r \in R$,

$$f(x)rb - ar^{\sigma^n} f(x) = \sum_{i=k}^{n-1} (a_i r^{\sigma^i} b^{\sigma^i} - ar^{\sigma^n} a_i)x^i \in U.$$

By minimality, $a_j r^{\sigma^j} b^{\sigma^j} - ar^{\sigma^n} a_j = 0$. By Lemma 1.3, $\sigma^j = \sigma^n$ and σ of infinite period implies $j = n$, a contradiction. Hence $f(x) = ax^n$. A similar argument gives $(f(x))\phi = \lambda ax^n$ for some $\lambda \in C$.

We now show $\lambda \in C_0$. Since R is prime, we may choose $r \in R$ such that $ar^{\sigma^n} a^{\sigma^n} \neq 0$. ϕ bimodule implies $f(x)r[(f(x))\phi] = [(f(x))\phi]rf(x)$. So we have $(ax^n)r(\lambda ax^n) = (\lambda ax^n)r(ax^n)$ which gives

$$\lambda^{\sigma^n} ar^{\sigma^n} a^{\sigma^n} = \lambda ar^{\sigma^n} a^{\sigma^n}$$

https://doi.org/10.4153/CMB-1985-006-1 Published online by Cambridge University Press

or

$$(\lambda^{\sigma^n} - \lambda)ar^{\sigma^n}a^{\sigma^n} = 0.$$

Hence $\lambda^{\sigma^n} = \lambda$. Now choose $r \in R$ such that $ar^{\sigma^{n+1}}a^{\sigma^{n+1}} \neq 0$. As above, $f(x)xr[(f(x))\phi] = [(f(x))\phi]xrf(x)$ yields $\lambda^{\sigma^{n+1}} = \lambda$ and so $\lambda \in C_0$.

Therefore $f(x) = ax^n$ and $(f(x))\phi = (ax^n)\lambda$ where $\lambda \in C_0$ (the center of $R[x, \sigma]$). By Lemma 1.4, the extended centroid of $R[x, \sigma]$ is isomorphic to C_0.

Now suppose R is a prime ring and let σ denote the extension to RC. One can show $\langle\sigma\rangle$ is X-outer and infinite. Since RC is closed prime, the extended centroid of $(RC)[x, \sigma]$ is isomorphic to C_0. As in Theorem 2.2, $R[x, \sigma]$ and $(RC)[x, \sigma]$ have isomorphic extended centroids. $\square$

3. **σ^m X-inner**. To treat the case where σ^m is X-inner for some m, we need the notion of the normal closure of a prime ring R. Set $N = \{n \in Q \mid nR = Rn\}$. We remark that if $0 \neq n \in N$, then n is invertible and $n^{-1} \in N$. The normal closure RN of R in Q is the subring of Q generated by R and N, i.e.,

$$RN = \left\{\sum_i r_i n_i \in Q \mid r_i \in R,\ n_i \in N\right\}.$$

LEMMA 3.1. *RN has the following properties* [3]:
(1) *RN is a closed prime ring with extended centroid C.*
(2) *For any $0 \neq q \in RN$, there exists a nonzero ideal I of R such that $0 \neq Iq \subseteq R$ and $0 \neq qI \subseteq R$.*
(3) *If $\sigma \in$ Aut (R), then its extension to Q restricts to an automorphism of RN.*

LEMMA 3.2. *For any $\sigma \in$ Aut (R), $R[x, \sigma]$ and $(RN)[x, \sigma]$ have isomorphic extended centroids.*

PROOF. Let E and F be the extended centroids of $R[x, \sigma]$ and $S = (RN)[x, \sigma]$ respectively. Choose $0 \neq \overline{(\phi, U)} \in E$. Define Φ: $SUS \to S$ by

$$\sum_i f_i(x)u_i(x)g_i(x) \to \sum_i f_i(x)[(u_i(x))\phi]g_i(x).$$

Suppose

$$\sum_i f_i(x)u_i(x)g_i(x) = 0$$

where

$$f_i(x) = \sum_j a_{ij}x^j$$

and

$$g_i(x) = \sum_k b_{ik}x^k.$$

https://doi.org/10.4153/CMB-1985-006-1 Published online by Cambridge University Press

By Lemma 3.1, there exists a nonzero ideal I of R such that $0 \neq Ia_{ij} \subseteq R$ and $0 \neq b_{ik}I \subseteq R$. For each i, set $J_i = \bigcap_k I^{(\sigma^k)^{-1}}$ where k runs through the sum in $g_i(x)$. Then $0 \neq g_i(x)J_i \subseteq R[x,\sigma]$. Set $J = \bigcap_i J_i$. J is a nonzero ideal of R and $0 \neq g_i(x)J \subseteq R[x,\sigma]$ for all i. Hence we have

$$I\Big(\sum_i f_i(x)[(u_i(x))\phi]g_i(x)\Big)J = 0$$

which implies

$$\sum_i f_i(x)[(u_i(x))\phi]g_i(x) = 0,$$

proving Φ is well-defined. Define T: $E \to F$ by$(\overline{\phi, U}) \to (\overline{\Phi, SUS})$. The usual argument shows T is a ring isomorphism. $\square$

For the remainder of this section, let m be the least positive integer such that σ^m is X-inner. We assume no lower power of σ is the identity on C. Note that by a result of Kharchenko [3, p. 48], if R satisfies a GPI, this assumption is superfluous.

LEMMA 3.3. *The center of* $(RN)[x,\sigma]$ *is* $C_0[y]$ *where* $y = nx^m$ *is central.*

PROOF. Since σ^m is X-inner, there exists $n \in N$ such that $a^{\sigma^m} = n^{-1}an$ for all $a \in Q$. It is easy to verify that $n^\sigma n^{-1} = \lambda \in C$ and the norm of λ (i.e., $\lambda^{\sigma^{m-1}}\lambda^{\sigma^{m-2}}\dots\lambda^\sigma\lambda$) equals 1. Since σ induces an automorphism of period m on C, Hilbert's Theorem 90 implies $\lambda = \mu^\sigma\mu^{-1}$, $\mu \in C$. Setting $n_1 = n\mu^{-1}$, observe that $n_1^\sigma = n_1$ and $a^{\sigma^m} = n_1^{-1}an_1$ for all $a \in Q$. Hence without loss of generality, we may assume $n^\sigma = n$. Set $y = nx^m$. Then $xy = xnx^m = n^\sigma x^{m+1} = nx^m x = yx$ and $ya = nx^m a = n(n^{-1}an)x^m = ay$ for any $a \in RN$. So $C_0[y] \subseteq$ center $((RN)[x,\sigma])$.

Suppose

$$f(x) = \sum_i a_i x^i \in \text{center } ((RN)[x,\sigma]).$$

As usual, $a_i^\sigma = a_i$ and $sa_i = a_i s^{\sigma^i}$ for all i and $s \in RN$. If $a_i \neq 0$, then σ^i is X-inner and hence $i = mq_i$ where $q_i \in Z^+ \cup \{0\}$. Now $a_i^{-1}sa_i = s^{\sigma^{mq_i}} = n^{-q_i}sn^{q_i}$ for all $s \in RN$ implying $a_i = \lambda_i n^{q_i}$, $\lambda_i \in C$. Since a_i and n are fixed by σ, $\lambda_i \in C_0$. Rewriting we have

$$f(x) = \sum_i \lambda_i(nx^m)^{q_i} = \sum_i \lambda_i y^{q_i} \in C_0[y]. \quad \square$$

The proof of Lemma 3.3 follows Cohn [1]. We now prove the main result of this section.

THEOREM 3.4. *Let R be a prime ring with extended centroid C and m the least positive integer such that σ^m is X-inner. If no smaller power of σ fixes C, then the extended centroid of $R[x,\sigma]$ is isomorphic to $C_0(y)$ where $y = nx^m$ is central.*

PROOF. For any $a \in Q$, $a^{\sigma^m} = n^{-1}an$ where $n \in N$ and $n^\sigma = n$. By Lemma 3.2, it suffices to show that the extended centroid of $(RN)[x,\sigma]$ is isomorphic to $C_0(y)$. Let

$0 \neq \overline{(\phi, U)} \in$ extended centroid of $(RN)[x, \sigma]$ and choose

$$f(x) = \sum_{i=k}^{p} a_i x^i \in U$$

of minimal degree. There exists $b \in RN$ such that $b^{\sigma^p} = a_p = a$. For any $s \in RN$, $f(x)sb - as^{\sigma^p} f(x) \in U$ of smaller degree than f implying $as^{\sigma^p} a_i - a_i s^{\sigma^i} b^{\sigma^i} = 0$, $i = k, \ldots, p - 1$. Applying $(\sigma^p)^{-1}$ to this equation and Lemma 2 of [4], there exists $n_i \in N$ such that $a_i = an_i^{\sigma^p}$ and $n_i^{-1} sn_i = s^{\sigma^i}(\sigma^p)^{-1}$. Thus $\sigma^i(\sigma^p)^{-1}$ is X-inner and $\sigma^i = \sigma^p$ on C. It follows that $\sigma^i = \sigma^k$ on C and since $\sigma \in \text{Aut}(C)$ is of period m, $i = k + q_i m$ where $q_i \in Z^+ \cup \{0\}$, $i = k, \ldots, p$. Now $\sigma^i(\sigma^p)^{-1} = \sigma^{(q_i - q_p)m}$ implies $n_i^{-1} sn_i = n^{q_p - q_i} sn^{q_i - q_p}$ for all $s \in RN$. Therefore $n_i = \alpha_i n^{q_i - q_p}$, $\alpha_i \in C$, and $a_i = a(\alpha_i n^{q_i - q_p})^{\sigma^p} = a\beta_i n^{q_i - q_p}$, $\beta_i \in C$. Setting $y = nx^m$ we have

$$f(x) = \sum_{i=k}^{p} a\beta_i n^{q_i - q_p} x^{k + q_i m} = an^{-q_p} x^k \sum_{i=k}^{p} \beta_i^{(\sigma^k)^{-1}} n^{q_i} x^{q_i m} = an^{-q_p} x^k \sum_{i=k}^{p} \gamma_i y^{q_i}$$

for some $\gamma_i \in C$.

Suppose

$$(f(x))\phi = \sum_{j=\ell}^{r} b_j x^j.$$

For any $s \in RN$,

$$0 = (f(x)sb - as^{\sigma^p} f(x))\phi = [(f(x))\phi]sb - as^{\sigma^p}[(f(x))\phi]$$
$$= \sum_{j=\ell}^{r} (b_j s^{\sigma^j} b^{\sigma^j} - as^{\sigma^p} b_j) x^j$$

which implies $as^{\sigma^p} b_j - b_j s^{\sigma^j} b^{\sigma^j} = 0$, $j = \ell, \ldots, r$. As before, there exists $m_j \in N$ such that $b_j = am_j^{\sigma^p}$, $m_j^{-1} sm_j = s^{\sigma^j(\sigma^p)^{-1}}$, and $\sigma^j = \sigma^p$ on C. Thus $\sigma^k = \ldots = \sigma^p = \sigma^\ell = \ldots = \sigma^r$ on C. So $j = \ell + w_j m$ for all j and $p = \ell + tm$ where $w_j \in Z^+ \cup \{0\}$, $t \in Z$. Hence $m_j^{-1} sm_j = n^{t - w_j} sn^{w_j - t}$ and so $m_j = \delta_j n^{w_j - t}$, $\delta_j \in C$. As above, $b_j = a\lambda_j n^{w_j - t}$ and

$$(f(x))\phi = an^{-t} x^\ell \sum_{j=\ell}^{r} \rho_j y^{w_j}$$

for some $\rho_j \in C$.

Assume $k > \ell$. Now $p = \ell + tm = k + q_p m$ implies $k = \ell + (t - q_p)m$, $t - q_p \in Z^+$. Then

$$f(x) = an^{-q_p} x^{\ell + (t - q_p)m} \sum_{i=k}^{p} \gamma_i y^{q_i} = an^{-q_p} x^\ell \sum_{i=k}^{p} \nu_i x^{(t - q_p)m} y^{q_i}$$
$$= an^{-q_p} x^\ell \sum_{i=k}^{p} \nu_i n^{q_p - t} y^{t - q_p + q_i} = an^{-t} x^\ell \sum_{i=k}^{p} \nu_i y^{t - q_p + q_i}$$

for some $\nu_i \in C$.

An analogous argument works for $\ell > k$. Summarizing, we have shown that $f(x) =$

$an^ix^jg_1(y)$ and $(f(x))\phi = an^ix^jg_2(y)$ for some i, j and $g_1(y), g_2(y) \in C[y]$. We are not yet in a position to apply Lemma 1.4 since $g_1(y)$ and $g_2(y)$ are not necessarily in $C_o[y]$, the center of $(RN)[x, \sigma]$.

Now σ may be extended to $C[y]$ by mapping y to y. We claim $g_1(y)^\sigma g_2(y) = g_1(y)g_2(y)^\sigma$. First note that $C[y]$ centralizes RN in S = central closure of $(RN)[x, \sigma]$. Also if R is any prime ring, $\sigma \in \text{Aut}(R)$, and $p(x)Rq(x) = 0$ for $p(x), q(x) \in R[x, \sigma]$, then $p(x) = 0$ or $q(x) = 0$. For any $s \in RN, f(x)s[(f(x))\phi] = [f(x))\phi]sf(x)$ implies

$$(an^ix^j)s(an^ix^j(g_1(y)^{\sigma^j}g_2(y) - g_1(y)g_2(y)^{\sigma^j})) = 0.$$

Since $an^ix^j \neq 0$ the above remarks give $g_1(y)^{\sigma^j}g_2(y) - g_1(y)g_2(y)^{\sigma^j} = 0$. By using xs, we similarly obtain $g_1(y)^{\sigma^{j+1}}g_2(y) - g_1(y)g_2(y)^{\sigma^{j+1}} = 0$. The claim follows from these two equations.

Working in S, we have $f(x) = an^ix^jg_1(y)$ and $f(x)\lambda = an^ix^jg_2(y)$ for $\lambda = (\phi, U) \in$ extended centroid of $(RN)[x, \sigma]$. Hence $an^ix^j(g_1(y) - \lambda^{-1}g_2(y)) = 0$. If $g_1(y) - \lambda^{-1}g_2(y) \neq 0$, there exists a nonzero ideal V of $(RN)[x, \sigma]$ such that $0 \neq (g_1(y) - \lambda^{-1}g_2(y))V \subseteq (RN)[x, \sigma]$. Thus

$$(an^ix^j)(RN)(g_1(y) - \lambda^{-1}g_2(y))V = 0$$

implies

$$(g_1(y) - \lambda^{-1}g_2(y))V = 0,$$

a contradiction. Therefore $g_2(y) = \lambda g_1(y)$.

Note that the extension of σ to $C[y]$ agrees with the extension of σ to S when restricted to $C[y]$. Also the fixed ring of $\langle\sigma\rangle$ acting on $C[y]$ is $C_o[y]$.

Finally $g_1(y)^\sigma g_2(y) = g_1(y)g_2(y)^\sigma$ and $g_2(y) = \lambda g_1(y)$ imply $(\lambda - \lambda^\sigma)g_1(y)g_1(y)^\sigma = 0$ and so $\lambda^\sigma = \lambda$. Since any nonzero ideal of $C[y]$ intersects $C_o[y]$ nontrivially, there exists $0 \neq h(y) \in C[y]$ such that $0 \neq g_2(y)h(y) = \lambda g_1(y)h(y) \in C_o[y]$. It follows that $g_1(y)h(y) \in C_o[y]$. Now $0 \neq f(x)h(y) = an^ix^jg_1(y)h(y) \in U$ and $(f(x)h(y))\phi = [(f(x))\phi]h(y) = an^ix^jg_2(y)h(y)$ where $g_1(y)h(y), g_2(y)h(y) \in C_o[y]$. By Lemmas 1.4 and 3.3, the extended centroid of $(RN)[x, \sigma]$ is isomorphic to $C_o(y)$. □

We end this paper with a brief discussion of the remaining case: σ^m is X-inner and some lower power of σ is the identity on C. The primary difficulty seems to be in determining the center of $(RN)[x, \sigma]$. We can no longer use Hilbert's Theorem 90 to find an n fixed by σ that determines σ^m as an inner automorphism of Q. As already noted, if R satisfies a GPI, this remaining case cannot occur.

ACKNOWLEDGEMENT: We would like to thank the referee for finding an error in our first draft as well as for making several suggestions to improve the exposition. We are also grateful for his/her encouragement to extend our original work.

REFERENCES

1. P. M. Cohn, *Skew field constructions*. LMS Lecture Note Series 27, Cambridge University Press,

Cambridge, 1977.

2. V. K. Kharchenko, *Generalized identities with automorphisms*. Algebra i Logika **14** (1975), pp. 215–237. (English transl. Algebra and Logic **14** (1976), pp. 132–148).

3. S. Montgomery, *Fixed rings of finite automorphism groups of associative rings*. Lecture Notes in Math. No. 818. Springer-Verlag, Berlin, 1980.

4. S. Montgomery and D. S. Passman, *Outer Galois theory of prime rings*. Rocky Mountain Journal of Mathematics **14** (1984), pp. 305–318.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF IOWA
IOWA CITY, IOWA 52242