Math. J. Okayama Univ. 30 (1988), 13－20

EXTENDED CENTROIDS OF SKEW POLYNOMIAL RINGS

Dedicated to Professor Hisao Tominaga on his 60th birthday

JERZY MATCZUK

Let R be a prime ring with Martindale's ring of quotient Q. Let ϕ denote either an automorphism or a derivation of R. The aim of this paper is to show that the extended centroid of the skew polynomial ring $R[t, \phi]$ is equal to ZZ^{-1}, where Z is the center of $Q[t, \phi]$. In this case when ϕ is an automorphism of R, the above mentioned result was partially proved in [6]. Below is a uniform and shorter description of the center of $R[t, \phi]$ similar to the one known in the case R is a simple ring (cf. [1], [2]).

1. Preliminaries. Throughout the paper R and Q will denote a prime ring and its left Martindale's ring of quotient, respectively. C will stand for the extended centroid of R equal, by definition, to the center of Q. The subring of Q generated by R and C is called the central closure of R. In the following lemma we recall the well-known properties of Q (see [3]).

Lemma 1.1. 1. *For any $q_0, \ldots, q_n \in Q$ there exists a non-zero ideal I of R such that $Iq_i \subset R$ for $0 \leq i \leq n$.*

2. *If $Iq = 0$ or $qI = 0$ for some $q \in Q$ and a non-zero ideal I of R, then $q = 0$.*

3. *If I is a non-zero ideal of R and $\alpha: I \to R$ is a homomorphism of left R-module ($(R\text{-}R)$-bimodule), then there exists $q \in Q$ ($q \in C$) such that $\alpha(x) = xq$ for all $x \in I$.*

In the paper ϕ will always denote either an automorphism or a derivation of R. It is well-known that ϕ has a unique extension to Q. The extension will be also denoted by ϕ.

In the sequel we will use the following generalization of Martindale's lemma which is due to S. Montgomery and D. Passman ([5]).

Lemma 1.2. *Let ϕ be an automorphism of R and $0 \neq q \in Q$. If $q\phi(r) = rq$ for all $r \in R$, then q is an invertible element and ϕ is an inner automorphism of Q determined by q.*

Let us recall that the skew polynomial ring $R[t, \phi]$ is a free left R-

module with the basis 1, t, t^2,... and multiplication defined according to the rule: for any $r \in R$

$$tr = \begin{cases} \phi(r)t & \text{if } \phi \text{ is an automorphism of } R \\ rt + \phi(t) & \text{if } \phi \text{ is a derivation of } R. \end{cases}$$

We will frequently use, without indicating, the following easy consequence of Lemma 1.1.

Lemma 1.3. *Let $v \in V$, the central closure of $Q[t, \phi]$. If $Iv = 0$ for some non-zero ideal I of R, then $v = 0$.*

Proof. Let $v \in V$ and J be a non-zero ideal of $Q[t, \phi]$ such that $vJ \subset Q[t, \phi]$. Since $I(vJ) = 0$, Lemma 1.2 implies that $vJ = 0$ and $v = 0$.

2. The center of R[t, ϕ]. At the begining we will show that while investigating either the center or the extended centroid of $R[t, \phi]$ it is enough to look at either of these of $Q[t, \phi]$.

For a prime ring B, $Z(B)$, $C(B)$ will stand for the center, the extended centroid of B, respectively.

Lemma 2.1. 1. $Z(R[t, \phi]) = Z(Q[t, \phi]) \cap R[t, \phi]$.
2. $C(R[t, \phi])$ *is isomorphic to* $C(Q[t, \phi])$.

Proof. 1. Let $f \in Z(R[t, \phi])$ and $h \in Q[t, \phi]$. There exists a non-zero ideal I of R such that $Ih \subset R[t, \phi]$. For any $r \in I$ we have $rfh = f(rh) = rhf$. Hence $0 = I(fh - hf)$. It means that $fh = hf$ and $f \in Z(Q[t, \phi])$. The reverse inclusion is obvious.

2. Let $c \in C(R[t, \phi])$ and I be a non-zero ideal of $R[t, \phi]$ such that $cI \subset R[t, \phi]$. Define α: $Q[t, \phi]IQ[t, \phi] \to Q[t, \phi]$ by the rule $\alpha(\sum g_i a_i f_i) = \sum g_i c a_i f_i$ where $g_i, f_i \in Q[t, \phi]$, $a_i \in I$. To see that α is well-defined suppose that $\sum_{i=0}^{n} g_i a_i f_i = 0$. Let J be a non-zero ideal of R such that $Jg_i \subset R[t, \phi]$ for $0 \leq i \leq n$. Then for any $r \in J$ and $a \in I$

$$0 = (ca)r \sum_{i=0}^{n} g_i a_i f_i = \sum_{i=0}^{n} (ca(rg_i)a_i) f_i = ar \sum_{i=0}^{n} g_i c a_i f_i.$$

Thus $IJ \sum_{i=0}^{n} g_i c a_i f_i = 0$. This implies that $\sum_{i=0}^{n} g_i c a_i f_i = 0$. Because α is a homomorphism of $(Q[t, \phi]\text{-}Q[t, \phi])$-bimodules, α defines an element

$c_a \in C(Q[t, \phi])$. Now it is easy to check that the map $L: C(R[t, \phi]) \to C(Q[t, \phi])$ given by $L(c) = c_a$ is an isomorphism with the inverse L^{-1} described as follows: for any $c \in C(Q[t, \phi])$ $I_c = \{f \in R[t, \phi] \mid cf \in R[t, \phi]\}$ is a non-zero ideal of $R[t, \phi]$, and the restriction of the multiplication by c to I_c determines the element $L^{-1}(c) \in C(R[t, \phi])$.

Suppose now that $\phi = \sigma$ is an automorphism of R. The inner automorphism determined by an invertible element b will be denoted by σ_b.

Lemma 2.2. *Let* $T = \sum_{i=0}^{n} a_i t^i \in Z(Q[t, \sigma])$. *Then*:

1. $\sigma(a_i) = a_i$ *for* $0 \leq i \leq n$.
2. *If* $a_i \neq 0$ *for some* $0 \leq i \leq n$, *then* a_i *is invertible in* Q *and* $\sigma^i = \sigma_{a_i}$.
3. $a_i t^i \in Z(Q[t, \sigma])$ *for* $0 \leq i \leq n$.

Proof. The equality $Tt = tT$ gives 1.

2. For any $r \in R$ $rT = Tr$. Hence $ra_i = a_i \sigma^i(r)$ for all $r \in R$ and $0 \leq i \leq n$. Now, by using Lemma 1.2, we get 2. The statement 3 is a consequence of 1 and 2.

Proposition 2.3. *Let* $C_\sigma = \{c \in C \mid \sigma(c) = c\}$.

1. *If* σ^k *is not an inner automorphism of* Q *for all* $k \geq 1$, *then* $Z(Q[t, \sigma]) = C_\sigma$.
2. *If* σ^k *is an inner automorphism of* Q *for some* $k \geq 1$, *then* $Z(Q[t, \sigma]) = C_\sigma[bt^m]$, *where* m *is the smallest non-zero number such that* σ^m *is an inner automorphism of* Q *and there exists a* σ*-invariant element* $b \in Q$ *determing* σ^m.

Proof. The statement 1 is clear because of Lemma 2.2.

2. Suppose that $k \geq 1$ and $\sigma^k = \sigma_q$ for some $q \in Q$. For any $i \geq 0$ we have $\sigma^k = \sigma^i \sigma^k \sigma^{-i} = \sigma_{\sigma^i(q)}$. Hence

$$\sigma^{k^2} = \sigma_{\sigma^{k-1}(q)} \cdots \sigma_q = \sigma_{q\sigma(q)\cdots\sigma^{k-1}(q)}.$$

Let $a = q\sigma(q)\cdots\sigma^{k-1}(q)$. Then $\sigma^k(a) = a$ since $\sigma^k(q) = q$, and

$$\sigma(a) = \sigma(q)\cdots\sigma^{k-1}(q)q = q^{-1}aq = \sigma^k(a) = a.$$

Thus σ^{k^2} is an inner automorphism of Q determined by the element $a \in Q$ such that $\sigma(a) = a$. By the above there exists the minimal natural number m such that σ^m is an inner automorphism of Q determined by a σ-invariant

element $b \in Q$. Lemma 2.2 and the choice of m imply that $bt^m \in Z(Q[t, \sigma])$ is a polynomial of minimal non-zero degree. In particular $C_\sigma[bt^m] \subset Z(Q[t, \sigma])$. Let $pt^k \in Z(Q[t, \sigma])$ for some $p \in Q$. If $k < m$ then $k = 0$ and $p \in C_\sigma$. *If* $k \geq m$, then $pt^k = pb^{-1}t^{k-m}bt^m$. Since both pt^k and bt^m are central in $Q[t, \sigma]$, $pb^{-1}t^{k-m} \in Z(Q[t, \sigma])$. By the induction hypothesis $pb^{-1}t^{k-m} \in C_\sigma[bt^m]$, and $pt^k \in C_\sigma[bt^m]$. This shows that every monomial from $Z(Q[t, \sigma])$ belongs to $C_\sigma[bt^m]$. Now the statement 2 is a consequence of Lemma 2.2.

The argumentation showing that if σ^k is an inner automorphism then σ^{k^2} is an inner automorphism determined by σ-invariant element is due to G. Cauchon ([2]).

Suppose now, that $\phi = d$ is a derivation of R.

Proposition 2.4. *Let* $C_d = \{c \in C \mid d(c) = 0\}$. *Then either* $Z(Q[t, d]) = C_d$ *or* $Z(Q[t, d]) = C_d[z]$ *where* z *has the following form*:

$$z = \begin{cases} t - a \text{ if } charR = 0 \text{ and } d \text{ is an inner derivation of } Q \text{ adjoint to } a \\ t^{p^m} + c_{m-1}t^{p^{m-1}} + \cdots + c_0 t^{p^0} - a \text{ if } charR = p \neq 0 \end{cases}$$

where in the second case $c_i \in C_d$, $d(a) = 0$ *and* $d^{p^m} + c_{m-1}d^{p^{m-1}} + \cdots + c_0 d^{p^0}$ *is an inner derivation of* Q *adjoint to* a.

Proof. The main part of the proof of this proposition, based on Amitsur's idea ([1]), is a part of the proof of Lemma 1.7 from [4]. For completennes we present the sketch of the proof. Suppose that $Z(Q[t, d]) \neq C_d$ and let $f = \sum_{i=j}^{l} a_i t^i \in Z(Q[t, d])$ be a polynomial of minimal non-zero degree. For $j = 1, \ldots, l$ we put

$$f_j = \sum_{i=j}^{l} \binom{i}{j} a_i t^{i-j}.$$

It can be shown that all polynomials f_j's belong to $Z(Q[t, d])$. Thus, by the choice of f, $f_j = a_j \in C_d$ for $1 \leq j \leq l$ and

$$\binom{i}{j} a_i = 0 \text{ for } 1 \leq j < i \leq l.$$

The above enable us to write $f = a_l^{-1}z$ where $z \in Z(Q[t, d])$ is of the form described in the theorem. Therefore $C_d[z] \subset Z(Q[t, d])$ and z is a monic polynomial of minimal non-zero degree belonging to $Z(Q[t, d])$. Let $g \in Z(Q[t, d])$. If $\deg g < \deg z$ then $g \in C_d$. If $\deg g \geq \deg z$ then by dividing g by z we get $g = zh + r$ for some $h, r \in Q[t, d]$, $\deg r < \deg z$.

For any $q \in Q$ we have $0 = [g, q] = z[h, q] + [r, q]$ and $0 = [g, t] = z[h, t] + [r, t]$ where $[a, b]$ denotes the commutator of elements a, b. Therefore

$$z[h, q] = [q, r] \text{ for all } q \in Q, \text{ and}$$
$$z[h, t] = [t, r].$$

Because $\deg [t, r] \leq \deg r < \deg z$, the comparing of degrees of polynomials appearing in the above equalities yields $[h, q] = [q, r] = 0$ for all $q \in Q$ and $[h, t] = [t, r] = 0$. It means that $h, r \in Z(Q[t, d])$. Since degrees of these polynomials are smaller than $\deg g$, the induction hypothesis implies $h, r \in C_d[z]$, and, consequently, $g = th + r \in C_d[z]$. This shows that $Z(Q[t, d]) = C_d[z]$.

3. The extended centroid of R[t, ϕ]. As before ϕ denotes either an automorphism or a derivation of R. ϕ has a unique extension ϕ to $Q[t, \phi]$ such that t is a ϕ-invariant element. Next we can extend ϕ in a unique way to the central closure of $Q[t, \phi]$. The last extension will be also denoted by ϕ. Notice that every element $s \in C(Q[t, \phi])$ is ϕ-invariant, since $st = ts$.

In order to prove the main result some preparation is needed. Through the paragraph we fix $s \in C(Q[t, \phi])$. Let $I = |f \in R[t, \phi] \,|\, fs \in R[t, \phi]|$. Then I is a non-zero ideal of $R[t, \phi]$ and $\phi(I) \subset I$ since s is ϕ-invariant. Let n be the smallest natural number such that there exists $0 \neq f \in I$ with $\deg f = n$. We put $\mathcal{A} = |f \in I \,|\, \deg f \leq n|$ and $A = |a \in R \,|\, \text{there exist } a_{n-1}, \ldots, a_0 \in R \text{ such that } at^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathcal{A}|$. Using the definition of A it can be easily seen that A is a non-zero ideal of R and $\phi(A) \subset A$.

With the above notation we have the following

Lemma 3.1. *There exists a monic polynomial* $f_s = \sum_{i=0}^{n} q_i t^i \in Q[t, \phi]$ *such that* $\mathcal{A} = Af_s$. *The polynomial* f_s *has the following properties*:

1. *If* ϕ *is a derivation, then* $f_s \in Z(Q[t, \phi])$.

2. *If* ϕ *is an automorphism, then*:

a/ if $q_i \neq 0$ *for some* $0 \leq i \leq n-1$, *then* q_i *is invertible in* Q *and* $\phi^{i-m} = \sigma_{q_i}$.

b/ $\phi(q_i) = q_i$ *for* $0 \leq i \leq n$.

Proof. From the choice of n it follows that the maps α_i: $A \to R$ given by $\alpha_i(a) = a_i$, where $a = a_n$ and $\sum_{i=0}^{n} a_i t^i \in \mathcal{A}$, are well-defined

homomorphisms of left R-modules for all $0 \leq i \leq n$. Hence there exist elements $q_n = 1$, $q_{n-1}, \ldots, q_0 \in Q$ such that $a_i(a) = aq_i$ for every $a \in A$ and $0 \leq i \leq n$. Now it is enough to take $f_s = \sum_{i=0}^{n} q_i t^i \in Q[t, \phi]$.

1. Suppose that ϕ is a derivation. Let $a \in A$ and $b \in R$. Then both abf_s and $af_s b$ belong to $\mathcal{A}$. Since these polynomials have the same leading coefficient, they are equal. It means that $A(bf_s - f_s b) = 0$ for all $b \in R$. A is a non-zero ideal of R, so $bf_s = f_s b$ for all $b \in R$.

For any $a \in A$ polynomials $\phi(af_s) = \phi(a)f_s + a\phi(f_s)$ and $\phi(a)f_s$ are in $\mathcal{A}$, because $\phi(\mathcal{A}) \subset \mathcal{A}$ and $\phi(A) \subset A$. Hence $a\phi(f_s) \in \mathcal{A}$. However f_s is a monic polynomial and $\deg a\phi(f_s) < n$. The choice of n implies that $a\phi(f_s) = 0$ for every $a \in A$. Therefore $\phi(f_s) = 0$. It means that $\phi(q_i) = 0$ for all $0 \leq i \leq n$ and give us that f_s commutes with t.

Thus we have shown that f_s commutes with every element from $R[t, \phi]$. Now, the same argument as in Lemma 2.1.1 yields $f_s \in Z(Q[t, \phi])$.

2. Suppose that ϕ is an automorphism. Let $0 \leq i \leq n-1$ and $a \in A$, $b \in R$ be arbitrary. Since polynomials $a\phi^{n-i}(b)f_s$ and $af_s\phi^{-i}(b)$ belong to $\mathcal{A}$ and have the same leading coefficient, they are equal. Hence, in particular, we get $a\phi^{n-i}(b)q_i = aq_i b$. Therefore $A(\phi^{n-i}(b)q_i - q_i b) = 0$ for all $b \in R$, and, consequently, $\phi^{n-i}(b)q_i = q_i b$ for all $b \in R$. Now the statement a is a direct consequence of Lemma 1.2.

Let $a \in A$. Then $\phi(a)\phi(f_s) = \phi(af_s) \in \mathcal{A}$ is a polynomial with leading coefficient $\phi(a)$. It means that $\phi(A)(\phi(f_s) - f_s) = 0$. This shows that $\phi(f_s) = f_s$ and gives the property b.

Lemma 3.2. *Suppose that ϕ is an automorphism and $f = af_s \in \mathcal{A}$. Then there exists $T \in ZZ^{-1}$, where $Z = Z(Q[t, \phi])$, such that $f = at^n T$ in $Q[t, \phi]Z^{-1}$.*

Proof. Case 1. ϕ^k is not an inner automorphism of Q for all $k \geq 1$. In this case Lemma 3.1 yields directly that $f = at^n$.

Case 2. ϕ^k is an inner automorphism of Q for some $k \geq 1$. By Proposition 2.3 $Z = C_\varphi[bt^m]$, where m is the smallest natural number such that ϕ^m is an inner automorphism determined by a ϕ-invariant element $b \in Q$. Let $f_s = \sum_{i=0}^{n} q_i t^i$, $q_n = 1$, and $0 \leq i \leq n-1$. Suppose that $q_i \neq 0$. Then we know from Lemma 3.1 that $\phi^{i-n} = \sigma_{q_i}$ and $\phi(q_i) = q_i$. Therefore from the choice of m we get: m divides $i-n$ and $q_i = c_i b^{(i-n)/m}$ for some

$c_i \in C$, provided $q_i \neq 0$. Using the above we can write f in the following way: $f = af_s = a \sum_{0 \leq i \leq n, m \nmid (n-i)} q_i t^i = a(t^n + \sum_{0 \leq i < n, m \mid (n-i)} c_i b^{(i-n)/m} t^i) = at^n T$ where $T = 1 + \sum_{0 \leq i < n, m \mid n-i} c_i (bt^m)^{(i-n)/m}$ belongs to ZZ^{-1} since bt^m, $c_i \in Z$.

Now we are ready to prove the following

Theorem 3.3. *Suppose that ϕ is either a derivation or an automorphism of a prime ring R. Then the extended centroid of $R[t, \phi]$ is isomorphic to ZZ^{-1}, where Z is the center of $Q[t, \phi]$.*

Proof. Let S denote the extended centroid of $Q[t, \phi]$. By Lemma 2.1 it is enough to show that $S = ZZ^{-1}$. Obviously $ZZ^{-1} \subset S$.

Let $s \in S$ and $0 \neq f = af_s \in \mathcal{A}$ where $a \in A$. Let us take

$$l_\varphi = \begin{cases} 0 \text{ if } \phi \text{ is a derivation} \\ n = \deg f_s \text{ if } \phi \text{ is an automorphism.} \end{cases}$$

Depending whether the fact ϕ is a derivation or an automorphism we can use either Lemma 3.1. or Lemma 3.2, respectively, to find an element $T \in ZZ^{-1}$ such that $f = at^{l\varphi}T$. Thus $at^{l\varphi}Ts = fs \in R[t, \phi]$ for some $T \in ZZ^{-1}$. Because we intend to show that $s \in ZZ^{-1}$, it may be assumed, by replacing s by Ts, that

$$at^{l\varphi}s \in R[t, \phi] \text{ for some } 0 \neq a \in A.$$

Let $J = \{ b \in R \mid bt^{l\varphi}s \in R[t, \phi] \text{ and } \deg bt^{l\varphi}s \leqq k \}$ where $k = \deg at^{l\varphi}s$. It follows from the construction of J, that J is a non-zero ideal of R and for any $b \in J$ $bt^{l\varphi}s = \alpha_k(b)t^k + \cdots + \alpha_0(b)$ for some $\alpha_k(b), \ldots, \alpha_0(b) \in R$. The maps α_i: $J \to R$, for $0 \leq i \leq k$, are homomorphism of left R-modules and $\alpha_k \neq 0$. Hence there exist elements $a_k \neq 0$, $a_{k-1}, \ldots, a_0 \in Q$ such that $\alpha_i(b) = ba_i$ for all $b \in J$ and $0 \leq i \leq k$. Therefore the equality $J(t^{l\varphi}s - \sum_{i=0}^{k} a_i t^i) = 0$ holds in the central closure of $Q[t, \phi]$. Since J is a non-zero ideal of R, we get

$$t^{l\varphi}s = \sum_{i=0}^{k} a_i t^i \in Q[t, \phi] \text{ with } a_k \neq 0. \qquad (*)$$

In case when ϕ is a derivation $l_\varphi = 0$, and the above equality shows that $s \in Q[t, \phi] \cap S = Z$. This provides the proof of the theorem in this case.

Suppose now that ϕ is an automorphism.

Case 1. ϕ^i is not an inner automorphism of Q for all $i \geq 1$. Let $r \in R$. In virtue of identity $(*)$ we have

$$t^{l_\varphi} sr = (\sum_{i=0}^{k} a_i t^i) r = \sum_{i=0}^{k} a_i \phi^i(r) t^i \text{ and}$$

$$t^{l_\varphi} sr = \phi^{l_\varphi}(r) t^{l_\varphi} s = \sum_{i=0}^{k} \phi^{l_\varphi}(r) a_i t^i.$$

Therefore $a_i \phi^i(r) = \phi^{l_\varphi}(r) a_i$ for every $r \in R$ *and* $0 \leq i \leq k$. Because of our assumpion on ϕ, Lemma 1.2 implies that $k = l_\varphi$ since $a_k \neq 0$, and $a_i = 0$ for all $0 \leq i \leq k-1$. Thus $st^k = t^k s = a_k t^k$ for some $a_k \in Q$. The element t^k is regular in the central closure of $Q[t, \phi]$, so the last equality gives us $s = a_k \in S \cap Q \subset Z$.

Case 2. ϕ^l is an inner automorphism of Q for some $i \geq 1$. By Proposition 2.3 we can pick $l \geq l_\varphi$ and an element $b \in Q \backslash \{0\}$ such that $bt^l \in Z$. The fact that $t^{l_\varphi} s \in Q[t, \phi]$ gives us $(bt^l)s = (bt^{l-l_\varphi})(t^{l_\varphi} s) \in S \cap Q[t, \phi] = Z$. This shows that $s \in ZZ^{-1}$.

References

[1] S. A. Amitsur : Derivations in simple rings, Proc. London Math. Soc. 7(1957), 87−112.

[2] C. Cauchon : Les T-anneaux et les anneaux â identités polynomiales noethériness, thése, Orsay, 1977.

[3] I. N. Herstein : Rings with involution, Univ. Chicago Press, 1976.

[4] A. Leroy, J. Matczuk : Derivations et automorphismes algebraiques d'anneaux premiers, Comm. Algebra 13(6), 1985, 1245−1266.

[5] S. Montgomery, D. S. Passman : Outer Galois theory of prime rings, Rocky Mountain J. Math. 14(1984), 305−317.

[6] J. D. Rosen, M. P. Rosen : Extended centroids of skew polynomial rings, Canad. Math. Bull. 28(1), 1985, 67−76.

Institute of Mathematics
University of Warsaw
00−901 Warsaw, Pkin, Poland

(*Received October 31, 1986*)