PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 97(111) (2015), 181–186 DOI: 10.2298/PIM131217001A

CENTERS OF SKEW POLYNOMIAL RINGS

Waldo Arriagada and Hugo Ramírez

Abstract. We determine the center $\mathcal{C}(K[x;\delta])$ of the ring of skew polynomials $K[x;\delta]$, where K is a field and δ is a non-zero derivation over K. We prove that $\mathcal{C}(K[x;\delta]) = \ker\delta$, if δ is transcendental over K. On the contrary, if δ is algebraic over K, then $\mathcal{C}(K[x;\delta]) = (\ker\delta)[\eta(x)]$. The term $\eta(x)$ is the minimal polynomial of δ over K.

1. The ring of skew polynomials

Let K be a field and let δ be a non-zero *derivation* on K, cf. [**4, 13**]. That is, a linear function $\delta : K \to K$ such that $\delta(ab) = a\delta(b) + \delta(a)b$ for any $a, b \in K$. The ring of skew polynomials in x and coefficients in K is the set

$$K[x;\delta] = \Big\{ \sum_{i\in\mathbb{N}} x^i a_i : \{a_i\} \subset K \text{ has finite support} \Big\},$$

endowed with the usual equality, addition and equipped with multiplication rule: $ax = xa + \delta(a)$, $a \in K$. Since their formal introduction in the 1930's by Oystein Ore, skew polynomial rings and their iterated constructions have been further developed by N. Jacobson, S. A. Amitsur, P. M. Cohn, G. Cauchon, T. Y. Lam, A. Leroy, and J. Matczuk, and complete treatments can be found in the literature, cf. [**5, 9, 10**]. Computationally, such rings appear in the context of uncoupling and solving systems of linear differential and difference equations in closed form, cf. [**1, 3, 12**].

First, we notice that the multiplication rule and induction yield the relation:

$$ax^n = \sum_{k=0}^{n} \binom{n}{k} x^k \delta^{n-k}(a), \qquad a \in K,\ n \geqslant 1. \tag{1.1}$$

In addition, the following properties are satisfied in the ring $K[x;\delta]$, see [**2, 6, 8**].

(1) The function $\deg : K[x;\delta] \setminus \{0\} \to \mathbb{N}$ defined by $\deg(f) = \max\{i : a_i \neq 0\}$, where $f(x) = \sum_i x^i a_i \neq 0$, is a degree function satisfying

$$\deg(f \pm g) \leqslant \max\{\deg(f); \deg(g)\}$$

2010 *Mathematics Subject Classification:* 12E15, 12E10.
Key words and phrases: derivation, skew polynomial, center, ring, commutator.
Communicated by Žarko Mijajlović.

Further, $\deg(f \cdot g) = \deg(f) + \deg(g)$, for $f, g \in K[x;\delta] \setminus \{0\}$.

(2) $K[x;\delta]$ is an integral domain satisfying the right and left division algorithm. Hence, it is a principal right and left ideal domain.

(3) Consider the triple (A, a_0, σ), where A is a ring, $a_0 \in A$ and $\sigma : K \to A$ is a ring homomorphism. If

$$a_0\sigma(a) = \sigma(a)a_0 + \sigma(\delta(a)), \quad a \in K, \tag{1.2}$$

then there exists a unique $\bar{\sigma} : K[x;\delta] \to A$ with $\bar{\sigma}|_K = \sigma$ and $\bar{\sigma}(x) = a_0$. Further, when such a $\bar{\sigma}$ exists, $\bar{\sigma}(f(x)) = f^{\bar{\sigma}}(a_0)$, where $f^{\bar{\sigma}}(a_0) \in A$ is obtained via substitution of each coefficient of $f(x)$ by its image under $\bar{\sigma}$, and x by a_0.

Corollary 1.1. *The ring homomorphism $\sigma : K \to \mathrm{End}(K,+)$, $a \mapsto \sigma(a)$, where $\sigma(a) : b \mapsto ba$, extends as a unique $\bar{\sigma} : K[x;\delta] \to \mathrm{End}(K,+)$, where $\bar{\sigma}(x) = \delta$. Moreover, $\bar{\sigma}$ is K-linear when $\mathrm{End}(K,+)$ is considered as a right K-vector space via the action $f\lambda = f(\sigma(\lambda))$.*

Proof. To extend σ it suffices that identity (1.2) be fulfilled, with $a_0 = \delta$. But this is the case. Indeed, let $a \in K$; one has

$$[\sigma(a) \circ \delta + \sigma(\delta(a))](b) = \delta(b)a + b\delta(a) = \delta(ab) = (\delta \circ \sigma(a))(b), \quad b \in K.$$

The extension $\bar{\sigma}$ is K-linear since $\bar{\sigma}(f\lambda) = \bar{\sigma}(f) \circ \bar{\sigma}(\lambda) = \bar{\sigma}(f)(\sigma(\lambda)) = \bar{\sigma}(f)\lambda$. $\square$

Let $\bar{\sigma} : K[x;\delta] \to \mathrm{End}(K,+)$ be the linear homomorphism of Corollary 1.1 and

$$K[\delta] = \mathrm{Im}(\bar{\sigma}) = \left\{ \sum_{i=0}^{n} \delta^i a_i : n \in \mathbb{N}, ; a_i \in K \right\},$$

where $\delta^i a_i = \delta^i \circ \sigma(a_i)$. Then $K[\delta]$ is a subring of $\mathrm{End}(K,+)$ isomorphic to $K[x;\delta]$. It is, moreover, a right vector space over K.

Lemma 1.1 (Jacobson–Bourbaki). *Let $A \ni 1$ be a subring of $\mathrm{End}(K,+)$ such that:* (a) *A is a right vector subspace of $\mathrm{End}(K,+)$ over K,* (b) *$[A : K] = \nu$. Then $\mathbf{k} = \{a \in K : \sigma(a) \circ f = f \circ \sigma(a), \forall f \in A\}$ is a subfield of K such that $[K : \mathbf{k}] = \nu$. Further, $A = \mathrm{End}_{\mathbf{k}}(K,+)$ as a vector space over $\mathbf{k}$.*

The next result is a standard consequence of the division algorithm in $K[x;\delta]$, cf. [**9**].

Proposition 1.1. *Let $f(x) \in K[x;\delta]$ be of minimal degree $\deg(f)$, such that $f(\delta) = 0$. Then $[K[\delta] : K] = \deg(f)$. If $g \in K[x;\delta]$ satisfies $g(\delta) = 0$, then f divides g.*

2. Commutator

Let A be a ring. The commutator of $a, b \in A$ is $[a, b] = ab - ba$. It is easy to see that the commutator satisfies the following properties:

(4) $[\cdot,\cdot] : A \times A \to A$ is bi-additive.

(5) For every $a, b \in A$ the functions δ_a, $\delta_b : A \to A$ defined by $\delta_a = [a, \cdot]$ and $\delta_b = [\cdot, b]$ are derivations. They are called the internal derivations induced by a and b, respectively.

(6) Any ring homomorphism $\sigma : A \to B$ preserves the commutator, i.e.,

$$\sigma[a,b] = [\sigma(a), \sigma(b)], \quad a, b \in A.$$

In the sequel we will denote $\kappa = \ker \delta = \{a \in K : \delta(a) = 0\}$. (And hence, κ is a subfield of the field K.)

PROPOSITION 2.1. *In the ring $A = K[x;\delta]$ the following properties are fulfilled.*

(a) $[a, x^n] = \sum_{k=0}^{n-1} \binom{n}{k} x^k \delta^{n-k}(a)$, *for each $a \in K$ and $n \geqslant 1$. In particular, $[a, x] = \delta(a)$, and hence $[a, x^n] = 0$ for all $a \in \kappa$.*

(b) $[x^n a, x] = x^n [a, x]$ *for all $a \in K$ and $n \in \mathbb{N}$.*

(c) *The commutator $[\cdot,\cdot] : K[x;\delta] \times K[x;\delta] \to K[x;\delta]$ is κ-bilinear.*

PROOF. (a) This is a consequence of (1.1):

$$[a, x^n] = ax^n - x^n a = \sum_{k=0}^{n} \binom{n}{k} x^k \delta^{n-k}(a) - x^n a = \sum_{k=0}^{n-1} \binom{n}{k} x^k \delta^{n-k}(a).$$

(b) $[x^n a, x] = x^n ax - xx^n a = x^n ax - x^{n+1} a = x^n(ax - xa) = x^n[a, x]$.

(c) Let $f \in K[x;\delta]$ and let $\delta_f(\cdot) = [\cdot, f]$ be the internal derivation induced by f. Then for every $a, \lambda \in \kappa$ and any positive integer i,

$$[\lambda x^i a, f] = \delta_f(\lambda x^i a) = \delta_f(\lambda) x^i a + \lambda \delta_f(x^i a) = [\lambda, f] x^i a + \lambda [x^i a, f] = \lambda [x^i a, f],$$

since $[\lambda, f] = 0$. Indeed, if $f(x) = \sum_{i=0}^{n} x^i a_i$, then by (4),

$$\Big[\lambda, \sum x^i a_i\Big] = \sum \delta_\lambda(x^i a_i) = \sum \big(\delta_\lambda(x^i) a_i + x^i \delta_\lambda(a_i)\big) = \sum \big([\lambda, x^i] a_i + x^i [\lambda, a_i]\big),$$

and this last quantity vanishes by (a). Hence, $[\cdot, f]$ is homogeneous on monomials $x^i a_i$ and by additivity it is homogeneous on polynomials. We prove in an analogous way that $[f, \cdot]$ is homogeneous on polynomials. □

COROLLARY 2.1. *Let $f(x) = \sum_{i=0}^{n} x^i a_i \in K[x;\delta]$ and $a \in K$. Then*

(a) $[f(x), x] = \sum_{i=0}^{n} x^i \delta(a_i)$,

(b) $[a, f(x)] = \sum_{i=1}^{n} \sum_{k=0}^{i-1} \binom{i}{k} x^k \delta^{i-k}(a) a_i$.

PROOF. (a) $[\sum x^i a_i, x] = \sum x^i [a_i, x] = \sum x^i \delta(a_i)$.

(b) Since the commutator is bi-additive, we have

$$\begin{aligned}[a, f(x)] = [a, a_0 + xa_1 + \cdots + x^n a_n] &= [a, a_0] + [a, xa_1] + \cdots + [a, x^n a_n] \\ &= [a, x] a_1 + \cdots + [a, x^n] a_n.\end{aligned}$$

The conclusion follows from Proposition 2.1(a). □

3. Results

The *center* of a ring A is the subring $\mathcal{C}(A) = \{a \in A : [a, b] = 0, \ \forall b \in A\}$. The elements of $\mathcal{C}(A)$ are called *central*.

LEMMA 3.1. *Let $a, b \in \mathcal{C}(A)$ with b cancelable. If $c \in A$ such that $a = bc$, then c is also central.*

PROOF. For any $\alpha \in A$, $0 = \alpha a - a\alpha = \alpha bc - bc\alpha = b(\alpha c - c\alpha)$. □

The next lemma is a useful result that follows from Kummer's theorem [**7**].

Lemma 3.2. [**11**] *Let j be a nonzero natural number and p a prime number. Assume that $j = j_0 + j_1 p + \cdots + j_r p^r$ ($j_r \neq 0$) is the p-adic decomposition of j. If $\binom{j}{k} = 0 \pmod p$ for all $k = 1, \ldots, j-1$ then $j_0 = \cdots = j_{r-1} = 0$, $j_r = 1$. That is, $j = p^r$.*

The next theorem is the core result of the paper.

Theorem 3.1. *If the derivation δ is transcendental over K, then $\mathcal{C}(K[x;\delta]) = \kappa$. On the contrary, if δ is algebraic over K, then there exist a positive integer N and a prime p such that $\mathrm{ch}(K) = p$ (where ch(K) is the characteristics of K) and the center $\mathcal{C}(K[x;\delta]) = \kappa[\eta(x)]$, where*

$$\eta(x) = x\alpha_1 + x^{p^2}\alpha_2 + \cdots + x^{p^N} \quad \alpha_i \in \ker\delta,$$

is the minimal polynomial of δ over K. In this case we have also $[K : \kappa] = p^N$.

Proof. Let us assume that $f(x) = \sum_{i=0}^{m} x^i b_i \in K[x;\delta]$, with $b_m \neq 0$ and $m = \deg(f) \geqslant 1$. Then $f(x)$ is central if and only if $f(x)$ commutes with x and with every $a \in K$. That is, $[f(x), x] = [a, f(x)] = 0$. By Corollary 2.1, these conditions are simultaneously equivalent to $b_i \in \kappa$ for $i = 0, \ldots, m$ and

$$\delta(a)b_1 + \cdots + \sum_{k=0}^{i-1}\binom{i}{k}x^k\delta^{i-k}(a)b_i + \cdots + \sum_{k=0}^{m-1}\binom{m}{k}x^k\delta^{m-k}(a)b_m = 0, \tag{3.1}$$

for every $a \in K$. Hence, if δ is transcendental over K, the coefficients b_i, $i = 1, \ldots, m$ vanish and $f(x) = b_0 \in \kappa$, which proves the first statement of the theorem.

Let us suppose that δ is algebraic over K. Since (3.1) is a null polynomial, the coefficient of the power x^{i-1} is zero. That is:

$$\delta\binom{i}{i-1}b_i + \delta^2\binom{i+1}{i-1}b_{i+1} + \cdots + \delta^{m-i+1}\binom{m}{i-1}b_m = 0, \quad i = 1, \ldots, m.$$

In particular, $\delta b_1 + \delta^2 b_2 + \cdots + \delta^m b_m = 0$ for $i = 1$, and $\delta m b_m = 0$ for $i = m$. Since $\delta \neq 0$, $\delta m b_m = 0 \Rightarrow m b_m = 0 \Leftrightarrow (m \cdot 1_K)b_m = 0$, where 1_K is the multiplicative unit of K. Hence, $m \cdot 1_K = 0$ and then there exists a prime number p such that $\mathrm{ch}(K) = p$. (In particular, ch(K) is nonzero). Further, if we define $g(x) = f(x) - f(0)$, then $g(x)$ is central and $g(\delta) = 0$. Hence, there exists a monic polynomial $\eta(x) \in K[x;\delta]$ with $\eta(0) = 0$ and of minimal degree $\deg(\eta) = n \geqslant 1$, such that $\eta(\delta) = 0$. Write

$$\eta(x) = \sum_{i=1}^{n} x^i a_i, \tag{3.2}$$

with $a_n = 1$. Inasmuch as $\delta(1) = 0$, by Corollary 2.1(a) the bracket

$$[\eta(x), x] = \sum_{i=1}^{n-1} x^i \delta(a_i)$$

has a lower degree than $\eta(x)$. Consider the homomorphism $\bar{\sigma}$ of Corollary 1.1. We have $\bar{\sigma}[\eta(x), x] = [\bar{\sigma}(\eta(x)), \bar{\sigma}(x)] = [\eta(\delta), \delta] = [0, \delta] = 0$. Hence, $[\eta(x), x] = 0$. Similarly, for every $a \in K$ and by Corollary 2.1(b), the commutator $[a, \eta(x)]$ has a lower degree than $\eta(x)$. Also, $\bar{\sigma}[a, \eta(x)] = [\bar{\sigma}(a), \bar{\sigma}(\eta(x))] = [\sigma(a), \eta(\delta)] = [\sigma(a), 0] = 0$. Hence, $[a, \eta(x)] = 0$, for every $a \in K$. Thus, η is central. On the other hand, we notice that an element $a \in K$ is central if and only if $a \in \kappa$. (Indeed, $[a, q(x)] = 0$ if and only if $\delta(a) = 0$, for $q \in K[x; \delta]$). Hence, $\kappa[\eta(x)] \subset \mathcal{C}(K[x; \delta])$.

Conversely, we prove by induction on the degree of $f(x)$ that if $f(x)$ is central, with $\deg(f) \geqslant 1$, then there exists $g \in \kappa[x]$ such that $f(x) = g(\eta(x))$. Indeed, f central $\Rightarrow f(\delta) - f(0) = 0 \Rightarrow \eta(x)$ divides $f(x) - f(0) \Leftrightarrow f(x) - f(0) = \eta(x) f_1(x)$. By Lemma 3.1, f_1 is central. If $f_1(x) \in \kappa$, then the polynomial $g(x) = f(0) + f_1(x) \in \kappa[x]$ satisfies $f(x) = g(\eta(x))$. By minimality, if $\deg(f_1) \geqslant 1$, and since $\deg(f_1) < \deg(f)$, we have $f_1(x) = g_1(\eta(x))$ where $g_1 \in \kappa[x]$. This means $f(x) = f(0) + \eta(x) g_1(\eta(x))$. Hence if $g(x) = f(0) + x g_1(x) \in \kappa[x]$, we have $f(x) = g(\eta(x))$. This proves that $\mathcal{C}(\kappa[x; \delta]) = \kappa[\eta(x)]$.

Now, let us determine the explicit form of the minimal polynomial (3.2). Since $\eta(x)$ is central its coefficients satisfy $\delta\binom{i}{i-1}a_i + \delta^2\binom{i+1}{i-1}a_{i+1} + \cdots + \delta^{n-i+1}\binom{n}{i-1} = 0$, for $i = 1, \ldots, n$. That is, δ is root of the polynomials

$$f_i(x) = x\binom{i}{i-1}a_i + x^2\binom{i+1}{i-1}a_{i+1} + \cdots + x^{n-i+1}\binom{n}{i-1},$$

for $i = 1, \ldots, n$. Notice that if $i \geqslant 2$ then $1 \leqslant \deg(f_i) \leqslant n - 1$. Then by minimality, the coefficients of f_i, with $2 \leqslant i \leqslant n$, vanish identically. These coefficients can be arranged in rows:

$$\begin{array}{cccccccc}
\binom{2}{1}a_2 & \binom{3}{1}a_3 & \cdots & \binom{j}{1}a_j & \cdots & \binom{n}{1}, & & i=2 \\
 & \binom{3}{2}a_3 & \cdots & \binom{j}{2}a_j & \cdots & \binom{n}{2}, & & i=3 \\
 & & \ddots & \vdots & & \vdots & & \vdots \\
 & & & \binom{j}{j-1}a_j & \cdots & \binom{n}{j-1}, & & i=j \\
 & & & & \ddots & \vdots & & \vdots \\
 & & & & & \binom{n}{n-1}, & & i=n.
\end{array}$$

Thus if $a_j \neq 0$, for $2 \leqslant j \leqslant n$, then $\binom{j}{k} \cdot 1_K = 0$ for all $k = 1, \ldots, j-1$. Hence,

$$\binom{j}{1} = \binom{j}{2} = \cdots = \binom{j}{j-1} = 0 \pmod{p}.$$

By Lemma 3.2, there exists a positive integer r_j such that $j = p^{r_j}$. Let us denote $N = r_n$. For $l = 2, \ldots, N$ define coefficients

$$\alpha_l = \begin{cases} a_i & \text{if } l = r_i \text{ for some } i, \\ 0 & \text{otherwise.} \end{cases}$$

Then the minimal polynomial has the required form $\eta(x) = x\alpha_1 + x^{p^2}\alpha_2 + \cdots + x^{p^N}$, where $\alpha_1 = a_1$ and $\alpha_i \in \ker(\delta)$.

Finally, we know that $K[\delta]$ is a subring of $\mathrm{End}(K, +)$. It is moreover a right vector subspace of $\mathrm{End}(K, +)$ over K. By Proposition 1.1, $[K[\delta] : K] = \deg(\eta) = p^N$.

Further,

$$\{a \in K : \sigma(a) \circ A = A \circ \sigma(a),\ A \in K[\delta]\} = \{a \in K : \sigma(a) \circ \delta = \delta \circ \sigma(a)\} = \ker \delta = \kappa.$$

By Lemma 1.1, $[K : \kappa] = p^N$ and $K[\delta] = \mathrm{End}_\kappa(K, +)$. The proof is complete. $\square$

Acknowledgments. The authors are grateful to an unknown referee, who provided helpful suggestions and comments.

References

1. W. Arriagada, *Characterization of the generic unfolding of a weak focus*, J. Differ. Equations **253** (2012), 1692–1708.
2. P. Cohn, *Skew Fields. Theory of General Division Rings*, Academic Press, London (1985).
3. D. Yu. Grigoriev, *Complexity of factoring and calculating gcd of linear differential operators*, J. Symb. Comput. **10** (1990), 7–37.
4. N. Hamaguchi, A. Nakajima, *Derivations of skew polynomial rings*, Publ. Inst. Math., Nouv. Sér. **72(86)** (2002), 107–112.
5. N. Jacobson, *The Theory of Rings*, American Mathematical Society, New York, 1943.
6. A. V. Jategaonkar, *Skew polynomial rings over semisimple rings*, J. Algebra **19** (1971), 315–328.
7. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.
8. T. Y. Lam, *A First Course in Noncommutative Rings*, Grad. Texts Math., Springer-Verlag, Berlin–Heidelberg–New York, 1991.
9. A. Leroy, *Introduction to Noncommutative Polynomial Maps*, Univ. d'Artois, Faculté Jean Perrin, Notes online (Dec. 2011).
10. B. McDonald, *Finite Rings With Identity*, Marcel Dekker, New York, 1974.
11. D. Miheţ, *Legendre's and Kummer's theorems again*, Resonance **15**(2) (Dec. 2010), 1111–1121.
12. M. F. Singer, *Testing reducibility of linear differential operators: A group theoretic perspective*, Appl. Algebra Eng. Commun. Comput. **7**(2) (1996), 77–104.
13. M. G. Voskoglou, *Derivations and iterated skew polynomial rings*, Int. J. Appl. Math. Inform. **2**(5) (2011), 82–90.

Department of Applied Mathematics and Sciences
Khalifa University
Al Zafranah, P.O. Box 127788
Abu Dhabi
United Arab Emirates
waldo.arriagada@kustar.ac.ae

(Received 23 07 2012)
(Revised 28 08 2013)

Instituto de Ciencias Físicas y Matemáticas
Universidad Austral de Chile
Casilla 567, Valdivia
Chile
hramirez@uach.cl