A note on involutions in Ore extensions

Una nota sobre involuciones en extensiones de Ore

Waldo Arriagada[1,a], **Hugo Ramírez**[2,b]

Abstract. Skew-polynomial rings, or Ore extensions, constitute an important class in noncommutative ring theory. These structures are currently studied from different points of view such as ideal theory, order theory, Galois theory, homological algebras, etc. Computationally, Ore extensions appear in the context of uncoupling and solving systems of linear differential and difference equations in closed form. In this short note we let K denote a division ring, $\alpha : K \to K$ a ring endomorphism and $\delta : K \to K$ an α-derivation. We determine the involutions in the Ore extension $K[x;\alpha,\delta]$.

Keywords: Skew polynomials, involution, ring endomorphism, derivation.

Resumen. Los anillos de polinomios torcidos, o extensiones de Ore, forman una clase importante en la teoría de anillos noconmutativos. Tales estructuras son actualmente estudiadas desde diversos puntos de vista en matemáticas tales como la teoría de ideales en álgebra, la teoría del orden, la teoría de Galois, el álgebra homológica, etc. En aplicaciones, las extensiones de Ore aparecen en el desacoplamiento y posterior solución explícita de algunos sistemas de ecuaciones diferenciales lineales y en diferencias. En esta nota consideramos un cuerpo no conmutativo (o anillo de división) K, un endomorfismo de anillos $\alpha : K \to K$ y una α-derivación $\delta : K \to K$. Luego se determinan y caracterizan las involuciones en la extensión de Ore $K[x;\alpha,\delta]$.

Palabras claves: polinomios torcidos, involución, endomorfismo de anillos, derivación.

Mathematics Subject Classification: 16U20, 16U80, 16U30.

Recibido: septiembre de 2016 Aceptado: marzo de 2017

1. Ore extensions

Non-commutative polynomial rings were first introduced by Oystein Ore in 1933. Since the publication of his fundamental paper [8] Ore's extensions or *skew polynomial rings* have played an important role in non-commutative ring

[1] Department of Applied Mathematics and Sciences, Khalifa University, Abu Dhabi, United Arab Emirates

[2] Instituto de Ciencias Físicas y Matemáticas, Universidad Austral de Chile, Valdivia, Chile

[a] waldo.arriagada@kustar.ac.ae

[b] hramirez@uach.cl

theory. Great progress has been achieved and Ore extensions are studied from different points of view such as ideal theory, order theory, Galois theory, homological algebras, etc. Computationally, such rings appear in the context of uncoupling and solving systems of linear differential and difference equations in closed form [2, 9].

The formal definition of a skew polynomial ring is as follows. Let K be a ring with unit 1 and α a ring endomorphism of K. An additive map $\delta \in End(K, +)$ is called an α-derivation if

$$\delta(ab) = \delta(a)\alpha(b) + a\delta(b)$$

for any a, $b \in K$ [3, 10]. The Ore extension or skew polynomial ring in x and coefficients in K is the set

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

endowed with the usual equality, addition and equipped with multiplication rule:

$$ax = x\alpha(a) + \delta(a), \quad a \in K. \tag{1}$$

In the particular case $\alpha = id$ (the identity monomorphism) and $\delta = 0$ the ring of skew polynomials reduces to $K[x]$ which is the usual polynomial ring in a commutative variable. If $\alpha = id$ and $\delta \neq 0$ the skew polynomial ring is denoted by $K[x;\delta]$ and is called a *polynomial ring of derivation type.* If $\alpha \neq id$ but $\delta = 0$ the skew polynomial ring is denoted by $K[x;\alpha]$ and is called a *polynomial ring of endomorphism type.* For example, the *center* of polynomial rings of derivation type has been identified in the recent paper [1]. On the contrary, the characterization of centers of polynomial rings of endomorphism type is still an open problem.

The *degree* of a nonzero polynomial $f(x) = \sum_i x^i a_i \in K[x;\alpha,\delta]$ is defined to be

$$\deg f(x) = \max\{i : a_i \neq 0\}.$$

As usual, $\deg(0) = -\infty$. It is not hard to prove using the formula (1) that the degree function satisfies the three relations

(a) $\deg(f \pm g) \leq \max\{\deg f, \deg g\}$,

(b) $\deg(f \cdot g) = \deg f + \deg g$,

(c) $\deg(f \circ g) = \deg f \cdot \deg g$,

for $f, g \in K[x;\alpha,\delta]$. Ore used these properties to establish the unique factorization property when the coefficients belong to a division ring. Iterated constructions have been further developed by S.A. Amitsur, P.M. Cohn, G. Cauchon, A. Leroy and J. Matczuk. Complete treatments can be found in the literature [4, 6, 7].

Example 1.1. The next standard examples have been taken from [6].

(1) The ring $\mathbb{C}[z;\alpha]$ of skew polynomials in the complex coordinate z is a polynomial ring of endomorphism type, where α is the usual complex conjugation $z \mapsto \overline{z}$.

(2) Let κ be a field. The Weyl algebra is the polynomial ring of derivation type $\kappa[t][x;\delta]$, where δ is the usual derivative d/dt. This algebra corresponds to the ring of differential operators with polynomial coefficients in one variable

$$x^n f_n(t) + x^{n-1} f_{n-1}(t) + \cdots + x f_1(t) + f_0(t)$$

with $f_i(t) \in \kappa[t]$ for each $i = 0, \ldots, n$. Notice that $xt - tx = 1$.

(3) Let $a \in K$ and define the inner α-derivation δ_a induced by a via

$$\delta_a(b) = ab - \alpha(b)a.$$

Then the skew polynomial ring $K[x;\alpha,\delta_a] = K[x-a;\alpha]$ corresponds to the polynomial ring of endomorphism type in the variable $x - a$.

2. Anti-automorphisms and involutions

In the sequel, we let $K[x;\alpha,\delta]$ be a skew polynomial ring over a division ring K. We will use the notations $e_0 = \alpha$ and $e_1 = \delta$. For any given nonnegative integer n and any given collection $i_1, \ldots, i_n \in \{0,1\}$ we denote by

$$e_{i_1 \ldots i_n} = e_{i_1} \circ \cdots \circ e_{i_n}$$

the composite endomorphism. Let us choose $a \in K$. It is easy to check (via a simple inductive argument) that

$$ax^n = \sum_{k=0}^{n} \sum_{\substack{i_1+\cdots+i_n=n-k \\ i_j \in \{0,1\}}} x^k \; e_{i_1 \cdots i_n}(a). \tag{2}$$

Let A, A' be two rings. An *anti-homomorphism* from A onto A' is a surjection $J : A \to A'$ such that

$$J(a+b) = J(a) + J(b), \quad J(ab) = J(b)J(a)$$

for all $a, b \in A$. If J is moreover injective then it is called an *anti-isomorphism* and A, A' are then *anti-isomorphic*. If, in addition, $A = A'$ the map J is called and *anti-automorphism*. If the square (second iterate) of an anti-automorphism J is the identity then J is called an *involutive anti-automorphism* or simply an *involution*.

In the sequel, an element $f(x) = a_0 + xa_1 + \cdots + x^n a_n \in K[x;\alpha,\delta]$ will be denoted by $f(x) = x^i a_i$. (The summation is replaced by the repeated index i).

Proposition 2.1. *Consider the triple $(A, \mathfrak{x}, \sigma)$, where A is a ring, $\mathfrak{x} \in A$ and $\sigma : K \to A$ is a ring anti-homomorphism. If the relation*

$$\mathfrak{x}\sigma(a) = \sigma\alpha(a)\mathfrak{x} + \sigma\delta(a) \tag{3}$$

is satisfied by σ for all $a \in K$ then there exists a unique ring anti-homomorphism $\overline{\sigma} : K[x; \alpha, \delta] \to A$ such that $\overline{\sigma}|_K = \sigma$ and $\overline{\sigma}(x) = \mathfrak{x}$.

Proof. Let $f(x) = x^i a_i$ be an element in $K[x; \alpha, \delta]$. We define

$$\overline{\sigma} : f(x) \mapsto f^{\sigma}(\mathfrak{x}) \tag{4}$$

where $f^{\sigma}(\mathfrak{x}) = \sigma(a_i)\mathfrak{x}^i$ and $\sigma(a_i) \in A$. It is clear that $f(x) \mapsto f^{\sigma}(\mathfrak{x})$ defines a single valued mapping from $K[x; \alpha, \delta]$ onto A. If $g(x) = x^i b_i$ then $f(x)+g(x) = x^i(a_i + b_i)$ and the image of this element is

$$\sigma(a_i + b_i)\mathfrak{x}^i = (\sigma(a_i) + \sigma(b_i))\mathfrak{x}^i = \sigma(a_i)\mathfrak{x}^i + \sigma(b_i)\mathfrak{x}^i.$$

Likewise, let $a, b \in K$ and choose a pair s, ℓ of sufficiently large nonnegative integers. Successive iterations of the formula (3) yield

$$\mathfrak{x}^s\sigma(b) = \mathfrak{x}^{s-j}\Big\{\sigma\alpha^j(b)\mathfrak{x}^j + \sum_{k=0}^{j-1} \sum_{\substack{i_1+\cdots+i_j=j-k \\ i_r\in\{0,1\}}} \sigma(e_{i_1\ldots i_j})(b)\mathfrak{x}^k\Big\}, \quad j \leq s.$$

Evaluating the latter relation at $j = s$ and multiplying (on the left) by $\sigma(a)$ and (on the right) by $\mathfrak{x}^{\ell}$ yields $\sigma(a)\mathfrak{x}^s\sigma(b)\mathfrak{x}^{\ell} = \overline{\sigma}(x^{\ell}bx^s a)$ and hence $\overline{\sigma}(x^s a)\overline{\sigma}(x^{\ell}b) = \overline{\sigma}(x^{\ell}bx^s a)$. Further, a simple inductive argument proves that if $f(x), g(x)$ are two skew polynomials then we have the equivalence $\overline{\sigma}(f(x))\overline{\sigma}(g(x)) = \overline{\sigma}(g(x)f(x))$. Hence, the map (4) is an anti-homomorphism. Clearly $\overline{\sigma}|_K = \sigma$ and $\overline{\sigma}(x) = \mathfrak{x}$.

Let η be any anti-homomorphism of $K[x; \alpha, \delta]$ onto A which maps x into $\mathfrak{x}$ and which coincides with σ on K. Then $\eta(x^i a_i) = \eta(a_i)\mathfrak{x}^i = \sigma(a_i)\mathfrak{x}^i$. Hence η coincides with the map $\overline{\sigma}$ and the extension is unique. □

In the sequel we denote by K^* the division ring deprived of the zero element.

Theorem 2.2. *The anti-automorphisms J of $K[x; \alpha; \delta]$ are given by*

$$J(x^i a_i) = \sigma(a_i)(x\mathfrak{a}_{\circ} + \mathfrak{b}_{\circ})^i, \tag{5}$$

where $(\mathfrak{a}_{\circ}, \mathfrak{b}_{\circ}) \in K^* \times K$ and $\sigma = J|_K$ is an anti-automorphism of K which satisfies,

i. $\alpha\sigma\alpha(a)\mathfrak{a}_{\circ} = \mathfrak{a}_{\circ}\sigma(a)$ *for every* $a \in K$;

ii. $\mathfrak{b}_{\circ}\sigma(a) = \delta\sigma\alpha(a)\mathfrak{a}_{\circ} + \sigma\alpha(a)\mathfrak{b}_{\circ} + \sigma\delta(a)$ *for every* $a \in K$.

Further, if the identities

iii. $\sigma^2 = id|_K, \quad \alpha\sigma(\mathfrak{a}_{\circ})\mathfrak{a}_{\circ} = 1 \quad$ *and* $\quad \delta\sigma(\mathfrak{a}_{\circ})\mathfrak{a}_{\circ} + \sigma(\mathfrak{a}_{\circ})\mathfrak{b}_{\circ} + \sigma(\mathfrak{b}_{\circ}) = 0$

are fulfilled then J is an involution.

Proof. Let J be an anti-automorphism of the Ore extension $K[x;\alpha;\delta]$. The degree function $\deg(\cdot)$ permits to prove that the image of $\sigma = J|_K$ is all of K (and hence $\sigma : K \to K$ is an automorphism). Moreover, as $\deg(J \circ J)(x) = (\deg J(x))^2 = \deg x = 1$ we have $\deg J(x) = 1$. Hence, there exist $(\mathfrak{a}_{\circ}, \mathfrak{b}_{\circ}) \in K^* \times K$ such that

$$J(x) = x\mathfrak{a}_{\circ} + \mathfrak{b}_{\circ}. \tag{6}$$

On the other hand, applying the automorphism J on both sides of (1) yields

$$J(x)\sigma(a) = \sigma\alpha(a)J(x) + \sigma\delta(a). \tag{7}$$

Plugging the polynomial (6) into the latter equivalence yields (i) and (ii). The condition (iii) is equivalent to $J \circ J = id$.

Conversely, let $(\mathfrak{a}_{\circ}, \mathfrak{b}_{\circ}) \in K^* \times K$ and let $\sigma : K \to K$ be an anti-automorphism satisfying (i) and (ii). If we define $J(x) = x\mathfrak{a}_{\circ} + \mathfrak{b}_{\circ}$ then the relation (7) is verified for every $a \in K$. By Proposition 2.1 there exists an anti-homomorphism of the Ore extension $K[x;\alpha;\delta]$, denoted by J again, which extends σ, i.e $\sigma = J|_K$. By unicity J is given by the formula (5). Such an anti-homomorphism is clearly injective. Inasmuch as

$$J(\sigma^{-1}(a_i)\{\sigma^{-1}(\mathfrak{a}_{\circ}{}^{-1})x - \sigma^{-1}(\mathfrak{b}_{\circ}\mathfrak{a}_{\circ}{}^{-1})\}) = f(x)$$

for any given element $f(x) = x^i a_i \in K[x;\alpha,\delta]$, the anti-homomorphism is also surjective. The proof is complete. □

In the particular case $\delta = 0$ we obtain the following result.

Corollary 2.3. *Let us assume that α is not an inner automorphism of K. Then the involutions J of the polynomial ring of endomorphism type $K[x;\alpha]$ are given by*

$$J(x^i a_i) = \sigma(a_i)(x\mathfrak{a}_{\circ})^i$$

where $\mathfrak{a}_{\circ} \in K^*$ and $\sigma = J|_K$ is an involution of K such that $\alpha\sigma(\mathfrak{a}_{\circ})\mathfrak{a}_{\circ} = 1$ and $\alpha\sigma\alpha\sigma^{-1} = \overline{\mathfrak{a}_{\circ}}$. The term $\overline{\mathfrak{a}_{\circ}}$ is the inner automorphism $a \mapsto \mathfrak{a}_{\circ}a\mathfrak{a}_{\circ}{}^{-1}$.

Proof. By Theorem 2.2 the automorphisms of $K[x;\alpha]$ are given by the formula (5) with $(\mathfrak{a}_{\circ}, \mathfrak{b}_{\circ}) \in K^* \times K$ and where σ is an anti-automorphism of K which satisfies

(i)* $\alpha\sigma\alpha(a)\mathfrak{a}_{\circ} = \mathfrak{a}_{\circ}\sigma(a)$ for every $a \in K$;

(ii)* $\mathfrak{b}_{\circ}\sigma(a) = \sigma\alpha(a)\mathfrak{b}_{\circ}$ for every $a \in K$.

By (i)* $\alpha\sigma\alpha(a) = \mathfrak{a}_{\circ}\sigma(a)\mathfrak{a}_{\circ}{}^{-1} = \overline{\mathfrak{a}_{\circ}}\sigma(a)$ for every $a \in K$. Hence, $\alpha\sigma\alpha\sigma^{-1} = \overline{\mathfrak{a}_{\circ}}$. On the other hand, if $\mathfrak{b}_{\circ} \neq 0$ we have by (ii)*, $\sigma\alpha(a) = \mathfrak{b}_{\circ}\sigma(a)\mathfrak{b}_{\circ}{}^{-1} = \overline{\mathfrak{b}_{\circ}}\sigma(a)$ for $a \in K$. Therefore, $\sigma\alpha\sigma^{-1} = \overline{\mathfrak{b}_{\circ}}$. Combining both relations yields $\alpha\overline{\mathfrak{b}_{\circ}} = \overline{\mathfrak{a}_{\circ}}$

and hence $\alpha = \overline{\mathfrak{a}_\circ \mathfrak{b}_\circ{}^{-1}}$. This is a contradiction, since we have assumed that α is not an inner automorphism. Therefore $\mathfrak{b}_\circ = 0$.

Using the condition (iii) we see that J is moreover an involution if σ is an involution of K and $\alpha\sigma(\mathfrak{a}_\circ)\mathfrak{a}_\circ = 1$. □

Corollary 2.4. *Let us assume that K is a commutative ring and α is not an inner automorphism of K. Then the involutions J of $K[x;\alpha]$ are given by*

$$J(x^i a_i) = \sigma(a_i)(x\mathfrak{a}_\circ)^i$$

where $\mathfrak{a}_\circ \in K^*$ and σ is an involution of K which satisfies $\sigma\alpha(\mathfrak{a}_\circ)\mathfrak{a}_\circ = 1$ and $\alpha\sigma\alpha = \sigma$.

3. An example

Let n be a positive integer and p and odd prime number. Let us take K to be the splitting field of the polynomial $x^{p^n} - 1$ on the rational numbers $\mathbb{Q}$.

Lemma 3.1 (Theorem 3 of [5] pp. 96)**.** *The Galois group $G(K/\mathbb{Q})$ of the cyclotomic field $K/\mathbb{Q}$ of order p^n is isomorphic to a subgroup of the multiplicative group $U(\mathbb{Z}_{p^n}, +, \cdot\,)$ of units in $\mathbb{Z}_{p^n}$. Moreover, $G(K/\mathbb{Q})$ is cyclic of order an even number.*

Let us choose $\alpha \in G(K/\mathbb{Q})$ with order $|\alpha|$ equal to two. If we take $\sigma = \alpha$ then only $\mathfrak{a}_\circ = \pm 1$ verifies the conditions of the Corollary 2.4. Therefore, σ extends to two involutions J_1, J_2 on $K[x;\alpha]$ which are given by

$$J_1(x^i a_i) = \sigma(a_i)x^i \quad \text{and} \quad J_2(x^i a_i) = (-1)^i \sigma(a_i)x^i.$$

Acknowledgements

We are particularly grateful to Biblioteca Sotero Prieto (UNAM) for kindly providing us with useful references.

References

[1] W. Arriagada and H. Ramírez, *Centers of skew polynomial rings*, Publications de l'Institut Mathématique de Beograde **97** (2015), no. 111, 181–186.

[2] D. Y. Grigoriev, *Complexity of factoring and calculating gcd of linear differential operators*, J. Symb. Comp. **10** (1990), 7–37.

[3] N. Hamaguchi and A. Nakajima, *Derivations of skew polynomial rings*, Publications de l'Institut Mathématique **72** (2002), no. 86, 107–112.

[4] N. Jacobson, *The theory of rings*, Amer. Math. Soc., New York, 1943.

[5] ______, *Lectures in Abstract Algebra Vol. III: Theory of fields and Galois theory*, Van Nostrand, 1964.

[6] A. Leroy, *Introduction to noncommutative polynomial maps*, Université d'Artois, Faculté Jean Perrin, Notes online, Dec., 2011.

[7] B. McDonald, *Finite rings with identity*, Marcel Dekker Inc., New York, 1974.

[8] O. Ore, *Theory of non-commutative polynomials*, Annals of Math. **34** (1933), 480–508.

[9] M. F. Singer, *Testing reducibility of linear differential operators: A group theoretic perspective*, Applicable Algebra in Engineering, Communication and Computing **7** (1996), no. 2, 77–104.

[10] M. G. Voskoglou, *Derivations and iterated skew polynomial rings*, International Journal of Applied Mathematics And Informatics **2** (2001), no. 5, 82–90.