ITERATED ORE POLYNOMIAL MAPS

ANDRÉ LEROY AND MEHRDAD NASERNEJAD

Abstract. We study a natural notion of polynomial maps attached to elements of an iterated Ore extension $A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$. We develop some tools to analyze these maps such as good points, multilinear transformations, and P-independence. We also present polynomial maps arising in the Multivariate extensions $A[\underline{t};\sigma,\underline{\delta}]$, introduced by U. Martínez-Peñas and F. R. Kschischang [12], through the use of Multilinear polynomial maps.

1. Introduction and preliminaries

Polynomial maps are at the core of many areas in mathematics. For polynomials with coefficients in a commutative ring, the evaluation is multiplicative, that is, the evaluation of a product of polynomials is the product of their evaluations. In the case of polynomials with coefficients in a noncommutative ring, it is necessary to define the left and right evaluations and, moreover, these evaluations are no longer multiplicative. This is a serious obstacle to a smooth development of polynomial maps in a noncommutative settings. The case of polynomials in one variable with coefficients in a division ring is manageable thanks to a nice formula for the evaluation of a product. In a series of papers (see [8], [6], [9]) the case of the evaluation of skew (Ore) polynomials in one variable with coefficients in a division ring was studied. In these papers, an important tool is the notion of pseudo-linear transformation, first introduced by Jacobson [5]. Our aim, in this work, is to consider the evaluation of iterated Ore extensions. We first introduce the definition of the evaluation for polynomials belonging to an iterated Ore extension $R = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$ (see also [1]) and show that it corresponds to a factor of the ring R by an additive subgroup of some form. The fact that we don't divide by a left ideal causes many problems. In particular, we don't get (and cannot get) a product formula for the evaluation. We analyze when our additive subgroup is indeed a left ideal and introduce the notion of good points. In connection with the evaluation of a polynomial in R at $(a_1,\ldots,a_n)$, we introduce sequences of pseudo-linear transformations that help to understand the situation. The evaluation of elements in the ring $S = K[\underline{t};\sigma,\underline{\delta}]$, K a division ring, of multivariate polynomials has been recently studied by U. Martínez-Peñas and F. R. Kschischang [12]. The situation is in fact very similar to the univariate extension. We give the definition for polynomials with coefficients in a ring and introduce pseudo-multilinear transformations which help to get the product formula and various tools similar to those used in the case of a single variable.

Let us briefly describe the content of the paper as follows. In Section 2, we give the definition of the evaluation of skew polynomials in one variable and recall some of their properties. In addition, in this section, we discuss the definition of the evaluation for a polynomial belonging to an extension of the form $A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$ (iterated Ore extension).

The pseudo-(multi)linear transformations are introduced in Section 3, and their main properties are given. In particular, good points are defined, and many characterizations are presented.

Section 4 is devoted to some properties of the sets of roots of polynomials in an iterated Ore extension $K[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$.

Note that in [12] the evaluation of a polynomial in $A[\underline{t};\sigma,\underline{\delta}]$ was defined when $A = K$ is a division ring. In the last section, we define this evaluation on a general ring A and use pseudo-multilinear transformations to get a product formula.

2. Iterated Ore polynomials

Let A be a ring and $\sigma \in \mathrm{End}(A)$. An additive map $\delta : A \to A$ is a σ-derivation if, for any $a, b \in A$, we have $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$.

We can then construct the Ore polynomial ring $A[t;\sigma,\delta]$ (introduced in [14]) whose elements are polynomials $\sum_{i=0}^{l} a_i t^i$, where the coefficient a_i belong to A. Addition of such polynomials is done according to the degree, as in the case of classical polynomials, but the product is based on the commutation law, that is, $ta = \sigma(a)t + \delta(a)$, where $a \in A$.

In what follows, we will always assume that σ is injective. An easy induction leads to the following formula:

$$\forall a \in A,\ \forall n \in \mathbb{N}, \quad t^n a = \sum_{i=0}^{n} f_i^n(a) t^i, \qquad (1)$$

where f_i^n stands for the sum of compositions of i maps σ and $n-i$ maps δ.

If $\sigma = id.$ and $\delta = 0$, then the Ore extension $A[t;\sigma,\delta]$ is the usual polynomial ring. If $a \in A$ and $\sigma \in \mathrm{End}(A)$, then we define the inner σ-derivation of A by $\delta_a(x) = ax - \sigma(x)a$ for any $x \in A$. Let us remark that in this case, for any $x \in A$, we have $(t-a)x = \sigma(x)(t-a) \in R = A[t;\sigma,\delta]$. This implies that $A[t;\sigma,\delta_a] = A[t-a;\sigma]$. If the base ring is commutative, then the evaluation of usual polynomials is multiplicative; in other words, for $f(x), g(x) \in A[x]$ and $a \in A$, we have $(fg)(a) = f(a)g(a)$. This is not true for Ore polynomials, but in the case of a single variable, we have a product formula as we shall explain in Example 2.1(4).

When A is a division ring, then $A[t;\sigma,\delta]$ is always left principal, and hence admits a left Ore ring of quotients. There are strong connections between the ring structure and more arithmetical properties of the polynomials (for instance, invariant and semi-invariant polynomials, Wedderburn polynomials, fully reducible polynomials). This shows that the evaluation of these polynomials is very important. Evaluations are also related to factorizations and this has played a crucial role in coding theory, refer to [2]. More recently, evaluations of skew iterated Ore extensions have been used for "evaluation codes", see [1] for more details.

Let us briefly recall the definition of the evaluation of a polynomial $f(t) \in R = A[t;\sigma,\delta]$ at an element $a \in A$. We define $f(a) \in A$ to be the only element of A such that $f(t) - f(a) \in R(t-a)$. This means, in particular, that $a \in A$ is a right root of $f(t)$ when $t-a$ is right factor of $f(t)$. We then introduce, for any $i \geq 0$, a map N_i defined by induction as follows:

$$N_0(a) = 1, \quad N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a)).$$

This leads to a concrete formula for the evaluation of any polynomial $f(t) = \sum_{i=0}^{n} b_i t^i \in R = K[t;\sigma,\delta]$ at an element $a \in A$ as follows:

$$f(a) = \sum_{i=0}^{n} b_i N_i(a).$$

Before defining the evaluation of iterated polynomials, we now provide a few classical examples.

Examples 2.1.

(1) $R = \mathbb{C}[t;-]$, the commutation rule is here $t(a+ib) = (a-ib)t$, where $a, b \in \mathbb{R}$. An element $a \in \mathbb{C}$ is a (right) root of t^2+1 if $N_2(a)+1 = 0$, i.e., $\overline{a}a + 1 = 0$. From this, it is clear that t^2+1 is an irreducible polynomial in R. On the other hand, it is easy to check that t^2+1 is a central polynomial and we get the quotient $R/(t^2+1)$ is isomorphic to the quaternion algebra $\mathbb{H}$. Furthermore, the roots of the polynomial t^2+1 are exactly the complex numbers of norm 1.

(2) Another important kind of Ore extensions is obtained by presenting the Weyl algebra $A_1 = k[X][Y; id., \frac{d}{dx}]$, where k is a field. The commutation

rule that comes up is thus $YX = XY + 1$. In characteristic zero, this algebra is simple (it doesn't have any two-sided ideal except 0 and A_1). If $\mathrm{char}(k) = p > 0$, then A_1 is a p^2 dimensional algebra over its center $k[X^p, Y^p]$. Evaluating powers of Y at X we get for instance $Y^2(X) = X^2+1$, $Y^3(X) = X^3 + 3X$, and $Y^4(X) = X^4 + 6X^2 + 3$.
We can iterate the procedure and get the Weyl algebra $A_n(k)$.

(3) In coding theory, Ore extensions of the form $\mathbb{F}_q[t; \theta]$, where $q = p^n$ and θ is the Frobenius automorphism defined by $\theta(a) = a^p$, for $a \in \mathbb{F}_q$, have been extensively used (cf. [2]). In [10], both the evaluation and the factorization for these extensions were described in terms of classical (untwisted) evaluation of polynomials. General Ore extensions have also been used to construct codes, see [3].

(4) Let us recall the useful formula for the evaluation of the product of two polynomials $f(t), g(t) \in R = A[t; \sigma, \delta]$ in the case $A = K$ is a division ring:

$$(fg)(a) = 0 \text{ if } g(a) = 0 \quad \textit{and} \quad (fg)(a) = f(a^{g(a)})g(a) \text{ if } g(a) \neq 0,$$

where for $0 \neq c \in K$, we have $a^c = \sigma(c)ac^{-1} + \delta(c)c^{-1}$. We write $\Delta^{\sigma,\delta}(a) := \{a^c \mid c \in U(A)\}$, where $U(A)$ denotes the set of invertible elements of A.

Remarks 2.2. (a) We have defined $N_i(a)$ for $i \in \mathbb{N}$ and a an element of a ring A. These could be called the (σ, δ)-powers of $a \in A$. Any question concerning the powers of elements in a ring has an analog in the (σ, δ)-setting.

(b) The product formula has been mentioned in the last example is also available when A is a ring via the use of (σ, δ)-pseudo-linear transformations. They will be introduced later.

In what follows, we consider an iterated Ore extension

$$R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n].$$

We will always assume that, for any $1 \leq i \leq n$, we have $\sigma_i(A) \subseteq A$ and $\delta_i(A) \subseteq A$. It will be convenient to have notations for intermediate Ore extensions. For this purpose, we put $R_0 = A$, and, for $i \in \{1, \dots, n-1\}$, $R_i = R_{i-1}[t_i; \sigma_i, \delta_i]$. Notice that $R_n = R$. For $f \in R$ and $(a_1, \dots, a_n) \in A^n$, our aim is to define the value of $f(a_1, a_2, \cdots, a_n)$.

Suppose that $(a_1, a_2, \cdots, a_n) \in A^n$ and consider a polynomial

$$f_0 = f(t_1, \dots, t_n) \in R = R_{n-1}[t_n; \sigma_n, \delta_n].$$

We can define $f_1 = f(t_1, \dots, t_{n-1}, a_n) \in R_{n-1}$ as the remainder of the division of f_0 on the right by $t_n - a_n$. This is

$$f_0 = q(t_1, \dots, t_n)(t_n - a_n) + f_1.$$

By the same procedure, we divide $f_1 = f(t_1, \ldots, t_{n-1}, a_n)$ by $t_{n-1} - a_{n-1}$ and get the remainder $f_2 = f(t_1, \ldots, t_{n-2}, a_{n-1}, a_n) \in R_{n-2}$. This is

$$f_1 = f(t_1, \ldots, t_{n-1}, a_n) = q_2(t_1, t_2, \ldots, t_{n-1})(t_{n-1} - a_{n-1}) + f_2.$$

Continuing this process, we define $f_3 \in R_{n-3}, \ldots, f_{n-1} \in R_1, f_n \in R_0 = A$. The evaluation of $f(t)$ at $(a_1, \ldots, a_n)$ is $f_n \in A$. We also remark that for any $0 \leq i \leq n-1$, we have $f_i - f_{i+1} \in R_{n-i}(t_{n-i} - a_{n-i})$.

This leads us to the following definition.

Definition 2.3. *For $f(t_1, \ldots, t_n) \in R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ and $(a_1, \ldots, a_n) \in A^n$, we define the evaluation of $f(t_1, t_2, \ldots, t_n)$ at a point $(a_1, \ldots, a_n)$, denoted by $f(a_1, \ldots, a_n)$, as the representative in A of $f(t_1, t_2, \ldots, t_n)$ modulo*

$$I_n(a_1, \ldots, a_n) = R_1(t_1 - a_1) + \cdots + R_{n-1}(t_{n-1} - a_{n-1}) + R(t_n - a_n),$$

where, for each $1 \leq i \leq n$, R_i stands for $R_i = A[t_1; \sigma_1, \delta_1] \cdots [t_i; \sigma_i, \delta_i]$.

The above discussion shows that for any polynomial $f(t) \in R$ there exists an element $c \in A$ such that $f(t) - c \in I_n$. Notice that $I_n = I_n(a_1, \ldots, a_n)$ is an additive subgroup of $(R, +)$ and is not, in general, a left ideal in $R = R_n$. We will consider and characterize those points for which I_n is indeed a left ideal of R, see below.

Another way to compute the evaluation is to note that the polynomials in $R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ can be written in a unique way as sums of monomials of the form $\alpha_{l_1, \ldots, l_n} t_1^{l_1} t_2^{l_2} \cdots t_n^{l_n}$, for some $0 \leq l_1, l_2, \ldots, l_n \leq n$ and $\alpha_{l_1, \ldots, l_n} \in A$. The sum $\sum_{i=1}^n l_i$ is called the degree of the monomial and the degree of a polynomial is given by the degree of the monomials with a higher degree. First remark that if a monomial $m = m(t_1, \ldots, t_n)$ is of degree l, then for any $a \in A^*$, ma is a polynomial of degree l as well. We define the evaluation by induction on the degree. In practice, it is sufficient to define the evaluation of a monomial.

For $(a_1, a_2, \ldots, a_n) \in A^n$ and $m = m(t_1, \ldots, t_n)$, we define $m(a_1, \ldots, a_n)$ as follows:

If $\deg(m) = 1$ and $m = \alpha t_i$ for some $1 \leq i \leq n$ and $\alpha \in A$, then $m(a_1, \ldots, a_n) = \alpha a_i$. So, assume that the evaluation of the monomials of degree $< l$ has been defined and consider a monomial $m = m(t)$ such that $\deg(m) = l \geq 1$ and $m = m'(t_1, \ldots, t_j)t_j$ for some $1 \leq j \leq n$, then $m(a_1, \ldots, a_n) = m''(a_1, \ldots, a_j)$ such that the polynomial $m''(t_1, \ldots, t_j) = m'(t_1, \ldots, t_j)a_j$ is of the degree smaller than l.

We are now going to make some remarks about this evaluation.

Remark 2.1. (1) First let us notice that, before we evaluate a polynomial, we must write it with the variables appearing in the precise order $t_1, t_2, \ldots, t_n$ (from left to right). In other words, before evaluating a polynomial we must write it as a sum of monomials of the form $t_1^{l_1} t_2^{l_2} \cdots t_n^{l_n}$.

(2) Of course, this is not the only possible definition, but although it might look a bit strange, it is still natural if we want the zeros being right roots. Let us look more closely at the case of two variables. In other words, it is natural for (a_1, a_2) to annihilate a polynomial of the form $g(t_1)(t_2 - a_2)$; but we don't necessarily expect (a_1, a_2) to be a zero of a polynomial of the form $(t_1 - a_1)h(t_1)$.

(3) Since the base ring is not assumed to be commutative, we must be very cautious while evaluating a polynomial, even when the variables commute. With this definition, $t_1 t_2 \in A[t_1, t_2]$ evaluated at (a, b) gives $(t_1 t_2)(a, b) = ba$. This might look very strange, but if we think of evaluation in terms of "operators" via the right multiplication by b followed by the right multiplication by a this evaluation looks perfectly fine and the apparent awkwardness disappears.

(4) We assume that the different endomorphisms σ_i's are such that $\sigma_i(A) \subseteq A$. In other words, for $i > 1$, σ_i is an extension of $\sigma_i|_K$ to R_{i-1}. Some commutation relations exist between the different endomorphisms σ_i. For instance, consider the polynomial ring extension $R = A[t_1; \sigma_1][t_2; \sigma_2]$. If we put $\sigma_2(t_1) = \sum_{i=0}^{l} a_i t_1^i$ computing $\sigma_2(\sigma_1(a)t_1) = \sigma_2(t_1 a) = \sigma_2(t_1)\sigma_2(a)$, leads to the following equations

$$\forall \ 0 \leq i \leq l, \quad a_i \sigma_1^i(\sigma_2(a)) = \sigma_2(\sigma_1(a))a_i.$$

Let us now give some examples.

Examples 2.4. (1) Let $A_1(k) = k[X][Y; id., \frac{d}{dX}]$ and $(a, b) \in k^2$. Then

- $YX = XY + 1 = X(Y - b) + bX + 1 = X(Y - b) + b(X - a) + ba + 1$, and hence $(YX)(a, b) = ba + 1$.
- $YX^2 = X^2Y + 2X = X^2(Y - b) + bX^2 + 2X = X^2(Y - b) + bX(X - a) + baX + 2(X - a) + 2a$, and hence $(YX^2)(a, b) = ba^2 + 2a$.
- $Y^2X = XY^2 + 2Y = XY(Y - b) + bX(Y - b) + bXb + 2(Y - b) + 2b$, and therefore $(Y^2X)(a, b) = b^2a + 2b$.

(2) Consider the double Ore extension $R = \mathbb{F}_q[t_1; \theta][t_2; \overline{\theta}]$, where $q = p^n$, $\overline{\theta}(a) = a^p$, and $\overline{\theta}(t_1) = t_1$. A polynomial $p(t_1, t_2) \in R$ can be written as $p(t_1, t_2) = \sum_{i=0}^{n} p_i(t_1) t_2^i = \sum_{i,j} a_{i,j} t_1^j t_2^i$, and we can easily check

that

$$p(t_1,t_2)(a,b)=\sum_{i,j}\theta^j(N_i(b))N_j(a)=b^{\frac{(p^i-1)p^j}{p-1}}a^{\frac{p^i-1}{p-1}}.$$

(3) Consider the polynomial ring $R=K[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]$, and let us evaluate the polynomials t_1t_2 and t_2t_1 at $(a_1,a_2)\in K^2$. So, we want to compare $(t_1t_2)(a_1,a_2)$ and $(t_2t_1)(a_1,a_2)$.
   - We have $t_1t_2=t_1(t_2-a_2)+t_1a_2=t_1(t_2-a_2)+\sigma_1(a_2)t_1+\delta_1(a_2)$. This leads to $(t_1t_2)(a_1,a_2)=\sigma_1(a_2)a_1+\delta_1(a_2)$.
   - $(t_2t_1)(a_1,a_2)=(\sigma_2(t_1)t_2+\delta_2(t_1))(a_1,a_2)=\sigma_2(a_1)a_2+\delta_2(a_1)$.

(4) Let us compute $(t_1t_2t_3)(a_1,a_2,a_3)$ and $(t_3t_2t_1)(a_1,a_2,a_3)$.
   - We have $t_1t_2t_3=t_1t_2(t_3-a_3)+t_1t_2a_3=t_1t_2(t_3-a_3)+t_1(\sigma_2(a_3)t_2$ $+\delta_2(a_3))=t_1t_2(t_3-a_3)+t_1\sigma_2(a_3)t_2+t_1\delta_2(a_3)=t_1t_2(t_3-a_3)+$ $\sigma_1(\sigma_2(a_3))t_1t_2+\sigma_1(\delta_2(a_3))t_1+\delta_1(\delta_2(a_3))$. This leads to $(t_1t_2t_3)(a_1,a_2,a_3)=\sigma_1(\sigma_2(a_3))a_1a_2+\sigma_1(\delta_2(a_3))a_1+\delta_1(\delta_2(a_3))$.
   - $t_3t_2t_1=t_3(\sigma_2(t_1)t_2+\delta_2(t_1))=t_3(\sigma_2(t_1)t_2)+t_3\delta_2(t_1)=$ $\sigma_3(\sigma_2(t_1)t_2)t_3+\sigma_3(\delta_2(t_1))+\delta_3(\delta_2(t_1))$. We thus get $t_3t_2t_1(a_1,a_2,a_3)=\sigma_3(\sigma_2(a_1)a_2)a_3+\sigma_3(\delta_2(a_1))+\delta_3(\delta_2(a_1))$.

(5) Monomials in a single variable can be evaluated in the classical ways (as has been stated at the beginning of this section). Hence, let us introduce the following notation. For $1\le i\le n$, $j\in\mathbb{N}$, and $x\in A$, we put

$$N_{i,j}(x)=(t_i^j)(x).$$

Of course, this is just the usual evaluation in $A[t_i;\sigma_i,\delta_i]$. As in (1) above we can introduce, for any $1\le i\le l$, the maps $f_{k,i}^l$ from A to A as being the sum of all monomials with i maps σ_k and $l-i$ maps δ_k. We can then evaluate monomials over a general ring A. To see an example, we compute the case in which $n=2$ the evaluation of $t_1^it_2^j$ at (a_1,a_2). We thus compute modulo $R_1(t_1-a_1)+R_2(t_2-a_2)$ and get successively:

$$t_1^it_2^j\equiv t_1^iN_{2,j}(a_2)\equiv\sum_l f_{1,l}^i(N_{2,j}(a_2))t_1^l\equiv\sum_l f_{1,l}^i(N_{2,j}(a_2))N_{1,l}(a_1).$$

3. Pseudo-linear transformations

The pseudo-linear transformations were introduced by Jacobson (cf. [5]). They are the analog of the usual linear transformations of vector spaces and many of the classical results of linear algebra have their analog for pseudo-linear transformations, see [10]. In the case of one variable, the pseudo-linear transformations are fundamental since, as we will see, they allow us to describe the left $R = K[t;\sigma;\delta]$ modules, they give a way to evaluate the polynomials, they provide a product formula, and they lead to vector spaces in the set of roots of a polynomial, and that finally gives a bound on "the number of roots".

If V is a left module over $R := A[t;\sigma,\delta]$, then V is a left A-module, and the variable t acts on the left of V. We thus have

$$t.(\alpha v) = (t\alpha).v = (\sigma(\alpha)t + \delta(\alpha)).v = \sigma(\alpha)t.v + \delta(\alpha)v.$$

Of course, left multiplication by t on V is additive. This justifies the following definition.

Definitions 3.1. *Let V be a left A-module and σ and δ be respectively an endomorphism and a σ-derivation of A. An additive map $T : V \to V$ such that, for all $\alpha \in A$ and $v \in V$, we have $T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v$ is called a (σ,δ)-pseudo-linear map.*

We have seen that whenever V is an $A[t;\sigma,\delta]$-left module, the action of t on V gives rise to a (σ,δ)-pseudo-linear map on ${}_AV$. Conversely, if ${}_AV$ is a left A-module, and $T : V \longrightarrow V$ is a (σ,δ)-pseudo-linear map defined on V, then V can be given a left $A[t;\sigma,\delta]$-module structure by defining $t.v = T(v)$ for any $v \in V$. This leads to a one-to-one correspondence between the set of A-modules V equipped with a (σ,δ)-pseudo-linear map and $A[t;\sigma,\delta]$-left module. For more details on pseudo-linear maps, we refer the reader to [5], [10], and [6]. If $a \in A$, then the map $T_a : A \to A$ defined by $T_a(x) = \sigma(x)a + \delta(x)$ is a (σ,δ)-pseudo-linear transformation on A. Notice that for $a = 0$, we have $T_0 = \delta$. Coming back to a general (σ,δ)-PLT on A, it is easy to check that if T is a (σ,δ)-PLT defined on ${}_AV$, we have for any $a \in A$, $n \in \mathbb{N}$, and $v \in V$

$$T^n(av) = \sum_{i=0}^{n} f_i^n(a)T^i(v),$$

where f_i^n is the sum of all the words in i letters σ and $n-i$ letters δ. Comparing this last equation with the one given in (1) (see Section 1) leads to the following ring homomorphism:

$$\varphi : R = A[t;\sigma,\delta] \to \mathrm{End}(V,+) \text{ given by } \varphi(\sum_{i=0}^{n} a_i t^i) = \sum_{i=0}^{n} L_{a_i}T^i,$$

where, for each $a \in A$, L_a stands for the left multiplication by a, i.e., $L_a(v) = av$, for any $a \in A$ and $v \in V$. The details can be found in the papers that have been mentioned above. The (σ,δ)-PLT T_a defined above allows us to translate the evaluation, as follows:

$$P(a) = P(T_a)(1).$$

Using the fact that the map φ is a ring homomorphism, we easily get the product formula for Ore polynomial with coefficients in a ring. This easily leads to $(f(t)g(t))(a) = f(T_a)(g(a))$.

This can be viewed as a general product formula also valid for an Ore extension based on a ring A that is not a division ring. The (σ,δ)-PLT is also connected with roots of a polynomial inside a given (σ,δ)-conjugacy class. We start by considering a special case of the product formula when $g(t) = x \in A$. We then get $(f(t)x)(a) = f(T_a)(x)$, and hence

$$\mathrm{Ker} f(T_a) = \{x \in A \mid (f(t)x)(a) = 0\}.$$

We also introduce the following subring of A

$$C^{\sigma,\delta}(a) = \{b \in A \mid T_a(b) = ab\}.$$

We compute $T_a(xb) = \sigma(xb)a + \delta(xb) = \sigma(x)(\sigma(b)a + \delta(b)) + \delta(x)b = \sigma(x)T_a(b) + \delta(x)b = \sigma(x)ab + \delta(x)b = T_a(x)b$, and conclude that T_a is a right $C^{\sigma,\delta}(a)$-morphism. Therefore, for $f(t) \in R = A[t;\sigma,\delta]$ and $a \in A$, the kernel $\mathrm{Ker} f(T_a)$ is a right $C^{\sigma,\delta}(a)$-module. When $A = K$ is a division ring, the subring $C^{\sigma,\delta}(a)$ is a division ring (isomorphic to $\mathrm{End}_R(R/R(t-a))$) and the right roots of a polynomial belong to a finite number of conjugacy classes, say $\{\Delta^{\sigma,\delta}(a_1), \ldots, \Delta^{\sigma,\delta}(a_n)\}$. Denoting C_i as the class $C^{\sigma,\delta}(a_i)$, we obtain

$$\sum \dim_{C_i}(\mathrm{Ker}(f(T_i))) \leq \deg(f).$$

We now consider an iterated extension $A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$. We will always assume that, for any $1 \leq i \leq n$, $\sigma_i(A) \subseteq A$ and $\delta_i(A) \subseteq A$. First, we introduce some notations as follows:

$R_0 = A = S_0$ and for $1 \leq i \leq n$, we put $S_i = A[t_i;\sigma_i,\delta_i]$ and define

$R_1 = A[t_1;\sigma_1,\delta_1]$,

$R_2 = R_1[t_2;\sigma_2,\delta_2] = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]$,

$R_3 = R_2[t_3;\sigma_3,\delta_3] = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2][t_3;\sigma_3,\delta_3]$, and finally

$R = R_n = R_{n-1}[t_n;\sigma_n,\delta_n] = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$. We also define, for $1 \leq i < j \leq n$, $p_{i,j} = \sigma_j(t_i) \in R_{j-1}$ and $q_{i,j} = \delta_j(t_i) \in R_{j-1}$.

The following proposition is the analog of a classical result in the case of a single variable Ore extension (cf. [6]).

Proposition 3.2. *Let A be a ring and, for each $1 \leq i \leq n$, let (σ_i,δ_i) be endomorphisms and σ_i-derivations on A, and*

$$R = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n].$$

Let also ${}_AV$ be a left A-module. Then the following statements are equivalent:

(i) ${}_AV$ *has a left R-module structure.*
(ii) *For each $1 \leq i \leq n$, V is a left R_i-module structure.*
(iii) *For each $1 \leq i \leq n$, the left multiplication by t_i is a (σ_i, δ_i)-PLT on V considered as a left R_{i-1} module.*
(iv) *There exists a subset $\{T_1, \ldots, T_n\} \subset \mathrm{End}(V, +)$ such that for each $1 \leq i \leq n$, T_i is a (σ_i, δ_i)-PLT on ${}_{R_i}V$ such that for all $1 \leq i < j \leq n$, we have $T_j \circ T_i = p_{i,j}(T_1, \ldots, T_{j-1})T_j + q_{i,j}(T_1, \ldots, T_{j-1})$.*

Proof. (i) $\Rightarrow$ (ii) This is straightforward since R_i is a subring of $R = R_n$.

(ii) $\Rightarrow$ (iii) The proof goes by induction on $i \geq 1$.

(iii) $\Rightarrow$ (iv) The maps T_i are given by the left multiplication by t_i. We prove the equality given in (iv) for $j = 2$ and $v \in V$.

We have $(T_2 \circ T_1)(v) = T_2(t_1.v) = \sigma_2(t_1).T_2(v) + \delta_2(t_1).v = p_{12}(t_1).T_2(v) + q_{1,2}(t_1).v = p_{1,2}(T_1)(T_2(v)) + q_{1,2}(T_1)(v) = (p_{1,2}(T_1) \circ T_2)(v) + q_{1,2}(T_1)(v)$. This proves the formula for $j = 2$. The general case is similar.

(iv) $\Rightarrow$ (i) The left $R = R_n$ module structure on V is given via $t_i.v = T_i(v)$. The equality given in (iv) will insure that the successive action of t_i and t_j are compatible with the product in R. □

With the notations of the above proposition, we get the following corollary.

Corollary 3.3. *The map $\varphi : R \to \mathrm{End}(V, +)$ defined by*

$$\varphi(\sum a_{i_1,\ldots,i_n} t_1^{i_1} t_2^{i_2} \cdots t_n^{i_n}) = \sum L_{a_{i_1,\ldots,i_n}} T_1^{i_1} \circ T_2^{i_2} \circ \cdots \circ T_n^{i_n},$$

is a ring homomorphism.

Proof. First, note that we have the following equalities

$$\varphi(t_i a) = \varphi(\sigma_i(a)t_i + \delta_i(a)) = L_{\sigma_i(a)} \circ T_i + L_{\delta_i(a)} = T_i \circ L_a = \varphi(t_i) \circ \varphi(L_a).$$

We leave it to the reader to check that $\varphi(t_i t_j) = \varphi(t_i) \circ \varphi(t_j)$. □

Remark 3.4. Having a sequence $T_1, \ldots, T_n$ such that T_i is a (σ_i, δ_i)-PLT on a left A-module V, we get a left structure of $S_i = A[t; \sigma_i, \delta_i]$-module on V. This is of course not enough to get a structure of left R-module on V. In fact, what is needed is to have an "increasing" sequence of structures defined on V as follows: T_1 on ${}_AV$ leads to a left R_1-structure on V, T_2 defined on ${}_{R_1}V$ leads to a left R_2 structure on V, T_3 defined on ${}_{R_2}V$ leads to a left R_3 structure on V, and so on. This will be of particular importance while considering a sequence of elements $(a_1, \ldots, a_n) \in A^n$ and their associated PLT defined on $V = A$ via $T_i(x) = \sigma_i(x)a_i + \delta_i(x)$ for all $x \in A$.

We continue our argument with the following definition.

Definition 3.5. *Let A a ring, $R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ be an iterated Ore extension, ${}_AV$ a left A-module, and $(T_1, \dots, T_n)$ be a sequence of maps in $\mathrm{End}(V, +)$ such that for each $1 \le i \le n$, T_i is a (σ_i, δ_i)-PLT of ${}_AV$. This sequence $(T_1, \dots, T_n)$ is called good if $({}_AV, T_1)$ gives a ${}_{R_1}V$ structure on V, and T_2 is a (σ_2, δ_2)-PLT on ${}_{R_1}V$ so that $({}_{R_1}V, T_2)$ defines an ${}_{R_2}V$ structure on V and inductively, for any $1 \le i < n$, T_{i+1} is a (σ_i, δ_i)-PLT on ${}_{R_i}V$-structure which leads to an R_{i+1} module structure on V.*

Example 3.6. For our purpose, one of the most important examples of sequences of PLT comes from the evaluation maps. Let $a = (a_1, \dots, a_n) \in A^n$ and consider the following iterated Ore extension

$$R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n].$$

For $1 \le i \le n$, we define the map $T_i : A \to A$ given by $T_i(x) = \sigma_i(x)a_i + \delta_i(x)$ for all $x \in K$. This sequence of PLT's defined on K corresponds to a left R-module structure on K. This R-module structure is closely related to evaluation at a. The point of the next theorem is to study this connection.

Theorem 3.7. *Let A be a ring and $R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ an iterated Ore extension on A. For $a = (a_1, \dots, a_n) \in A^n$, we let $T_i = T_{a_i}$ be the PLT on A defined in the above example and $f = f(t_1, \dots, t_n) \in R$. Then the following statements hold.*

(1) *For any $x \in A$, we have $(fx)(a_1, \dots, a_n) = f(T_{a_1}, \dots, T_{a_n})(x)$.*
(2) *We have $f(a_1, \dots, a_n) = f(T_{a_1}, \dots, T_{a_n})(1)$.*
(3) *For any $x \in U(A)$, we have*

$$f(T_{a_1}, \dots, T_{a_n})(x) = (fx)(a_1, \dots, a_n) = f(a_1^x, \dots, a_n^x)x,$$

where for each $i \in \{1, \dots, n\}$, $a_i^x = \sigma_i(x)a_ix^{-1} + \delta_i(x)x^{-1}$.

Proof. (1) It is enough to consider the case in which $f = m = t_1^{l_1}t_2^{l_2} \cdots t_n^{l_n}$ is a monomial. We then use induction on the length of the monomial. So, if $m = t_i$, for some $1 \le i \le n$, then we have the following equalities

$$(t_ix)(a_1, \dots, a_n) = (\sigma_i(x)t_i + \delta_i(x))(a_1, \dots, a_n) = \sigma_i(x)a_i + \delta_i(x) = T_{a_i}(x),$$

for any $x \in A$, and hence the formula is verified. Now, assume that $m(t_1, \dots, t_n) = m'(t_1, \dots, t_i)t_i$ for some $m' \in R$ and $i \in \{1, \dots, n\}$ and also the equality holds for m'. Notice that $m' \in R_i$. We then compute modulo $I_n = R_1(t_1 - a_1) + \cdots + R_n(t_n - a_n)$ and deduce that

$$mx + I_n = m't_ix + I_n = m'(\sigma_i(x)t_i + \delta_i(x)) + I_n.$$

As $m' \in R_i$ and $R_i(t_i - a_i) \subseteq I_n$, we get $mx + I_n = m'(\sigma_i(x)a_i + \delta_i(x)) + I_n$. Our induction hypothesis then implies that

$$mx + I_n = m'(T_{a_1}, \ldots, T_{a_n})(\sigma_i(x)a_i + \delta_i(x)) + I_n.$$

Hence, we conclude that $(mx)(a_1, \ldots, a_n) = m'(T_{a_1}, \ldots, T_{a_n})(\sigma_i(x)a_i + \delta_i(x)) = m'(T_{a_1}, \ldots, T_{a_n})(T_{a_i}(x)) = m(T_{a_1}, \ldots, T_{a_n})(x)$. This finishes the induction and yields the result.

(2) This is obtained by choosing $x = 1$ in statement (1) of this theorem.

(3) The first equality is just the equation (1) above. We have

$$f + \sum_i R_i(t_i - a_i^x) = f(a_1^x, \ldots, a_n^x) + \sum_i R_i(t_i - a_i^x),$$

and right multiplying by x, this gives that

$$fx + \sum_i R_i(t_i - a_i^x)x = f(a_1^x, \ldots, a_n^x)x + \sum_i R_i(t_i - a_i^x)x.$$

We then remark that $(t_i - a_i^x)x = \sigma_i(x)(t_i - a_i)$ and get the following equality

$$fx + \sum_i R_i(t_i - a_i) = f(a_1^x, \ldots, a_n^x)x + \sum_i R_i(t_i - a_i).$$

This shows our claim. □

Example 3.8. The statement (3) above can be used to obtain a closed formula for the evaluation of $f(t_1, \ldots, t_n) = \sum \alpha_{l_1,\ldots,l_n} t_1^{l_1} t_2^{l_2} \cdots t_n^{l_n}$ at the point $(a_1, \ldots, a_n) \in K^n$. For instance, in the case in which $n = 2$ and $(a, b) \in K^2$, we consider the evaluation of $f(t_1, t_2) = \sum_{i=0,j=0}^{l_1,l_2} a_{i,j} t_1^i t_2^j$ at (a, b) and, assuming $x_j := N_j^{\sigma_2,\delta_2}(b) \neq 0$ for $0 \leq j \leq l_2$, we deduce that

$$f(a, b) = \sum_{i,j} a_{i,j} N_i^{\sigma_1,\delta_1}(a^{x_j})x_j.$$

Let us now turn to another possible way of evaluating a polynomial $f(t_1, \ldots, t_n) \in R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ at $(a_1, a_2, \ldots, a_n) \in K^n$. We consider the element of K representing f in the quotient R/I, where $I = R(t - a_1) + R(t - a_2) + \cdots + R(t - a_n)$. The set I is the usual left ideal of R and this evaluation looks more classical. Unfortunately, in general, for a sequence $(a_1, \ldots, a_n) \in A^n$ it arises frequently that $I = R$ and this new evaluation is then not a good one. We say that a point $(a_1, \ldots, a_n) \in A^n$ is *good* if we have $I_n = \sum_{i=1}^n R_{i-1}[t_i; \sigma_i, \delta_i] = I$. The next proposition will compare the two evaluations by comparing $I_n = R_1(t_1 - a_1) + \cdots + R_{n-1}(t_{n-1} - a_{n-1}) + R(t_n - a_n)$ and I. It will show that a point $(a_1, \ldots, a_n) \in A^n$ is good if and only if the sequence $(T_{a_1}, \ldots, T_{a_n})$ is a good sequence.

Theorem 3.9. *Let A be a ring and $R = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]$. We consider $(a_1,a_2,\ldots,a_n)\in A^n$ and put*

$$I = R(t_1-a_1)+R(t_2-a_2)+\cdots+R(t_n-a_n),$$

and

$$I_n = R_1(t_1-a_1)+\cdots+R_{n-1}(t_{n-1}-a_{n-1})+R(t_n-a_n),$$

where, for each $1\le i\le n$, $R_i = A[t_1;\sigma_1,\delta_1]\cdots[t_i;\sigma_i,\delta_i]$. With these notations, the following statements are equivalent:

(1) *$I_n = I$;*
(2) *$R(t_i-a_i)\subseteq I_n$;*
(3) *$I\neq R$;*
(4) *For $1\le i<j\le n$, we have $t_j(t_i-a_i)\in I_n$;*
(5) *For $1\le i<j\le n$, we have $\sigma_j(t_i-a_i)a_j+\delta_j(t_i-a_i)\in I_n$;*
(6) *For $1\le i<j\le n$, we have $(t_jt_i)(a_1,\ldots,a_n)=\sigma_j(a_i)a_j+\delta_j(a_i)$;*
(7) *For all $f,g\in R$, we have*

$$(fg)(a_1,a_2,\ldots,a_n) = (f(T_{a_1},T_{a_2},\ldots,T_{a_n})\circ g(T_{a_1},T_{a_2},\ldots,T_{a_n}))(1);$$

(8) *The sequence $(T_{a_1},T_{a_2},\ldots,T_{a_n})$ of PLT on A is good;*
(9) *The map $\psi : R = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta_2]\cdots[t_n;\sigma_n,\delta_n]\longrightarrow End(A,+)$ defined by $\psi(f(t_1,\ldots,t_n)) = f(T_{a_1},\ldots,T_{a_n})$ is a ring homomorphism.*

Proof. (1) $\Leftrightarrow$ (2) is straightforward.
(2) $\Rightarrow$ (3) If $I=R$, then $I_n=R$ and, for $1\le i\le n$, there exist polynomials $g_i(t_1,t_2,\ldots,t_i)\in R_i$ such that $1=\sum_{i=1}^n g_i(t_1,\ldots,t_i)(t_i-a_i)$. The change of variables defined by putting $y_i=t_i-a_i$ gives that, for some $h_i\in R_i$, we have $1=\sum_{i=1}^n h_i(y_1,\ldots,y_i)y_i$. A comparison of the coefficients of degree zero of this equality, leads to a contradiction.
(3) $\Rightarrow$ (4) There exists $c\in A$ such that $t_j(t_i-a_i)-c\in I_n\subseteq I$. Since $t_j(t_i-a_i)\in I$, we obtain $c\in I$; hence, by (3), we must have $c=0$. This shows that $t_j(t_i-a_i)\in I_n$.
(4) $\Rightarrow$ (5) It follows from $t_j(t_i-a_i)\in I_n$ that $\sigma_j(t_i-a_i)t_j+\delta_j(t_i-a_i)\in I_n$. Since $(t_j-a_j)\in I_n$, we obtain $\sigma_j(t_i-a_i)a_j+\delta_j(t_i-a_i)\in I_n$.
(5) $\Rightarrow$ (6) This is clear since (5) implies that

$$t_jt_i-\sigma_j(a_i)a_j-\delta_j(a_i)=\sigma_j(t_i)t_j+\delta_j(t_i)-\sigma_j(a_i)a_j-\delta_j(a_i)\in I_n.$$

(6) $\Rightarrow$ (1) The equality in (6) yields that $t_jt_i-\sigma_j(a_i)a_j-\delta_j(a_i)\in I_n$ for $1\le i<j\le n$. This gives that $t_j(t_i-a_i)\in I_n$. On account of we also have $R_i(t_i-a_i)\subseteq I_n$, we conclude that $t_j(t_i-a_i)\in I_n$ for any integer

$1 \le i \le j \le n$, and hence $R(t_i - a_i) \subseteq I_n$ for any $1 \le i \le n$. This yields $I_n = I$, as required.
(6) $\Rightarrow$ (7) It is enough to prove the formula when f, g are two monomials. We proceed by induction on the length l of fg, and we may assume that in both monomials f and g the variables appear with increasing indexes. If the monomial fg itself has its variables appearing in increasing order, then the result comes from statement (2) in the Theorem 3.7. So, we may assume that the variables appearing on the right of f and on the left of g have decreasing indexes. If $l = 1$, then $g = b$ is a constant and $f = t_i$ for some $1 \le i \le n$. We then have

$$fg(a_1, \dots, a_n) = (t_i b)(a_1, \dots, a_n) = \sigma_i(b)a_i + \delta_i(b) = T_{a_i}(b) = (T_{a_i} \circ L_b)(1).$$

If $l = 2$, then the result comes from the statement (6) which can be translated as $(t_j t_i)(a_1, \dots, a_n) = (T_{a_j} \circ T_{a_i})(1)$. Hence, suppose the formula is true for monomials f, g such that length of fg is less than or equal to $l > 2$ and consider two monomials f, g such that the length of fg is $l + 1$. The length of g must be at least 1 and we can write $g = g't_i$ for some $i \in \{1, \dots, n\}$. Since the statement (6) is equivalent to (1), we know that $I_n = I$ is a left R-module and hence working modulo I, we can write $fg = fg't_i \equiv fg'a_i$. Hence, writing a for $(a_1, \dots, a_n)$ and T_a for the sequence $(T_{a_1}, \dots, T_{a_n})$, we get $(fg)(a) = (fg't_i)(a) = (fg'a_i)(a)$. The inductive hypothesis then leads to $(fg'a_i)(a) = (f(T_a) \circ (g'a_i)(T_a))(1) = (g(T_a) \circ (g't_i)(T_a))(1) = (f(T_a) \circ g(T_a))(1)$. This yields the required formula.

(7) $\Rightarrow$ (8) We show by induction on $j \in \{1, \dots, n\}$ that A has a left R_{j-1}-module structure and that the associated (σ_j, δ_j)-PLT on A is T_j. It is easy to check that T_{a_1} is a left (σ_1, δ_1)-derivation defined on ${}_AA =_{R_0} A$. This gives a left R_1-module structure on A. Suppose that we have shown A has a left R_i structure for $1 \le i < j$ given by the actions of the T_{a_i}. We have to show that T_{a_j} is a (σ_j, δ_j)- PLT on ${}_{R_i}A$ for every $i < j$. In fact, the Remark 3.4 implies that one only needs to show that, for every $1 \le j \le n$, T_{a_j} is a left R_j-module. We compute, for $x \in A$, $T_{a_j}(t_i.x) = T_{a_j}(T_{a_i}(x)) = (T_{a_j} \circ T_{a_i} \circ L_x)(1) = (t_j t_i x)(a) = (\sigma_j(t_i)t_j + \delta_j(t_i)x)(a)$, where we have used the formula given in (7). Let us write $\sigma_j(T_{a_j})$ and $\delta_j(T_{a_i})$ for $\sigma_j(t_i)(T_{a_j})$ and $\delta_j(t_i)(T_{a_i})$ respectively. Using the first statement given in Theorem 3.7, we then get $(\sigma_j(t_i)t_j + \delta_j(t_i)x)(a) = ((\sigma_j(T_{a_i}) \circ T_{a_j} + \delta_j(T_{a_i}))(x) = \sigma_j(T_{a_i})(T_{a_j}(x)) + \delta_j(T_{a_i})(x) = \sigma_j(t_i).T_{a_j}(x) + \delta_{a_j}(T_i).x$. This shows that we have $T_{a_j}(t_i.x) = \sigma_j(t_i).T_{a_j}(x) + \delta_{a_j}(T_i).x$, as required.

(8) $\Rightarrow$ (9) This is a direct consequence of Corollary 3.3.

(9) ⇒ (1) Since ψ is a ring homomorphism, we have thanks to Theorem 3.7, for every $f, g \in R$,

$$(fg)(a) = (fg)(T_{a_1}, \ldots, T_{a_n})(1) = f(T_{a_1}, \ldots, T_{a_n})g(T_{a_1}, \ldots, T_{a_n})(1).$$

Therefore, if $i < j$, one can conclude that

$$(t_j(t_i - a_i))(a_1, \ldots, a_n) = (T_j \circ (T_i - a_i))(1) = T_{a_j}(T_{a_i}(1) - a_i) = 0.$$

This shows that statement (4) above is satisfied, and hence I_n is indeed a left ideal of R and is equal to I. □

Remark 3.10. *When the sequence $T_{a_1}, \ldots, T_{a_n}$ is good, we get a left R-module structure on A given by $p(t_1, \ldots, t_n) \star a = p(T_{a_1}, \ldots, T_{a_n})(a)$.*

Remarks 3.11. 1) If $n = 1$, we obviously have $I = I_1$ and all points are good.

2) In general, the two additive subsets $I_n \subset I$ are different. As mentioned above, we will use I_n for our evaluation. The reason is that while evaluating with respect to I we often face the following problem: the left R-module I can be the entire ring. So that the evaluation of any polynomial at $(a_1, a_2 \ldots, a_n) \in K^n$ with respect to I is zero. This is the case in the Weyl algebra $R = A_1(K) = K[t_1][t_2; id, \frac{d}{dt_1}]$ for the point $(0, 0)$ since we then have $t_2t_1 - t_1t_2 = 1$, and hence $Rt_1 + Rt_2 = R$. This is not the case with our evaluation since, for instance, $t_2t_1 = t_1t_2 + 1$, so that $t_2t_1 + I_2(0, 0) = 1 + I_2(0, 0)$, and hence the evaluation of t_2t_1 at $(0, 0)$ is just 1.

3) In fact, it is quite often the case that $I = R$, even if we are using Ore polynomials with zero derivations. For example, consider the Ore extension $R = K[t_1; \sigma_1][t_2; \sigma_2]$, where K is a field and σ_2 is an endomorphism of $K[t_1; \sigma_1]$ such that $\sigma_2(t_1) = t_1$. It is easy to check that for any $(a_1, a_2) \in K^2$, we have $(t_2 - \sigma_1(a_2))(t_1 - a_1) + (-t_1 + \sigma_2(a_1))(t_2 - a_2) = \sigma_1(a_2)a_1 - \sigma_2(a_1)a_2$. So that if $\sigma_1(a_2)a_1 - \sigma_2(a_1)a_2 \neq 0$, then the left ideal $I(a_1, a_2) = R$. This shows that very often the evaluation modulo I turns out to be trivial. Once again, this is not the case with our evaluation, since we have $t_2(t_1 - a_1)$ is represented by $\sigma_1(a_2)a_1 - \sigma_2(a_1)a_2$ modulo $I_2(a_1, a_2)$.

Definition 3.1. *A point $(a_1, \ldots, a_n) \in A^n$ will be called a good point if the two ways of evaluating a polynomial in $K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ at $(a_1, \ldots, a_2)$ coincide, i.e., if $I_n(a_1, \ldots, a_n) = I$.*

The advantage of the good points is that in this case the evaluations via the left ideal I and via the additive subgroup I_n coincide and we can use the product formula. But, of course, we can still evaluate a polynomial at any point via our additive subset $I_n = R_1(t_1 - a_1) + \cdots + R_{n-1}(t_{n-1} - a_{n-1}) + R(t_n - a_n)$.

Example 3.2. (1) In the classical case ($\sigma_i = id_K$ and $\delta_i = 0$, for every $1 \le i \le n$) we have every point $(a_1, \ldots, a_n) \in A^n$ is good.

(2) If K is a division ring, $\sigma_1 = id_K$, $\delta_1 = 0$, $\sigma_2 = id$, and $\delta_2 = d/dt_1$, then we have $(t_2 - b)(t_1 - a) = (t_1 - a)(t_2 - b) + 1$ for any $a, b \in K$. This shows that in this case there are no good points.

(3) Although we don't have a nice product formula in general, we still have one when the point that is considered for evaluation is a good point and also in some cases depending on the polynomials. Let us notice in particular, that if $g \in R_n$, then for any $f \in R_1$ and any point $a \in A^n$, we have $fg(a) = f(T_a)(g(a))$. Indeed, Remarking that $I_n = \sum_{i=1}^{n} R_i(t_i - a_i)$ is a left R_1 submodule of $R = R_n$, and using Theorem 3.9 (7) as well as Theorem 3.7 (2) we get that $g - g(a) \in I_n$, so $f(g - g(a)) \in I_n$ and hence $fg - f(T_a)(g(a)) \in I_n$, as required.

Finally, note that working with I_n instead of I, we avoid the problem of having points that are zeros of every polynomial in the ring $R = A[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$.

4. The set of zeros and interpolation

In this section, we will assume that the base ring $A = K$ is a division ring.

If $\Sigma \subseteq K^n$, then we can consider the subset of the following ring

$$R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n],$$

given by

$$I(\Sigma) = \{f(t_1, \ldots, t_n) \in R \mid f(\sigma) = 0 \text{ for all } \sigma \in \Sigma\}.$$

And, on the other hand, to $J \subset R$, we attach the following subset

$$V(J) = \{a = (a_1, \ldots, a_n) \in K^n \mid f(a) = 0 \text{ for all } f \in J\}.$$

A subset $\Sigma \subseteq K^n$ is said to be *algebraic* if there exists $f \in R$ such that $f(\Sigma) = 0$, i.e., if $I(\Sigma) \neq 0$. Let us remark that, in general, $I(\Sigma)$ is an additive subset of R, but is not a left ideal. Nevertheless, the following lemma shows many similarities with classical algebraic geometry.

Lemma 4.1. *With the above notations, we have the following statements:*

(1) *If $\Sigma_1 \subseteq \Sigma_2 \subseteq K^n$ then $I(\Sigma_2) \subseteq I(\Sigma_1) \subseteq R$.*

(2) *If $J_1 \subseteq J_2 \subseteq R$ then $V(J_1) \subseteq V(J_2) \subseteq K^n$.*

(3) *For any* $\Sigma \subseteq K^n$*, we have* $\Sigma \subseteq I(V(I(\Sigma)))$*.*
(4) *For any* $J \subseteq R$*, we have* $J \subseteq I(V(J))$*.*
(5) $I(\Sigma_1 \cup \Sigma_2) = I(\Sigma_1) \cap I(\Sigma_2)$*.*

For a subset $\Sigma \subset K^n$, we denote by $\overline{\Sigma}$ the set $V(I(\Sigma))$.

Examples 4.2. (a) Let us mention a fundamental difference with the classical algebraic geometry that appears even in dimension 1, i.e., while working with $R = K[t;\sigma,\delta]$. Consider the algebraic set $\Sigma = \{a, b\} \subset K$ such that $b = a^x = \sigma(x)ax^{-1} + \delta x x^{-1}$ for some nonzero $x \in K$. It is easy to check that the polynomial $p(t) = (t - a^{a-b})(t - b)$ is a generator of the (principal) left ideal $I(\Sigma)$. But $\overline{\Sigma}$ is exactly the sets of elements of the form $a^{\lambda + x\mu}$ with $\lambda, \mu \in C^{\sigma,\delta}(a)$. Of course, if K is commutative, $\sigma = id.$, and $\delta = 0$, then we get back the fact that $\overline{\Sigma} = \Sigma$.

(b) In dimension $n = 2$, let us compute $I(\{(a_1, a_2), (b_1, b_2)\})$. If $q(t_1, t_2) \in I(\{(a_1, a_2)\}) \cap I(\{b_1, b_2\})$, then we can write

$$q(t_1, t_2) = p_1(t_1)(t_1 - a_1) + p_2(t_1, t_2)(t_2 - a_2),$$

with $q(b_1, b_2) = 0$. A short computation shows that this last equation is equivalent to $p_1(b_1^x)x + p_2(b_1^y, b_2^y)y = 0$. So, denoting $x := b_1 - a_1$ and $y = b_2 - a_2$, we conclude that $I(\{(a_1, a_2), (b_1, b_2)\}) = \{p_1(t_1)(t_1 - a_1) + p_2(t_1, t_2)(t_2 - a_2) \in R \mid p_1(t_1)x + p_2(t_1, t_2)y \in R_1(t_1 - a_1) + R_2(t_2 - a_2)\}$.

(c) Any finite subset of K^n is algebraic.

As in the case of a single variable, we introduce the notions of P-basis and P-independence in the following definition.

Definition 4.3. *If* $\Sigma \subset K^n$ *is algebraic and* $\underline{a} \in K^n$*, we say that* $\underline{a}$ *is* P*-dependent on* Σ *if* $\underline{a} \in V(I(\Sigma))$*. An algebraic subset* $\Sigma \subset K^n$ *is called* P*-independent if for any* $s \in \Sigma$*, there exists* $P_s \in V(\Sigma \setminus \{s\})$ *such that* $P_s(s) \neq 0$*. A maximal* P*-independent subset* $B \subseteq \Sigma$ *is called a* P*-basis.*

These definitions are direct generalizations of the ones given in the case of one variable setting.

In addition, for a subset $\Sigma \subseteq K^n$, and $1 \leq i \leq n$, we define

$$\Sigma_i = \{a \in K \mid (a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n) \in \Sigma, \text{for some } a_j \in K\}.$$

Proposition 4.4. *If, for some* $1 \leq i \leq n$*,* Σ_i *is an* (σ, δ_i)*-algebraic set, then* Σ *is an algebraic set as well. Moreover, any* P*-basis for* Σ_i *will give rise to a* P*-basis for* Σ*.*

Proof. Assume Σ_i is a (σ_i, δ_i)-algebraic set. This means that there exists a polynomial $f_i(t_i) \in K[t_i; \sigma, \delta_i]$ such that $f_i(\Sigma_i) = 0$. The existence of

P-basis in the univariate case is a well-known fact, and hence we can find $\{s_1, \ldots, s_r\} \subseteq \Sigma_i$ that is a P-basis for Σ_i. In particular, this subset is (σ_i, δ_i) P-independent. If, for $1 \le j \le r$, $\underline{a}_j \in \Sigma$ are such that $(\underline{a}_j)_i = s_j$, we have that for any polynomial f from $K[t_i; \sigma_i, \delta_i]$, $f(\underline{a}_j) = f(s_j)$. This quickly gives the conclusion that the set $\{\underline{a}_1, \ldots, \underline{a}_r\} \subset \Sigma$ is P-independent. The fact that the set $\{\underline{a}_1, \ldots, \underline{a}_r\} \subset \Sigma$ is a P-basis is clear since any polynomial from $K[t_i; \sigma_i, \delta_i]$ annihilating $\{s_1, \ldots, s_r\} \subseteq \Sigma_i$ will also annihilate Σ_i, and hence Σ. This finishes the proof. □

Of course, the converse of this proposition is untrue, in other words, there exist subsets Σ of K^n that are algebraic but none of the Σ_i, $1 \le i \le n$ is algebraic.

Lemma 4.5. *Let $\Sigma \subset K^n$ be a P-independent set. Then, for any $1 \le i \le n$, the set $\Sigma_i \subset K$ of i-th coordinates of elements of Σ is P-independent with respect to (σ_i, δ_i).*

We first recall the classical commutative setting of the elementary interpolation (so $K = k$ is commutative, $\sigma = id., \delta = 0$, and $n = 1$): for a finite subset $\Sigma = \{a_1, \ldots, a_l\} \subset K$ of distinct points and any set $\{b_1, \ldots, b_n\} \subset K$, there exists a monic polynomial $p(X) \in k[X]$ such that, for any $i = 1, \ldots, n$, we have $p(a_i) = b_i$. The analogue of the fact that the points are distinct will be here the fact that the points are P-independent. The case when $n = 1$ was treated in different papers, refer to [8] and [6] for more information.

Theorem 4.6. *Consider two finite subsets $\Sigma = \{\underline{a_1}, \ldots, \underline{a_l}\} \subset K^n$ and $\{b_1, \ldots, b_l\} \subset K$. Suppose that Σ is P-independent. Then there exists a monic polynomial $p \in R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \cdots [t_n; \sigma_n, \delta_n]$ such that $p(\underline{a_i}) = b_i$ for each $i = 1, \ldots, l$.*

Proof. Since Σ is P-independent, we know that, for any $1 \le i \le l$, there exists a polynomial $p_i \in R$ such that $p_i(\underline{a}_j) = 0$ if $i \ne j$ and $p_i(\underline{a}_i) \ne 0$. By scaling we may assume that $p_i(a_i) = 1$. The polynomial $p = \sum_{i=1}^{l} b_i p_i$ is the desired polynomial. □

5. Multivariate Ore extensions

This short section is concerned with a construction of a noncommutative polynomial ring that is essentially due to U. Martínez-Peñas and F. R. Kschischang [12]. We slightly extend the context by considering a general ring for the coefficients. The theory resembles very much the case of one variable and the introduction of PMT (see below) is, as usual, a useful tool.

Definition 5.1. *Consider a ring A, $t_1, \dots, t_n$ are n variables, $\sigma : A \to M_n(A)$ a ring homomorphism, and a sequence of n additive maps $\delta_1, \dots, \delta_n$. We denote by F the free monoid generated by the variables $\{t_1, \dots, t_n\}$ and by $S = A[\underline{t}; \sigma, \underline{\delta}]$ the set of polynomials of the form $\sum_{m \in F} \alpha_m m$, where $\alpha_m \in A$. On this set, we define the natural addition and we introduce a multiplication based on the multiplication in F (concatenation) and on the following commutation rules:*

$$\forall\, 1 \leq i \leq n,\ \forall\, a \in A, \quad t_i a = \sum_{j=1}^{n} \sigma(a)_{ij}(a) t_j + \delta_i(a).$$

For editorial reasons, for $a \in A$, we will write $\sigma_{ij}(a)$ instead of $\sigma(a)_{ij}$, viewing σ_{ij} as a map from A to A.

Remarks 5.2. (1) The associativity of the ring S leads to the following rule for the maps $\delta_1, \dots, \delta_n$:

$$\forall a, b \in A, \quad \delta_i(ab) = \sum_{j=1}^{n} \sigma_{ij}(a)\delta_j(b) + \delta_i(a)b.$$

In a compact form, this can be written as $\underline{\delta}(ab) = \sigma(a)\underline{\delta}(b) + \underline{\delta}(a)b$.

(2) The fact that σ and δ satisfy the above properties can also be summarized by asking that the map ϕ from A to the matrix ring $M_{n+1}(A)$ defined by

$$\phi : \ A \to M_{n+1}(A) \text{ with } a \mapsto \begin{pmatrix} \sigma(a) & \underline{\delta}(a) \\ 0 & a \end{pmatrix},$$

is a ring homomorphism.

(3) If V is a left S-module, then V is also a left A-module and, for any $1 \leq i \leq n$, the action of t_i on V must satisfy the following equality

$$t_i.a.v = (\sum_j \sigma_{ij}(a) t_j + \delta_i(a)).v.$$

This leads to maps $T_1, \dots, T_n \in \mathrm{End}(V, +)$ that satisfy

$$\forall\, 1 \leq i \leq n, T_i(a.v) = \sum_j \sigma_{ij}(a) T_j(v) + \delta_i(a).v.$$

In other words, writing $\underline{T} = (T_1, T_2, \dots, T_n)^t$ for a column of elements in $\mathrm{End}(V, +)$, we can write in a compact form as follows:

$$\underline{T}(a.v) = \sigma(a)\underline{T}(v) + \underline{\delta}(a)v.$$

A sequence of maps satisfying these equations will be called a $(\sigma, \underline{\delta})$-pseudo-multilinear transformation ($(\sigma, \underline{\delta})$)-PMT, for short) on V. For example, one can check that the sequence $\underline{\delta} = (\delta_1, \dots, \delta_n)$ is a PMT on A. What we just said is that there is a one-to-one correspondence between left modules over S and the set of PMTs over left A-modules.

As in the case of a single variable, the following map

$$\varphi : S \to \mathrm{End}(V, +) \text{ such that } \varphi(f(\underline{t})) = f(\underline{T}),$$

is a ring homomorphism.

(4) We define the evaluation of $f(\underline{t}) \in S = A[\underline{t}; \sigma, \underline{\delta}]$ at $(a_1, \ldots, a_n) \in A^n$, via the representative of $f(\underline{t}) + I \in S/I$ by an element of A, where I is the left ideal $I = S(t_1 - a_1) + S(t_2 - a_2) + \cdots + S(t_n - a_n)$. For example, if $n = 2$, then evaluating $t_1 t_2$ at (a_1, a_2) we get $\sigma_{11}(a_2)a_1 + \sigma_{12}(a_2)a_2 + \delta_1(a_2)$.

Since S/I is a left S-module, it gives rise to a $(\sigma, \underline{\delta})$-PMT on S/I given by the actions of t_i for $1 \leq i \leq n$. The elements of S/I are represented by an element of A so that the action of t_i on S/I can be described by

$$t_i.(x + I) = t_i x + I = \sum \sigma_{ij}(x)a_j + \delta_i(x).$$

The PMT attached to $(a_1, a_2, \ldots, a_n) \in A^n$ is $T_{\underline{a}} = (T_{a_1}, T_{a_2}, \ldots, T_{a_n})$ where, for $x \in A$ and $1 \leq i \leq n$, we have $T_{a_i}(x) = \sum_{j=1}^{n} \sigma_{ij}(x)a_j + \delta_i(x)$. As in the case of a single variable, the link between evaluation and PMT is given by the formula:

$$f(\underline{a}) = f(T_{\underline{a}})(1).$$

The proof of this formula is easily obtained by first reducing it to monomials and then proceeding by induction on the length of a monomial. The fact that the map φ in (3) above is a ring homomorphism, then immediately leads to the product formula $(fg)(\underline{a}) = f(T_{\underline{a}})g(\underline{a})$ for $f, g \in S$ and $a \in A$. In particular, if $g(\underline{t}) = x \in A$, then we have $(f.x)(\underline{a}) = f(T_{\underline{a}})(x)$. This shows the link between the kernel of $f(T_{\underline{a}})$ and the roots of $f(\underline{t})$. One can readily check that $T_{\underline{a}}$ is a right linear map over the subring given by $C^{\sigma,\underline{\delta}}(a) := \{x \in A \mid T_{\underline{a}}(x) = \underline{a}x\}$. In the case when $A = K$ is a division ring, $C^{\sigma,\underline{\delta}}(a)$ is a division ring isomorphic to $\mathrm{End}_S(S/I)$, where $I = \sum_i S(t_i - a_i)$. Some information can be obtained on the roots of a multivariate polynomial by fixing all the variables but one.

(5) Since the map φ associated with a PMT is a ring homomorphism from S to $\mathrm{End}(V, +)$, when φ is not injective, the multivariate polynomial ring is not simple. The simplicity is thus related to some algebraicity of a PMT, exactly as in the case of a single variable. We will not go deeper into this subject. MR4394033 (sent May 2022) Kim, Nam Kyun et al., Annihilating properties of ideals generated by coefficients of polynomials and power series. Internat. J. Algebra Comput. 32 (2022), no. 2 6) As a final remark let us mention that, if the division ring K is finite-dimensional over its center F and

σ is F-linear, the Skolem Noether theorem shows that σ is diagonalizable. In other words, there exist an invertible matrix U and a set of n automorphisms of K, say $\sigma_1, \ldots, \sigma_n$, such that $\sigma = Inn_U \circ diag(\sigma_1, \ldots, \sigma_n)$. In this situation, the multivariate extension $S = K[\underline{t}; \sigma, \underline{\delta}]$ contains the Ore extensions $S_i = K[t_i; \sigma_i, \delta_i]$. In the iterated Ore extension this last fact is always true.

Acknowledgement

This work was partially done while the first author was staying in Universidade de São Paulo (Brazil) under the grant FAPESP, Proc. 2022/13508-1. He would like to thank Prof. César Polcino Milies and the algebra group of this institution for their warm welcome and for the many nice discussions we had.

References

[1] N. Bennenni and A. Leroy, *Evaluation of iterated Ore polynomials and skew Reed-Muller codes*, Contemp. Math. Vol. **785** (2023).

[2] D. Boucher and F. Ulmer, *Coding with skew polynomial rings,* J. Symbolic Comput. **44** (2009), no. 12, 1644–1656.

[3] M. Boulagouaz and A. Leroy, *(σ, δ)-codes*, Advances in Mathematics of communications, Vol. **7** (4) (2013) 463-474.

[4] J. Delenclos and A. Leroy, *Noncommutative symmetric functions and W-polynomials,* J. Algebra Appl. **6** (2007), no. 5, 815–837.

[5] N. Jacobson, *Pseudo-linear transformations,* Ann. of Math. (2) **38** (1937), no. 2, 484–507.

[6] T. Y. Lam and A. Leroy, *Algebraic conjugacy classes and skew polynomial rings*, Perspectives in ring theory (Antwerp, 1987), 153–203, NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci., 233, Kluwer Acad. Publ., Dordrecht, 1988.

[7] T. Y. Lam and A. Leroy, *Principal one-sided ideals in Ore polynomial rings,* Algebra and its applications (Athens, OH, 1999), 333–352, Contemp. Math., **259**, Amer. Math. Soc., Providence, RI, 2000.

[8] T. Y. Lam and A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), no. 2, 308–336.

[9] T. Y. Lam, A. Leroy, and A. Ozturk, *Wedderburn polynomials over division rings. II,* Noncommutative rings, group rings, diagram algebras and their applications, 73–98, Contemp. Math., **456**, Amer. Math. Soc., Providence, RI, 2008.

[10] A. Leroy, *Noncommutative polynomial maps,* J. Algebra Appl. **11** (2012), no. 4, 1250076, 16 pp.

[11] A. Leroy and A.Ozturk, *Algebraic and F-independent sets in 2-firs,* Comm. Algebra **32** (2004), no. 5, 1763–1792.

[12] U. Martínez-Peñas and F. R. Kschischang, *Evaluation and interpolation over multivariate skew polynomial rings,* J. Algebra **525** (2019), 111–139.

[13] D. E. Muller, *Application of Boolean algebra to switching circuit design and to error detection,* Transactions of the I.R.E. Professional Group on Electronic Computers, vol. **3** (1954), no. 3, 6–12.

[14] O. Ore, *Theory of noncommutative polynomials*, Ann. of Math. (2) **34** (1933), 480-508.

Univ. Artois, UR 2462, Laboratoire de Mathématique de Lens (LML), F-62300 Lens, France, email: andre.leroy@univ-artois.fr

Univ. Artois, UR 2462, Laboratoire de Mathématique de Lens (LML), F-62300 Lens, France, https://orcid.org/0000-0003-1073-1934, email: m_nasernejad@yahoo.com