Introduction to Noncommutative Polynomial Maps

André Leroy
Université d'Artois, Faculté Jean Perrin
Rue Jean Souvraz 62 307 Lens, France

Abstract

These notes give a short introduction to Ore extensions, polynomial maps and pseudo-linear transformations. They are based on talks given in King Abdulaziz University, Jeddah. They were written during a very pleasant stay in the MECAA center in March 2011.

INTRODUCTION

Since their formal introduction in the 1930's by Oystein Ore, skew polynomial rings and their iterated constructions have been the subject of many studies. It quickly appeared that their "manageable" noncommutativity offers a very good tool for constructing counter-examples. For instance:

(1) They were used by Bergman to produce a left but not right primitive ring.

(2) They enable Cohn and Schofield to construct division rings having different left and right dimension over some subdivision ring.

After their introduction by Ore, the structure theory of skew polynomial rings was further developed by N. Jacobson, S.A. Amitsur, P.M. Cohn, G. Cauchon, T.Y.Lam, A. Leroy, J. Matczuk and many many others. Ore extensions are also an essential tool in the theory of quantum groups. Many quantum groups can be presented using iterated Ore extensions. In this case one powerful tool is what is called the "erasing of derivations" process due to G. Cauchon. (Cf. [Ca]).

Ore extensions have both a "ring theoretical aspect": characterization of simplicity, description of prime ideals, passage of properties from the base ring to the skew polynomial rings (often with the aim of giving examples of a non left/right symmetryc behaviour) and a more "arithmetical aspect" mainly related to the factorization of polynomials, computation of the roots and also in relation with special matrices, in particular Vandermonde and Wronskian matrices. The link between these two aspects is given, in particular, by special types of polynomial

(invariant, semmi-invariant, cv, irreducible, Wedderburn, fully reducible,...). Another important feature of the Ore extensions is their relation with differential equation and operator theory. This was the origin of their study even before their formal definition given by Ore.

1 Skew polynomial rings

Let us try to construct a noncommutative polynomial ring with "reasonable" behaviour. Let A be a ring with unity 1. As for commutative polynomial rings we try to give the left A-module $S := A^{\oplus\mathbb{N}}$ a structure of ring. Let $a = (a_0, \dots, a_n, 0, \dots)$, $b = (b_0, \dots, b_l, 0, \dots, 0, \dots) \in S$. We need to define the product ab. We put: $e_0 = (1, 0, 0 \dots, 0 \dots), e_1 := (0, 1, 0 \dots, 0 \dots), e_2 := (0, 0, 1, 0 \dots, 0 \dots), \dots$. So any element of S is a finite sum $\sum a_i e_i$ where $a_i \in A$. We require that

a) $e_i e_j = e_{i+j}$ (for $i, j \in \mathbb{N}$).

b) $e_1(re_0) \in Ae_0 \oplus Ae_1$, for any $r \in A$.

Since $e_i = e_1^i$, we can write $ab = \sum_{i,j} a_i e_i b_j e_j = \sum_{i,j} a_i e_1^i b_j e_j$. Hence to define a multiplication on S respecting the left A-module structure of S and satisfying our constraint a) we must define $e_1 b$ since we have $e_1 b = e_1 \sum b_j e_j = e_1(bje_0)e_j$, we finally only need to define the product $e_1(re_0)$. The constraint b) above gives that there should exist maps σ, δ from A to A such that $e_1(re_0) = \delta(r)e_0 + \sigma(r)e_1$. Since $e_1((r+s)e_0) = e_1(re_0) + e_1(se_0)$ we get that $\sigma, \delta \in End(R, +)$. On the other hand the associativity of the multiplication in S gives that $\delta(rs)e_0 + \sigma(rs)e_1 = e_1(rse_0) = e_1((re_0)(se_0)) = (e_1(re_0))(se_0) = (\delta(r)e_0 + \sigma(r)e_1)(se_0) = \delta(r)se_0 + \sigma(r)(e_1(se_0)) = (\delta(r)s + \sigma(r)\delta(s))e_0 + \sigma(r)\sigma(s)e_1$. This gives that, for any $r, s \in A$, we have:$\sigma(rs) = \sigma(r)\sigma(s)$ and $\delta(rs) = \sigma(r)\delta(s) + \delta(r)s$. Let us now remark that if we put $t := e_1$, the elements of S are polynomials in t i.e. finite sums $\sum a_i t^i$, $a_i \in R$ and the product is defined by the relation $tr = \sigma(r)t + \delta(r)$, for $r \in A$.

We can now formally introduce the following definitions:

Definitions 1.1. Let A be a ring with 1 and σ a ring endomorphism of A.

(a) An additive map $\delta \in End(A, +)$ is a σ-derivation if, for any $a, b \in R$, we have :

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

(b) The elements of the skew polynomial ring $R = A[t; \sigma, \delta]$ are polynomials $\sum a_i t^i$. They are added as ordinary polynomials and the multiplication is based on the commutation law

$$ta = \sigma(a)t + \delta(a) \; for \; a \in A.$$

(c) The degree of a nonzero polynomial $f = a_0 + a_1t + a_2t^2 + \dots a_nt^n \in R$ is defined to be $\deg(f) = max\{i|a_i \neq 0\}$ and we put, as usual, $\deg(0) = -\infty$.

The paragraph preceding the above definition introduces the σ-derivation in a fairly natural way. Another way will be presented later while discussing pseudo-linear transformations. Let us give a few standard examples:

Examples 1.2. (1) If $\sigma = id.$ and $\delta = 0$ we have $A[t;\sigma,\delta] = A[t]$, the usual polynomial ring in a commuting variable. If only $\sigma = id.$ but $\delta \neq 0$ we denote $A[t;id.,\delta]$ as $A[t;\delta]$ and speak of a polynomial ring of derivation type. On the other hand if $\delta = 0$ but $\sigma \neq id.$ we write $A[t;\sigma,\delta]$ as $A[t;\sigma]$ and refer to it as a polynomial ring of endomorphism type.

(2) $\mathbb{C}[t;\sigma,0]$ where σ is the usual conjugation in the complex number. Notice that since $\sigma^2 = id.$, we can check that t^2 is a central polynomial.

(3) Let k be field, $R = k[x][t;id.;d/dx]$. This is the weyl algebra. Notice the relation $tx - xt = 1$. If char$k = 0$ the Weyl algebra is a simple ring. In contrast if char$k = p > 0$ then t^p and x^p are central elements.

(4) Let $A := k[x]$ be the polynomial ring over a field k and σ the k- endomorphism of A defined by $\sigma(x) = x^2$. Notice that the polynomial ring $S := A[t;\sigma]$ is a domain (since σ is injective and $k[x]$ is a domain) but it is not a right Ore domain indeed we have $xS \cap tS = 0$. In particular, S is not right noetherian. (consider the ascending chain $xS \subset xS + txS \subset xS + txS + t^2xS \subset \dots$). The problem remains even if we localize the base ring, extend σ and consider $T := k(x)[t;\sigma]$. T is then a left principal left Ore domain but is not right noetherian. Notice that this gives an easy example of a ring with left uniform dimension equal to 1 but with infinite right uniform dimension.

(5) For $a \in A$ we define the inner σ-derivation induced by a (denoted $d_{a,\sigma}$) in the following way: for $r \in A$, $d_a(r) := ar - \sigma(r)a$. Let us remark that $A[t;\sigma,d_{a,\sigma}] = A[t-a,\sigma]$ and similarly for an inner automorphism induced by $a \in U(A)$ denoted by I_a and defined by $I_a(x) = xax^{-1}$ for $x \in A$: $A[t;I_a] = A[a^{-1}t]$.

(6) Let $0 \neq q \in k$ where k is a field and let I_q be the two- sided ideal of the free algebra $k\{x,y\}$ generated by the element $yxqxy$. We define the *quantum plane* as the quotient-algebra $k_q[x,y] := k\{x,y\}/I_q$. Alternatively this k-algebra can be seen as $k[x][t;\sigma]$ where σ is the k-endomorphism defined by $\sigma(x) = qx$. It is easy to check that, for $i,j > 0$, $y'^jx^i = q^{ij}x^iy^j$. Let us mention first of all that this algebra is noetherian (Cf. the properties mentioned just after these examples). Arithmetic can be developed in this

algebra resembling very much to the classical one. For instance we can define the following

1. For $n > 0$ let us define $(n)_q = 1 + q + \cdots + q^{n-1} = \frac{q^n-1}{q-1}$.
2. For $n > 0$, $(n)!_q = (1)_q(2)_q \dots (n)_q = \frac{(q-1)(q^2-1)\dots(q^n-1}{(q-1)^n}$ while $(0)!_q = 1$ (of course $(n)!_q$ is called the q factorial of n).
3. For $0 \leq k \leq n$ we put $\binom{n}{k}_q := \frac{(n)!_q}{(k)!_q(n-k)!_q}$.

Using these definitions we can now state the following:

a) $\binom{n}{k}_q$ is a polynomial in q with integer coefficients.
b) $\binom{n}{k}_q = \binom{n}{n-k}_q$.
c) $\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k\binom{n-1}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q$.
d) If $yx = qxy$ then $(x+y)^n = \sum_{k=0}^n \binom{n}{k}_q x^k y^{n-k}$.

The quantum plane is a member of a huge family of algebras called the quantum groups. A big number of these algebras can be built as iterated Ore extensions.

(7) Let p be a prime number, $n \in \mathbb{N}$ and $q = p^n$. Consider $R = \mathbb{F}_q$ a finite field and θ the Frobenius automorphism. We can of course look at the skew polynomial ring $R[t;\theta]$. this kind of Ore extensions have been used recenntly in the context of noncommutative codes.

The following proposition gives some of the most basic properties of an Ore extension. The proofs of these statements can be found in many books (Cf. [Co], [La])

Proposition 1.3. *Let $R = A[t;\sigma,\delta]$ be a skew polynomial ring over a ring A.*

(a) If A is a domain and σ is injective then R is a domain as well.

(b) If $A = K$ is a division ring then R is a left principal ideal domain. Hence it is a left Ore domain and admits a left division ring of quotients denoted by $K(t;\sigma,\delta)$. R is also right noetherian (and then in fact right principal) if and only if σ is an automorphism.

(c) If $p(t) \in R$ is a monic polynomial then for any polynomial $f(t) \in R$ there exists $q(t), r(t) \in R$ such that $f(t) = p(t)q(t) + r(t)$ and $deg(r(t)) < deg(p(t))$.

(d) If A is a division ring then R is a unique factorization domain i.e. every element f of R can be expressed as a product of irreducible polynomials and if $f = p_1 \cdots p_n = q_1 \cdots q_m$ are two such decompositions then $m = n$ and there exists a permutation $\pi \in S_n$ such that, for every $1 \leq i \leq n$, there is an isomorphism $R/Rp_i \cong R/Rq_{\pi(i)}$.

When the base ring $A = K$ is a division ring, the study of the ideal structure of the ring of polynomial rings is helped by the euclidean algorithm. Let us mention, for example, the criterion for simplicity. We need the following definition:

Definitions 1.4. a) Let $p(t) \in R = A[t; \sigma, \delta]$, we say that $p(t)$ is a right semi-invariant polynomial if for every $x \in A$ there exists $y \in A$ such that $p(t)x = yp(t)$. If additionally $p(t)t = (bt + a)p(t)$ for some $a, b \in A$ then we say that the polynomial $p(t)$ is right invariant. We often will drop the adjective right and speak about semi-invariant and invariant polynomials.

b) A σ-derivation δ of A is called quasi-algebraic if there exist an endomorphism θ of A and elements $0 \neq a_n, a_{n-1}, a_{n-2}, \ldots, a_0, b \in A$ with $n > 0$, such that

$$\sum_{i=1}^{n} a_i \delta^i(x) + b\delta_{a_0,\theta}(x) = 0 \text{ for all } x \in A$$

When $A = K$ is a division ring these polynomials were used to characterize when the extension $R = K[t; \sigma, \delta]$ is simple. Let us sum up here a few of these results: In particular, the following is proved in [LLLM]: let $p(t) \in R$ be a nonconstant monic semi-invariant polynomial of minimal degree. Then
(1) if σ is not an automorphism or if σ is an automorphism of infinite inner order, $p(t)$ is already invariant.
(2) call $J = \{h(t) \in R\colon\ h(t) \cdot R \subseteq R \cdot p(t)\}$ the "bound" of $R \cdot p(t)$ (it is the largest 2-sided ideal of R contained in $R \cdot p(t)$). J is given by $R \cdot p(t)^s$ for some integer $s \leq \deg(p(t))$. If σ is not an inner automorphism, then $p(t)^s$ is an invariant polynomial of minimal degree in R. If $p(t)$ is not necessarily of minimal degree, then: if $\sigma(K)$ has finite right codimension m in K, $J = R \cdot f(t)$ where $f(t)$ is invariant of degree $\leq n(1 + m + \cdots + m^{n-1})$ where $n = \deg(p(t))$.

Let us point out explicitly that the above shows that R is not simple if and only if there exists a nonconstant semi-invariant polynomial.

In the same paper (loc. cit.) these results are extended to the case when K is a simple ring and S is an automorphism.
The next step is to consider the case of a prime ring A and the Ore extension $R = A[t; \sigma, \delta]$. For studying this case it is necessary to extend the base ring and consider the Martidale ring of quotients. Let us recall that $Q_l = \lim_{I \in \mathcal{F}} Hom({}_A I, {}_A A)$, where $\mathcal{F}$ is the filter of all nonzero two-sided ideals of A. T is the subring of Q_l, consisting of elements $q \in Q_l$ for which there exists a non-zero two-sided ideal I of A such that $ql \subset A$. T can also be seen as the set of elements q in the maximal quotient ring of A such that there exists a nonzero two sided ideal I of A for which $Iq \subset A$ and $qI \subset A$. Using these notations we obtain (Cf. [LM]) the following basic proposition:

Proposition 1.5. *For any non-zero ideal I of $A[t; \sigma, \delta]$ there exists a unique monic invariant polynomial $f_I(t) \in T[t; \sigma, \delta]$ having the following properties:*

(1) $degf(t) = min\{degf(t) \mid f(t) \in I \setminus 0\} = n$ *and every polynomial* $g(t) \in I$ *of degree* n *can be written in the form* $af(t)$ *for some* $a \in A$

(2) $I \subseteq T[t;\sigma,\delta]f(t)$.

Let us also mention that there is a strong link between the existence of some specific polynomials and the ideal structure of the Ore extension (eventually after some localization). In particular, CV polynomials, semi-invariant and invariant polynomials when they exist give these links.

2 Polynomial maps and pseudo-linear transformations

We start this section with the "obvious definition" of the polynomial map attached to an element of an Ore extension:

Definition 2.1. For any $f(t) \in R = A[t;\sigma,\delta]$ and $a \in A$ there exists a unique polynomial $q(t)$ and a unique element $r \in A$ such that $f(t) = q(t)(t-a) + r$. With these notations, the polynomial map associated to $f(t) \in R$ is the map $f : A \longrightarrow A$ defined by $f(a) := r$.

For $i \geq 0$, we denote N_i the polynomial map determined by t^i.

Let us first give some examples.

Examples 2.2. 1. If $\sigma = id.$ and $\delta = 0$ we get back the standard way of evaluating a polynomial. It should be noted though, that, since R is not commutative, we have to specify that this is a right polynomial map. For instance, although for $c \in A$ $f(t) = ct = tc \in R = A[t]$, the polynomial map we consider here is the map $f : A \longrightarrow A$ defined by $f(a) = ca$, for any $a \in A$.

2. The polynomial map associated to t is always the identity (i.e. $N_1 = id.$). The polynomial map associated to a polynomial $c_0 \in A$ of degree zero is always the constant map determined by c_0.

3. If k is a field the number of roots of polynomial $f(t) \in k[x]$ is bounded by its degree $\deg(f(x))$. This is not true if k is replaced by a ring even commutative: consider for instance $(x-2)(x-1) \in \frac{\mathbb{Z}}{4\mathbb{Z}}[x]$. In a noncommutative setting this can be badly wrong even over a division ring: the polynomial $t^2+1 \in \mathbb{H}[t]$ has infinitely many right roots given by all the conjugates of i.

4. A ring A is said to have the finite zero property if for any $f(x) \in A[x]$, the number of roots of $f(x)$ in A is finite. (Cf. [F]).

5. The number of roots of polynomials over matrix rings over the complex numbers has been studied by Wilson and his students. For instance it is proved (Cf. [S]) that if a polynomial $p(t) \in M_2(\mathbb{C})[t]$ of degree n has more than $\binom{2}{2n}$ then it has infinitely many roots.

6. A little care is needed while thinking about (right) roots. For instance, if $\mathbb{H}$ stands for the skew field of quaternions over $\mathbb{R}$, in $\mathbb{H}[t]$ the polynomial $f(t) := (t-j)(t-i) = t^2-(i+j)t+ji$ is such that $f(j) = j^2-(i+j)j+ji = 2ji \neq 0$. This means that j is not a *right* root of $f(t)$. In fact, i is the only (right) root of $(t-j)(t-i)$. This phenomenon will be explained and generalized after the introduction of the so-called product formula

7. If $\delta = 0$, it is easy to check that, for $i > 0$ the polynomial map associated to $f(t) = t^i \in K[t;\sigma]$ is the i^{th}-norm i.e. $N_i(a) = \sigma^{i-1}(a)\dots\sigma(a)a$, and hence if $f(t) = \sum_{i=0}^n c_i t^i \in K[t;\sigma]$, we have $f(a) = \sum_{i=0}^n c_i\sigma^{i-1}(a)\dots\sigma(a)a$.

8. Let us denote "$-$" the conjugation in the field of complex numbers $\mathbb{C}$. The polynomial $t^2 - i \in \mathbb{C}[t;-]$ has no (right) root and hence it is irreducible. This shows that there exist irreducible polynomials of degree 2 in $\mathbb{C}[t;-]$. Of course, this contrasts sharply with the usual untwisted polynomial ring $\mathbb{C}[t]$. Later we will describe all the irreducible polynomials of $\mathbb{C}[t;-]$.

9. If $\sigma = id.$ one can check that $N_2(a) = t^2(a) = a^2 + \delta(a)$ and $N_3(a) = a^3 + 2\delta(a)a + a\delta(a) + \delta^2(a)$. Notice that if $\delta(a)$ commutes with a and characteristic of K is 3 then $N_3(a) = a^3 + \delta^2(a)$.

10. Let $\mathbb{F}_q$ denote the finite field with $q = p^n$ elements (p is prime). Consider θ the Frobenius automorphism on $\mathbb{F}_q$ defined by $\theta(x) = x^p$ for $x \in \mathbb{F}_q$. As in quantum theory let us write, for $n \geq 1$, $[n]$ for $\frac{p^n-1}{p-1}$ and put $[0] = 0$. It is then easy to check that, for $f(t) := \sum_{i=0}^m a_i t^i \in \mathbb{F}_q[t;\theta]$ and $b \in \mathbb{F}_q$, one has $f(b) = \sum_{i=0}^m a_i b^{[i]}$.

We now introduce the notion of a pseudo-linear transformation. This notion appears naturally while looking at modules over an Ore extensions and it will be very useful in respect with polynomial maps.

Definition 2.3. Let A be a ring, σ an endomorphism of A and δ a σ-derivation of A. Let also V stand for a left A-module.

An additive map $T : V \longrightarrow V$ such that, for $\alpha \in A$ and $v \in V$,

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

is called a (σ,δ) pseudo-linear transformation (or a (σ,δ)-PLT, for short).

In case V is a finite dimensional vector space and σ is an automorphism, the pseudo-linear transformations were introduced in [Ja_2].

We will see that PLT's are very useful tools why studying polynomial maps over rings. Even over division rings they will not only explain some features of the structure of roots of polynomial maps but also they seem required if we try to define polynomial maps of several noncommutative variables (even over division rings).

The (σ, δ)-PLT's appear naturally in the context of modules over an Ore extension $A[t; \sigma, \delta]$. This is explained in the next proposition.

Proposition 2.4. *Let A be a ring $\sigma \in End(A)$ and δ a σ-derivation of A. For an additive group $(V, +)$ the following conditions are equivalent:*

(i) V is a left $R = A[t; \sigma, \delta]$-module;

(ii) V is a left A-module and there exists a (σ, δ) pseudo-linear transformation $T : V \longrightarrow V$;

(iii) There exists a ring homomorphism $\Lambda : R \longrightarrow End(V, +)$.

Proof. The proofs are straightforward, let us nevertheless mention that, for the implication $(i) \Rightarrow (ii)$, the (σ, δ)-PLT on V is given by the left multiplication by t. □

The link just mentioned between pseudo-linear transformations and skew polynomial rings helps the study of the structure of such rings. For instance they permit (Cf. [L]) to determine when $R = K[t; \sigma, \delta]$ (K a division ring,$\sigma \in End(K), \delta$ a σ-derivation) is left or right primitive. Various statements can be shown to be equivalent to left primitivity of R (cf. [L]). One is that there exists a non-algebraic (σ, δ) pseudo-linear transformation of a finite- dimensional left K-vector space and another is that, for some n, there exists an $n \times n$ matrix A over K such that $f(A) \neq 0$ for all $f \in R$ with $fR = Rf$. This leads to the equivalence of the following statements:

1. R is left primitive.
2. R a right primitive.
3. R is simple or S^l is not an inner automorphism for any $l > 0$ or the polynomial ring $K[x]$ is primitive.

Let T be a (σ, δ)-PLT defined on an A-module V. Using the above notations, we define, for $f(t) = \sum_{i=0}^{n} a_i t^i \in R$, and T a (σ, δ)-PLT $f(T) := \Lambda(f(t)) = \sum_{i=0}^{n} a_i T^i \in End(V, +)$. We can now state the following corollary. It will be intensively used in these notes.

Corollary 2.5. *For any $f, g \in R = A[t; \sigma, \delta]$ and any pseudo-linear transformation T we have: $(fg)(T) = f(T)g(T)$.*

Examples 2.6. (1) If $\sigma = id.$ and $\delta = 0$, a pseudo-linear map is an endomorphism of left A-modules. If $\delta = 0$, a pseudo-linear map is usually called a (σ) semi-linear transformation.

(2) Let V be a free left A-module with basis $\beta = \{e_1, \ldots, e_n\}$ and let $T : V \longrightarrow V$ be a (σ, δ)-PLT. This gives rise to a (σ, δ)-PLT on the left A-module A^n as follows: first define $C = (c_{ij}) \in M_n(A)$ by $T(e_i) = \sum_i^n c_{ij}e_j$. and extend component-wise σ and δ to the ring A^n. We then define a (σ, δ)-PLT on A^n by $T_C(\underline{v}) = \sigma(\underline{v})C + \delta(\underline{v})$, for $\underline{v} \in A^n$. In particular, for $n = 1$ and $a \in A$, the map $T_a : A \longrightarrow A$ given by $T_a(x) = \sigma(x)a + \delta(x)$ is a (σ, δ)-PLT. T_a will be called the (σ, δ)-PLT induced by $a \in A$. Notice that $T_0 = \delta$ and $T_1 = \sigma + \delta$.

(3) It is well-known and easy to check that, extending σ and δ from a ring A to $M_n(A)$ component-wise, gives an endomorphism, still denoted σ, and a σ-derivation also denoted δ on the ring $M_n(A)$. For $n, l \in \mathbb{N}$ we may also extend component-wise σ and δ to the additive group $V := M_{n\times l}(A)$. Let us denote these maps by S and D respectively. Then S is a σ semi-linear map and D is a (σ, δ)-PLT of the left $M_n(A)$-module V. This generalizes the fact, mentioned in example (2) above, that δ itself is a pseudo-linear transformation on A.

(4) Let ${}_AV_B$ be an (A, B)-bimodule and suppose that σ and δ are an endomorphism and a σ-derivation on A, respectively. If S is a σ semi-linear map and T is a (σ, δ) PLT on ${}_AV$, then for any $b \in B$, the map T_b defined by $T_b(v) = S(v)b + T(v)$, for $v \in V$, is a (σ, δ) pseudo-linear map on V.

(5) Using both Examples (3) and (4) above, we obtain a (σ, δ) pseudo-linear transformation on the set of rectangular matrices $V := M_{n\times l}(A)$ (considered as an $(M_n(A), M_l(A))$-bimodule) by choosing a square matrix $b \in M_l(A)$ and putting $T_b(v) = S(v)b + D(v)$ where S and D are defined component-wise as in Example (3) and $v \in V$. This construction will be used in Proposition 2.8.

Remarks 2.7. (1) Let us mention that the composition of pseudo-linear transformations is usually not a pseudo-linear transformation. Indeed, let $T : V \longrightarrow V$ be a (σ, δ)-PLT. For $a \in A$, $v \in V$ and $n \geq 0$, we have $T^n(av) = \sum_{i=0}^n f_i^n(a)T^i(v)$, where f_i^n is the sum of all words in σ and δ with i letters σ and $n - i$ letters δ.

(2) Let σ, τ be endomorphisms of a ring A. Let also γ be a map from A to A. It is easy to see that the set

$$E(\sigma,\gamma,\tau) := \{\begin{pmatrix} \sigma(r) & \gamma(r) \\ 0 & \tau(r) \end{pmatrix} \mid r \in A\}$$

is a subring of the upper triangular matrix ring, $UT_2(A)$ if and only if $\gamma \in End(A,+)$ and satisfies $\gamma(rs) = \sigma(r)\gamma(s) + \gamma(r)\tau(s)$, for $r, s \in A$. Such a map is called a (σ,τ)-derivation. If $\tau = id.$ we get back our usual σ-derivation. We have seen that a σ-derivation, say δ, can be seen as a special case of a pseudo-linear transformation. It is natural to expect that the pseudo-linear transformations can also be presented using triangular matrices as above. This is indeed the case, we will then obtain just as above a small generalization of a (σ,δ)-PLT. Let V be a left A- module and consider three maps $\varphi_1, \varphi_2, \varphi_3$ from V to V. The subset

$$V(\varphi_1,\varphi_2,\varphi_3) := \{\begin{pmatrix} \varphi_1(v) & \varphi_2(v) \\ 0 & \varphi_3(v) \end{pmatrix} \mid v \in V\} \subset UT_2(V) := \begin{pmatrix} V & V \\ 0 & V \end{pmatrix}$$

is a left $UT_2(A)$-module of $UT_2(V)$ if and only if the maps φ_i, $i = 1, 2, 3$ are A-linear maps. Now, if we look at $UT_2(V)$ as a left $E := E(\sigma,\gamma,\tau)$-module then $V(\varphi_1,\varphi_2,\varphi_3)$ is a sub E-module of $UT_2(V)$ if and only if φ_1 and φ_3 are respectively a σ and a τ-semi linear transformations on V, and φ_2 is an additive map that satisfies $\varphi_2(rv) = \sigma(r)\varphi_2(v) + \gamma(r)\varphi_3(v)$. If $\tau = id._A$, γ is a σ-derivation and if moreover $\varphi_3 = id._V$ then φ_2 is a (σ,γ)- PLT. Of course, we can also consider the case when $\sigma = id.|_R$ and $\varphi_1 = id._V$.

Let us now indicate explicitly the link between polynomial maps and pseudo-linear transformations. Since, for $a \in A$, the pseudo-linear transformation on A associated to the left R-module $V = R/R(t-a)$ is T_a (Cf. Example 2.6(2)). The equality $f(t).1_V = f(a) + R(t-a)$ leads to

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

For a left R-module V, we consider the standard $(R, End_R V)$-bimodule structure of V. In the proof of Theorem 2.4 we noticed that that T corresponds to the left multiplication by t on V. This implies that, for any $f(t) \in R$, $f(T)$ is a right $End_R(V)$-linear map defined on V. In particular, $\ker f(T)$ is a right $End_R(V)$ submodule of V. Considering $V = R/R(t-a)$ for $a \in A$, this module structure on $\ker(f(T_a))$ explains and generalizes some important properties of roots of polynomials obtained earlier (Cf. [LL$_1$], [LL$_2$], [LLO]), see Corollary 2.15 for more details). Let us describe the elements of $End_R(V)$ in case V is a free left A-module. We extend the maps σ and δ to matrices over A by letting them act on every entry.

Proposition 2.8. *For $i = 1, 2$, let T_i be a (σ, δ)-PLT defined on a free A-module V_i with basis β_i and dimension n_i. Suppose $\varphi \in Hom_A(V_1, V_2)$ is an A-module homomorphism. Let also $B \in M_{n_1 \times n_2}(A)$, $C_1 \in M_{n_1 \times n_1}(A)$ and $C_2 \in M_{n_2 \times n_2}(A)$ denote matrices representing φ, T_1 and T_2 respectively in the appropriate bases β_1 and β_2. Let ${}_RV_1$ and ${}_RV_2$ be the left R-module structures induced by T_1 and T_2, respectively. The following conditions are equivalent:*

(i) $\varphi \in Hom_R(V_1, V_2)$;

(ii) $\varphi T_1 = T_2 \varphi$;

(iii) $C_1 B = \sigma(B) C_2 + \delta(B)$;

(iv) $B \in \ker(T_{C_2} - L_{C_1})$ *where T_{C_2} (resp. L_{C_1}) stands for the pseudo-linear transformation (resp. the left multiplication) induced by C_2 (resp. C_1) on $M_{n_1 \times n_2}(A)$ considered as a left $M_{n_1}(A)$-module.*

Proof. $(i) \Leftrightarrow (ii)$. This is clear since, for $i = 1, 2$, T_i corresponds to the left action of t on V_i.
$(ii) \Leftrightarrow (iii)$. Let us put $\beta_1 := \{e_1, \ldots, e_{n_1}\}$, $\beta_2 := \{f_1, \ldots, f_{n_2}\}$, $C_1 = (c_{ij}^{(1)})$, $C_2 = (c_{ij}^{(2)})$ and $B = (b_{ij})$. We then have, for any $1 \leq i \leq n_1$, $T_2(\varphi(e_i)) = T_2(\sum_j b_{ij} f_j) = \sum_j (\sigma(b_{ij}) T_2(f_j) + \delta(b_{ij}) f_j) = \sum_k (\sum_j \sigma(b_{ij}) c_{jk}^{(2)} + \delta(b_{ik})) f_k$. Hence the matrix associated to $T_2\varphi$ in the bases β_1 and β_2 is $\sigma(B)C_2 + \delta(B)$. This yields the result.
$(iii) \Leftrightarrow (iv)$. It is enough to remark that the definition of T_{C_2} acting on $M_{n_1 \times n_2}(A)$ shows that, for any $B \in M_n(A)$, $(T_{C_2} - L_{C_1})(B) = \sigma(B)C_2 + \delta(B) - C_1 B$. □

Remark 2.9. The above proposition 2.8 shows that the equality (iii) is independent of the bases. Hence, if $P_1 \in M_{n_1}(A)$ and $P_2 \in M_{n_2}(A)$ are invertible matrices associated to change of bases in V_1 and V_2 then $C_1' B' = \sigma(B') C_2' + \delta(B')$ for $B' := P_1 B P_2^{-1}$, $C_1' := \sigma(P_1) C_1 P_1^{-1} + \delta(P_1) P_1^{-1}$ and $C_2' := \sigma(P_2) C_2 P_2^{-1} + \delta(P_2) P_2^{-1}$. Of course, this can also be checked directly.

Let $p(t) = \sum_{i=0}^{n} a_i t^i$ be a monic polynomial of degree n and consider the left $R = A[t; \sigma, \delta]$ module $V := R/Rp$. It is a free left A-module with basis $\beta := \{\overline{1}, \overline{t}, \ldots, \overline{t^{n-1}}\}$, where $\overline{t^i} = t^i + Rp$ for $i = 1, \ldots, n-1$. In the basis β, the matrix corresponding to left multiplication by t is the usual companion matrix of p denoted by $C(p)$ and defined by

$$C(p) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}$$

Corollary 2.10. *Let $p_1, p_2 \in R = A[t;\sigma,\delta]$ be two monic polynomials of degree $n \geq 1$ with companion matrices $C_1, C_2 \in M_n(A)$. $R/Rp_1 \cong R/Rp_2$ if and only if there exists an invertible matrix B such that $C_1B = \sigma(B)C_2 + \delta(B)$.*

The pseudo-linear transformation induced on A^n by $C(p)$ will be denoted T_p.

Recall that Rp is a two sided ideal in its ideal ring $Idl(Rp)) = \{g \in R \,|\, pg \in Rp\}$. The quotient ring $\frac{Idl(Rp}{Rp}$ is called the eigenring of Rp and is isomorphic to $End_R(R/Rp)$. The $(R, End_R(R/Rp))$-bimodule structure of R/Rp gives rise to a natural $(R, End_R(R/Rp))$-bimodule structure on A^n. For future reference we sum up some information in the form of a corollary.

Corollary 2.11. *Let $p(t) \in R$ be a monic polynomial of degree n and denote $C = C(p)$ its companion matrix. We have:*

(a) The eigenring $End_R(R/Rp)$ is isomorphic to $C_p^{\sigma,\delta} := \{B \in M_n(A) \,|\, CB = \sigma(B)C + \delta(B)\}$.

(b) A^n has an $(R, C_p^{\sigma,\delta})$-module structure.

(c) For $f(t) \in R$, $f(T_p)$ is a right $C_p^{\sigma,\delta}$-morphism. In particular, $\ker f(T_p)$ is a right $C_p^{\sigma,\delta}$-submodule of A^n.

We need to fix some notations. Thinking of the evaluation $f(a)$ of a polynomial $f(t) \in R = A[t;\sigma,\delta]$ at $a \in A$ as an element of A representing $f(t)$ in $R/R(t-a)$, we introduce the following notation: for a polynomial $f(t) \in R$ and a monic polynomial $p(t) \in R$ of degree n, $f(p)$ stands for the unique element in R of degree $< \deg(p) = n$ representing $f(t)$ in $R/Rp(t)$. Since divisions on the right by the monic polynomial p can be performed in R, $f(p)$ is the remainder of the right division of $f(t)$ by $p(t)$. We write $\overline{f(p)}$ for the image of $f(p)$ in R/Rp. For $v \in V = R/RP$, we denote $v_\beta \in A^n$ the row of coordinates of v in the basis $\beta := \{\overline{1}, \overline{t}, \ldots, \overline{t^{n-1}}\}$. Using the above notations we can state the following theorem.

Theorem 2.12. *Let $p(t) \in R = A[t;\sigma,\delta]$ be a monic polynomial of degree $n \geq 1$. Then:*

(1) For $f(t) \in R$ we have: $\overline{f(p)}_\beta = f(T_p)(1, 0, \ldots, 0)$.

(2) For $f(t), g(t) \in R$, we have: $\overline{(fg)(p)}_\beta = f(T_p)(\overline{g(p)}_\beta)$.

(3) For $f(t) \in R$ there exist bijections between the following sets $\ker f(T_p)$, $\{g \in R \,|\, deg(g) < n$ and $fg \in Rp\}$ and $Hom_R(R/Rf, R/Rp)$.

(4) $Idl(Rp) = \{g \in R \,|\, g(T_p)(1, 0, \ldots, 0) \in \ker p(T_p)\}$.

Proof. (1) Let us denote $t.$ the (σ,δ)-PLT on R/Rp defined by left multiplication by t. Since $f(t).=f(t.)$, we get $\overline{f(p)}_\beta=(f(t).\overline{1})_\beta=(f(t.)(\overline{1}))_\beta=f(T_p)(1,0,\dots,0)$.
(2) The point (1) above and corollary 2.5 give $\overline{(fg)(p)}_\beta=(fg)(T_p)(1,0,\dots,0)=f(T_p)(g(T_p)(1,0,\dots,0))=f(T_p)(\overline{g(p)}_\beta)$.
(3) The map $\psi:\ker f(T_p)\longrightarrow R$ defined by $\psi((v_0,\dots,v_{n-1}))=\sum_{i=0}^{n-1}v_it^i$ is injective and, using (2) above with $g(t):=\sum_{i=0}^{n-1}v_it^i$, we obtain $0=f(T_p)(v_0,\dots,v_{n-1})=f(T_p)(\overline{g(p)}_\beta)=\overline{fg(p)}_\beta$. this means that $fg\in Rp$. The map ψ is the required first bijection of statement (3).
Now, if $g\in R$ is such that $deg(g)<n$ and $fg\in Rp$ then the map $\varphi_g:R/Rf\longrightarrow R/Rp$ defined by $\varphi_g(h+Rf)=hg+Rp$ is an element of $Hom_R(R/f,R/Rp)$. The map $\gamma:\{g\in R\,|\,deg(g)<n,fg\in Rp\}\longrightarrow Hom_R(R/Rf,R/Rp)$ defined by $\gamma(g)=\varphi_g$ is easily seen to be bijective.
(4) Let us remark that $g\in R$ is such that $pg\in Rp$ iff $\overline{(pg)(p)}_\beta=0$ iff $p(T_p)(\overline{g(p)}_\beta)=0$. The first statement (1) above gives the required conclusion. □

The next corollary requires a small lemma which is interesting by itself. For a free left A-module V with basis $\beta=\{e_1,\dots,e_n\}$ and $\varphi\in End(V,+)$ we write $\varphi(e_i)=\sum_j\varphi_{ij}e_j$ and denote $\varphi_\beta\in M_n(A)$ the matrix defined by $\varphi_\beta=(\varphi_{ij})$.

Lemma 2.13. *Let T be a pseudo-linear transformation defined on a free left A-module V with basis $\beta=\{e_1,\dots,e_n\}$ and $f(t)\in R=A[t;\sigma,\delta]$. Considering $f(t)$ as an element of $M_n(A)[t;\sigma,\delta]$, we have $f(T)_\beta=f(T_\beta)$.*

Proof. (Cf. [L] Lemma 3.3). □

The following corollary is an easy generalization of the classical fact that the companion matrix, $C:=C(p)\in M_n(A)$, of a monic polynomial p of degree n annihilates the polynomial itself. As earlier, we extend σ and δ to $M_n(A)$ component-wise.

Corollary 2.14. *Let $p(t)\in R=A[t;\sigma,\delta]\subset M_n(A)[t;\sigma,\delta]$ be a monic polynomial of degree $n>1$. Then the following assertions are equivalent:*

(i) $t\in Idl(Rp)$;

(ii) for any $f\in R$, $f\in Rp$ *if and only if* $f(C(p))=0$;

(iii) $p(C(p))=0$.

Proof. $(i)\Rightarrow(ii)$ Since $t\in Idl(Rp)$, $f\in Rp$ implies $ft^i\in Rpt^i\subset Rp$, for any $0\leq i\leq n-1$. Theorem 2.12(4) then gives $((f(t)t^i)(T_p)(1,0,\dots,0)=(0,\dots,0)$. Hence, $f(T_p)(T_p^i(1,0,\dots,0))=(0,\dots,0)$, for $i\in\{0,\dots,n-1\}$. This leads to $f((T_p))_\beta=0$, where β is the standard basis of A^n. The above lemma 2 shows

that $0 = f((T_p))_\beta = f((T_p)_\beta) = f(C)$, where $f(C)$ stands for the evaluation of $f(t) \in M_n(A)[t;\sigma,\delta]$ at C.
$(ii) \Rightarrow (iii)$ This is clear.
$(iii) \Rightarrow (i)$ This is obtained by retracing the steps in $(i) \Rightarrow (ii)$ in the special case when $f(t) = p(t)$. □

Let us sum up all the information that we have gathered in the special case when $V = R/R(t-a)$. When, moreover, $A = K$ is a division ring, these results were proved in earlier papers (Cf. [LL$_1$], [LL$_2$], [LLO]) using different, more computational proofs. $U(A)$ stands for the set of invertible elements of A. For $x \in U(A)$, we denote a^x the element $\sigma(x)ax^{-1} + \delta(x)x^{-1}$ and $\Delta^{\sigma,\delta}(a) := \{a^x \,|\, x \in U(A)\}$.

Corollary 2.15. *Suppose $a \in A$ and $f, g \in R = A[t;\sigma,\delta]$. Let V stand for the R-module $R/R(t-a)$. Then:*

(a) The map $\Lambda_a : R \longrightarrow End(V,+)$ defined by $\Lambda_a(f) = f(T_a)$ is a ring homomorphism. For $f, g \in R$, we have $(fg)(a) = f(T_a)(g(a))$.

(b) Suppose $g(a)$ is invertible, then: $fg(a) = f(a^{g(a)})g(a)$. In particular, for an invertible element $x \in A$ we have: $f(T_a)(x) = f(a^x)x$.

(c) The set $C^{\sigma,\delta}(a) := \{b \in A \,|\, ab = \sigma(b)a + \delta(b)\}$ is a ring isomorphic to $End_R V$.

(d) If A is a division ring, then so is $C^{\sigma,\delta}(a)$. In this case, for any $f(t) \in R$ and any $a \in A$, $\ker(f(T_a)) = \{x \in A \setminus \{0\} \,|\, f(a^x) = 0\} \cup \{0\}$ is a right $C^{\sigma,\delta}(a)$-vector space.

Proof. (a) This is a special case of Corollary 2.5 and Theorem 2.12(2).
(b) It is easy to check that, for $x \in U(A)$, $(t - a^x)x = \sigma(x)(t-a)$. This leads to $f(t)x - f(a^x)x = (f(t) - f(a^x))x \in R(t-a^x)x \subseteq R(t-a)$. Hence, using (a) above with $g(t) = x$, we have $f(a^x)x = (f(t)x)(a) = f(T_a)(x)$. The other equality is now easy to check.
(c) This comes directly from Proposition 2.8.
(d) If A is a division ring, $R(t-a)$ is a maximal left ideal of R and Schur's lemma shows that $End_R(R/R(t-a))$ is a division ring. The other statements are clear from our earlier results. □

Remark 2.16. In a division ring K, a (σ,δ)-conjugacy class $\Delta^{\sigma,\delta}(a)$ can be seen as a projective space associated to K considered as a right $C^{\sigma,\delta}(a)$-vector space. With this point of view, for $f(t) \in R = K[t;\sigma,\delta]$ without roots in $\Delta^{\sigma,\delta}(a)$, the projective map associated to the right $C^{\sigma,\delta}(a)$-linear map $f(T_a)$ is the map ϕ_f defined by $\phi_f(a^x) = (a^x)^{f(a^x)} = a^{f(T_a(x))}$. This map ϕ_f is useful to detect pseudo-roots of a polynomial (i.e. elements $a \in K$ such that $t-a$ divides $gf \in R$ but

$f(a) \neq 0$). This point of view shed some lights on earlier results on ϕ-transform (Cf. [LL$_3$]).

Examples 2.17. 1. If $b - a \in A$ is invertible, it is easy to check that the polynomial $f(t) := (t - b^{b-a})(t - a) \in R = A[t; \sigma, \delta]$ is a monic polynomial right divisible by $t-a$ and $t-b$. $f(t)$ is thus the least left common multiple (abbreviated LLCM in the sequel) of $t - a$ and $t - b$ in $R = A[t; \sigma, \delta]$. Pursuing this theme further leads, in particular, to noncommutative symmetric functions (Cf. [DL]).

2. Similarly one easily checks that, if $f(a)$ is invertible then the LLCM of $f(t)$ and $t - a$ in $R = A[t; \sigma, \delta]$ is given by $(t - a^{f(a)})f(t)$.

3. It is now easy to construct polynomials that factor completely in linear terms but have only one (right) root. Let K be a division ring and $a \in K$ be an element algebraic of degree two over the center C of K. We denote $f_a(t) \in C[t]$ the minimal polynomial of a. $f_a(t)$ is also the minimal polynomial of the algebraic conjugacy class $\Delta(a) := \{xax^{-1} \,|\, x \in K \setminus \{0\}\}$. For $\gamma \in \Delta(a)$, we note $\overline{\gamma}$ the unique element of K such that $f_a(t) = (t - \overline{\gamma})(t - \gamma)$. Let us remark that if $\gamma \neq a$ then $\overline{\gamma} = a^{a-\gamma}$. Using an induction on m, the reader can easily prove that if a polynomial $g(t)$ is such that $g(t) := (t - a_m)(t - a_{m-1}) \dots (t - a_1)$ where $a_i \in \Delta(a)$ but $a_{i+1} \neq \overline{a_i}$, for $i = 1, \dots, m - 1$ then a_1 is the unique root of $g(t)$. For a concrete example consider $\mathbb{H}$, the division ring of quaternions over $\mathbb{Q}$. In this case, for $a \in \mathbb{H}$, $\overline{a}$ is the usual conjugate of a. Of course, one can generalize this example to a (σ, δ)-setting by considering an algebraic conjugacy class of rank 2.

4. Let us describe all the irreducible polynomials of $R := \mathbb{C}[t; -]$. First notice that the left (and right) Ore quotient ring $\mathbb{C}(t; -)$ of R is a division ring of dimension 4 over its center $\mathbb{R}(t^2)$. This implies that any $f(t) \in \mathbb{C}[t; -] \setminus \mathbb{R}[t^2]$ satisfies an equation of the form: $f(t)^2 + a_1(t^2)f(t) + a_0(t^2) = 0$ for some $a_1(t^2), a_0(t^2) \in \mathbb{R}(t^2)$ with $a_0(t^2) \neq 0$. This shows that for any polynomial $f(t) \in \mathbb{C}[t; -] \setminus \mathbb{R}[t]$ there exists $g(t) \in \mathbb{C}[t; -]$ such that $g(t)f(t) \in \mathbb{R}[t^2] \subset \mathbb{R}[t] \subset \mathbb{C}[t; -]$. In particular, the irreducible factors of $g(t)f(t)$ in $\mathbb{C}[t; -]$ are of degree ≤ 2. We can now conclude that the monic irreducible non linear polynomials of $\mathbb{C}[t; -]$ are the polynomials of the form $t^2 + at + b$ with no (right) roots. In other words the monic irreducible non linear polynomials of $\mathbb{C}[t; -]$ are of the form $t^2 + at + b$ such that for any $c \in \mathbb{C}$, $c\overline{c} + ac + b \neq 0$.

We now collect a few more observations.

Proposition 2.18. *Let $f, g \in R = A[t; \sigma, \delta]$ be polynomials such that g is not a zero divisor and $Rf + Rg = R$. Suppose that there exists $m \in R$ with $Rm = Rf \cap Rg$. Let $f', g' \in R$ be such that $m = f'g = g'f$. Let also T be any pseudo-linear transformation. We have:*

a) $R/Rf' \cong R/Rf$.

b) $g(T)(\ker f(T)) = \ker f'(T)$.

c) $\ker(m(T)) = \ker f(T) \oplus \ker g(T)$.

Proof. *a*) The morphism $\varphi : R/Rf' \longrightarrow R/Rf$ of left R-modules defined by $\varphi(1 + Rf') = g + Rf$ is in fact an isomorphism.
b) Since $f'g = g'f$, we have $(f'g)(T)(\ker f(T)) = 0$. Hence $g(T)(\ker f(T)) \subseteq \ker f'(T)$. Let φ be the map defined in the proof of *a*) above and let $h \in R$ be such that $\varphi^{-1}(1 + Rf) = h + Rf'$. Since φ^{-1} is well defined, we have $fh \in Rf'$ and $h(T)(\ker f'(T) \subseteq \ker f(T)$. We also have $gh - 1 \in Rf'$ and so $(gh)(T)|_{\ker f'(T)} = id.|_{\ker f'(T)}$. This gives $\ker f'(T) = gh(T)(\ker f'(T)) \subseteq g(T)(\ker f(T)) \subseteq \ker f'(T)$. This yields the desired conclusion.
c) Obviously $\ker g(T) + \ker f(T) \subseteq \ker(m(T))$. Now let $v \in \ker m(T)$. Then $f'g(T)(v) = 0 = g'f(T)(v)$. This gives $g(T)(v) \in \ker f'(T)$ and so, using the equality *b*) above, we have $g(T)(v) \in g(T)(\ker f(T))$. This shows that there exists $w \in \ker f(T)$ such that $g(T)(v) = g(T)(w)$. We conclude $v - w \in \ker g(T)$ and $v \in \ker g(T) + \ker f(T)$. The fact that the sum is direct is clear from the equality $R = Rf + Rg$. □

As an application of the preceding proposition, we have a relation between the roots of two similar polynomials with coefficients in a division ring. For $f \in K[t; \sigma, \delta]$, where K is a division ring, we denote $V(f)$ the set of right roots of f. For $x \notin V(f)$ we put $\phi_f(x) := x^{f(x)} := \sigma(f(x))xf(x)^{-1} + \delta(f(x))f(x)^{-1}$. With these notations we have the following corollary of the previous proposition:

Corollary 2.19. *Let $f, f' \in K[t; \sigma, \delta]$ be such that $\varphi : R/Rf' \longrightarrow R/Rf$ is an isomorphism defined by $\varphi(1 + Rf') = g + Rf$. Then $V(f') = \phi_g(V(f))$.*

Proof. Since $Rf + Rg = R$, $g(x) \neq 0$ for any $x \in V(f)$ and we have: $f'(\phi_g(x))g(x) = (f'g)(x) = (g'f)(x) = 0$. This shows that $\phi_g(V(f)) \subseteq V(f')$. For the reverse inclusion let us remark that $y \in V(f')$ implies that $1 \in \ker f'(T_y)$ the assertion *b*) in the above proposition 2.18 shows that there exists $z \in \ker f(T_y)$ such that $1 = g(T_y)(z) = g(y^z)z$. An easy computation then gives that $y = \phi_g(y^z)$. Since $f(T_y)(z) = 0$ implies $f(y^z) = 0$, we conclude that $V(f') \subseteq \phi_g(V(f))$, as required. □

3 Applications

Statement 1 of the following theorem is more general and statement 2 is more precise than the classical Gordon-Motzkin result (which is statement 1 of Theorem 3.1 with $(\sigma, \delta) = (id., 0)$). We will state it in the language of the maps T_a introduced in Section 2 (an even stronger statement was given in [LO]). For an element a in a division ring K, we recall that $C^{\sigma,\delta}(a) := \{0 \neq x \in K \mid a^x = a\} \cup \{0\}$ (Cf. Section 1) and $\Delta^{\sigma,\delta}(a) := \{x \in K \setminus \{0\} \mid \sigma(x)a + \delta(x) = ax\}$. $C^{\sigma,\delta}(a)$ is a subdivision ring of K and for any $f(t) \in R = K[t; \sigma, \delta]$, $f(T_a)$ is a right $C^{\sigma,\delta}(a)$-linear map (Cf. Corollary 2.15(d)). The set $\Delta(a) = \Delta^{\sigma,\delta}(a)$ is the (σ, δ)-conjugacy class determined by a.

Theorem 3.1. *Let $f(t) \in R = K[t; \sigma, \delta]$ be a polynomial of degree n. Then:*

1) $f(t)$ has roots in at most n (σ, δ)-conjugacy classes, say $\{\Delta(a_1), \ldots, \Delta(a_r)\}$, $r \leq n$;

2) $\sum_{i=1}^{r} dim_{C(a_i)} \ker(f(T_{a_i})) \leq n$, where $C(a_i) := C^{\sigma,\delta}(a_i)$ for $1 \leq i \leq r$.

Proof. We refer the reader to [LLO] and [LO]. □

Remark 3.2. In [LLO] it is shown that equality in formula 2) holds if and only if the polynomial $f(t)$ is Wedderburn.

We now offer an application of the previous Theorem 3.1.

In coding theory some authors have used Ore extensions to define noncommutative codes (Cf. [BGU], [BU]). In particular, noting $\mathbb{F}_q$ the finite field of characteristic p with $q = p^n$ elements, they considered the Ore extension of the form $R := \mathbb{F}_q[t; \theta]$, where θ is the usual Frobenius automorphism given by $\theta(x) = x^p$. The following theorem shows that the analogue of the usual minimal polynomial $X^q - X \in \mathbb{F}_q[X]$ annihilating $\mathbb{F}_q$ is of much lower degree in this noncommutative setting.

Theorem 3.3. *Let p be a prime number and $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Denote by θ the Frobenius automorphism. Then*

a) There are p distinct θ-conjugacy classes in $\mathbb{F}_q$.

b) For $0 \neq a \in \mathbb{F}_q$ we have $C^\theta(a) = \mathbb{F}_p$ and $C^\theta(0) = \mathbb{F}_q$.

c) In $R = \mathbb{F}_q[t; \theta]$, the least left common multiple of all the elements of the form $t - a$ for $a \in \mathbb{F}_q$ is the polynomial $G(t) := t^{(p-1)n+1} - t$. In other words, $G(t) \in \mathbb{F}_q[t; \theta]$ is of minimal degree such that $G(a) = 0$ for all $a \in \mathbb{F}_q$.

d) The polynomial $G(t)$ obtained in c). above is invariant, i.e. $RG(t) = G(t)R$.

Proof. a) Let us denote by g a generator of the cyclic group $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. The conjugacy class determined by the zero element is reduced to $\{0\}$ i.e. $\Delta(0) = \{0\}$. The conjugacy class determined by 1 is a subgroup of $\mathbb{F}_q^*$: $\Delta(1) = \{\theta(x)x^{-1} \,|\, 0 \neq x \in \mathbb{F}_q\} = \{x^{p-1} \,|\, 0 \neq x \in \mathbb{F}_q\}$. It is easy to check that $\Delta(1)$ is cyclic generated by g^{p-1} and has order given by $\frac{p^n-1}{p-1}$. Its index $(\mathbb{F}_q^* : \Delta(1)) = p-1$. Since two nonzero elements a, b are θ-conjugate if and only if $ab^{-1} \in \Delta(1)$, we indeed get that the number of different nonzero conjugacy classes is $p-1$. This yields the result.
b) If $a \in \mathbb{F}_q$ is nonzero, then $C^\theta(a) = \{x \in \mathbb{F}_q \,|\, \theta(x)a = ax\}$ i.e. $C^\theta(a) = \mathbb{F}_p$.
c) We have, for any $x \in \mathbb{F}_q$, $(t^{(p-1)n+1} - t)(x) = \theta^{(p-1)n}(x) \dots \theta(x)x - x$. Since $\theta^n = id.$, we get $(t^{(p-1)n+1} - t)(x) = x(\theta^{n-1}(x) \dots \theta(x)x)^{p-1} - x = xN_n(x)^{p-1} - x = 0$, since $N_n(x) \in \mathbb{F}_p$. This shows that indeed $G(t)$ annihilates all the elements of $\mathbb{F}_q$ and hence $G(t)$ is a left common multiple of the linear polynomials $\{(t-a) \,|\, a \in \mathbb{F}_q\}$. Let us put $h(t) := [t - a \,|\, a \in \mathbb{F}_q]_l$. It remains to show that $\deg h(t) \geq n(p-1)+1$. Let $0 = a_0, a_1, \dots, a_{p-1}$ be elements representing the θ-conjugacy classes (Cf. a) above). Denote $C_0, C_1, \dots, C_{p-1}$ their respective θ-centralizer. Theorem 2.12 7) shows that $h(T_a)(x) = h(a^x)x = 0$ for any nonzero element $x \in K$. Hence $\ker h(T_a) = \mathbb{F}_q$. Using the inequality 2) in Theorem 3.1 and the statement $b)$ above, we get $\deg h(t) \geq \sum_{i=0}^{p-1} dim_{C_i} \ker h(T_{a_i}) = dim_{\mathbb{F}_q}\mathbb{F}_q + \sum_{i=1}^{p-1} dim_{\mathbb{F}_p}\mathbb{F}_q = 1 + (p-1)n$, as required.
d) Since $\theta^n = id.$, we have immediately that $G(t)x = \theta(x)G(t)$ and obviously $G(t)t = tG(t)$. □

Remark 3.4. The polynomial $G(t) = t^{n(p-1)+1} - t \in \mathbb{F}_{p^n}[t;\theta]$ defined in the previous theorem 3.3 can have roots in an extension $\mathbb{F}_{p^l} \supsetneq \mathbb{F}_{p^n}$. This is indeed always the case if $l = n(p-1)$. Let us denote $\Delta_l(1) := \{1^x \,|\, 0 \neq x \in \mathbb{F}_{p^l}\}$ and $\Delta_n(1) := \{1^x \,|\, 0 \neq x \in \mathbb{F}_{p^n}\}$. Since $\theta^l = id.$ on $\mathbb{F}_{p^l}$, we have $G(t)a = \theta(a)G(t)$ for any $a \in \mathbb{F}_{p^l}$. This gives, for any $0 \neq x \in \mathbb{F}_{p^l}$, $G(1^x)x = (G(t)x)(1) = (\theta(x)G(t))(1) = \theta(x)G(1) = 0$. In other words, $G(t)$ annihilates the θ-conjugacy class $\Delta_l(1) \subseteq \mathbb{F}_{p^l}$. It is easy to check that $|\Delta_l(1)| = \frac{p^l-1}{p-1} > \frac{p^n-1}{p-1} = |\Delta_n(1)|$. We conclude that $G(t)$ has roots in $\mathbb{F}_{p^l} \setminus \mathbb{F}_{p^n}$. This contrasts with the classical case where $:[x - a \,|\, a \in \mathbb{F}_{p^n}]_l = x^{p^n} - x \in \mathbb{F}_{p^n}[x]$ has all its roots in $\mathbb{F}_{p^n}$.

We continue our investigations of finite fields and the Frobenius automorphism and come back to the comments made in the paragraph just after the last example in 2.2. For a prime p and an integer $i \geq 1$, we define $[i] := \frac{p^i-1}{p-1} = p^{i-1} + p^{i-2} + \dots + 1$ and put $[0] = 0$. We fix an integer $n \geq 1$ and continue to denote $q = p^n$. Let us introduce the following subset of $\mathbb{F}_q[x]$:

$$\mathbb{F}_q[x^{[]}] := \{\sum_{i \geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x]\}$$

A polynomial belonging to this set will be called a $[p]$-polynomial. We extend θ to the ring $F_q[x]$ and put $\theta(x) = x^p$ i.e. $\theta(g) = g^p$ for all $g \in F_q[x]$. We

thus have $R := F_q[t;\theta] \subset S := F_q[x][t;\theta]$. Considering $f \in R := \mathbb{F}_q[t;\theta]$ as an element of $\mathbb{F}_q[x][t;\theta]$ we can evaluate f at x. We denote the resulting polynomial by $f^{[]} \in \mathbb{F}_q[x]$ i.e. $f(t)(x) = f^{[]}(x)$.

The last statement of the following theorem will show that the question of the irreducibility of a polynomial $f(t) \in R := \mathbb{F}_q[t;\theta]$ can be translated in terms of irreducibility in $\mathbb{F}_q[x^{[]}]$. This makes Berlekamp algorithm available to test irreducibility of polynomials in $R = \mathbb{F}_q[t;\theta]$. This will also provide an algorithm for factoring polynomials in $\mathbb{F}_q[t;\theta]$, as explained in the paragraph following the proof of the next theorem.

Theorem 3.5. *Let $f(t) = \sum_{i=0}^{n} a_i t^i$ be a polynomial in $R := \mathbb{F}_q[t;\theta] \subset S := \mathbb{F}_q[x][t;\theta]$. With the above notations we have:*

1) For any $b \in \mathbb{F}_q$, $f(b) = \sum_{i=0}^{n} a_i b^{[i]}$.

2) $f^{[]}(x) = \sum_{i=0}^{n} a_i x^{[i]} \in \mathbb{F}_q[x^{[]}]$.

3) $\{f^{[]} | f \in R = \mathbb{F}_q[t;\theta]\} = \mathbb{F}_q[x^{[]}]$.

4) For $i \geq 0$ and $h(x) \in \mathbb{F}_q[x]$ we have $T_x^i(h) = h^{p^i} x^{[i]}$.

5) For $g(t) \in S = F_q[x][t;\theta]$ and $h(x) \in \mathbb{F}_q[x]$ we have $g(T_x)(h(x)) \in \mathbb{F}_q[x]h(x)$.

6) For any $h(t) \in R = \mathbb{F}_q[t;\theta]$, $f(t) \in Rh(t)$ if and only if $f^{[]}(x) \in \mathbb{F}_q[x]h^{[]}(x)$.

Proof. 1) This has been noted earlier (Cf. the last example in 2.2).
2) We compute: $f(t)(x) = (\sum_{i=0}^{n} a_i t^i)(x) = \sum_{i=0}^{n} a_i N_i(x)$. Since, for $i > 0$, $N_i(x) = \theta^{i-1}(x) \cdots \theta(x)x = x^{[i]}$ and $N_0(x) = 1 = x^{[0]}$, we do get the desired result.
3) This is clear from the statement 2) above.
4) This is easily proved by induction (notice that $T_x^0(h) = h = h^{p^0} x^{[0]}$).
5) Let us put $g(t) = \sum_{i=0}^{n} g_i(x) t^i$. Statement 4) above then gives: $g(T_x)(h(x)) = (\sum_{i=0}^{n} g_i(x) T_x^i)(h(x)) = \sum_{i=0}^{n} g_i(x) h^{p^i} x^{[i]} \in \mathbb{F}_q[x]h$.
6) Let us write $f(t) = g(t)h(t)$ in R. The generalized product formula and the statement 5) above gives $f^{[]}(x) = f(t)(x) = (g(t)h(t))(x) = g(T_x)(h(t)(x)) = g(T_x)(h^{[]}(x)) \in \mathbb{F}_q[x]h^{[]}(x)$.
Conversely, suppose there exists $g(x) \in \mathbb{F}_q[x]$ such that $f^{[]}(x) = g(x)h^{[]}(x)$. Let $f(t), h(t) \in \mathbb{F}_q[t;\theta]$ be such that $f(t)(x) = f^{[]}(x)$ and $h(t)(x) = h^{[]}(x)$. Using the euclidean division algorithm in $\mathbb{F}_q[t;\theta]$ we can write $f(t) = q(t)h(t) + r(t)$ with $\deg r(t) < \deg h(t)$. Evaluating both sides of this equation at x we get, thanks to the generalized product formula, $f^{[]}(x) = f(t)(x) = q(T_x)(h(t)(x)) + r(t)(x) = q(T_x)(h^{[]}(x)) + r^{[]}(x)$ and $\deg r^{[]}(x) = [\deg r(t)] < [\deg h(t)] = \deg h^{[]}(x)$. Statement 5) above and the hypothesis then give that $r^{[]}(x) = 0$. Let us write $r(t) = \sum_{i=0}^{l} r_i t^i \in \mathbb{F}_q[t;\theta]$. With these notations we must have $\sum_{i=0}^{l} r_i x^{[i]} = 0$. This yields that for all $i \geq 0$, $r_i = 0$ and hence $r(t) = 0$, as required. □

Let us mention the following obvious but important corollary:

Corollary 3.6. *A polynomial $f(t) \in \mathbb{F}_q[t;\theta]$ is irreducible if and only if its attached $[p]$-polynomial $f^{[]}$ has no non trivial factor in $\mathbb{F}_q[x^{[]}]$.*

Of course, the condition stated in the above corollary 3.6 can be checked using, for instance, the Berlekamp algorithm for factoring polynomials over finite fields. In fact this leads easily to an algorithm for factoring $f(t) \in \mathbb{F}_q[t;\theta]$. Indeed given $f(t) \in \mathbb{F}_q[t;\theta]$ we first find a polynomial $h^{[]} \in \mathbb{F}_q[x^{[]}]$ such that $h^{[]}$ divides $f^{[]}$ (if possible) and we write $f^{[]} = g(x)h^{[]}$ for some $g(x)$ in $\mathbb{F}_q[x]$. This gives $f(t) = g'(t)h(t) \in \mathbb{F}_q[t;\theta]$. We then apply the same procedure to $g'(t)$ and find a right factor of $g'(t)$ in $\mathbb{F}_q[t;\theta]$ by first finding (if possible) a $[p]$-factor of $g'^{[]}$... The above correspondence between polynomials in $\mathbb{F}_q[t;\theta]$ and $[p]$-polynomials will be further studied and generalized in a forthcoming paper. For the moment let us give some concrete examples.

Examples 3.7. In the next three examples we will consider the field of four elements $\mathbb{F}_4 = \{0, 1, a, 1+a\}$ where $a^2+a+1 = 0$. $\theta(a) = a^2 = a+1$; $\theta(a+1) = (a+1)^2 = a$.

a) Consider the polynomial $t^3 + a \in \mathbb{F}_4[t;\theta]$. Its associated [2]-polynomial is given by $x^7 + a \in \mathbb{F}_4[x]$. Since a is a root of $x^7 + a$ it is also a root of $t^3 + a$. This gives $t^3 + a = (t^2 + at + 1)(t + a)$ in $\mathbb{F}_4[t;\theta]$. Now, the [2]-polynomial associated to the left factor $t^2 + at + 1$ is $x^3 + ax + 1 \in \mathbb{F}_4[x]$. Since this last polynomial is actually irreducible we conclude that $t^2 + at + 1$ is also irreducible in $\mathbb{F}_4[t;\theta]$. Hence the factorization of $t^3 + a$ given above is in fact a decomposition into irreducible factorizations.

b) Let us now consider $f(t) = t^4 + (a+1)t^3 + a^2t^2 + (1+a)t + 1 \in \mathbb{F}_4[t;\theta]$. Its attached $[p]$-polynomial is $x^{15} + (a+1)x^7 + (a+1)x^3 + (1+a)x + 1 \in \mathbb{F}_4[x]$. We can factor it as follows:

$$(x^{12}+ax^{10}+x^9+(a+1)x^8+(a+1)x^5+(a+1)x^4+x^3+ax^2+x+1)(x^3+ax+1)$$

This last factor is a $[p]$-polynomial which corresponds to $t^2+at+1 \in \mathbb{F}_4[t;\theta]$. Moreover since $x^3 + ax + 1$ is actually irreducible in $\mathbb{F}_4[x]$, we have that $t^2 + at + 1$ is also irreducible in $\mathbb{F}_4[t;\theta]$. We then easily conclude that $f(t) = (t^2 + t + 1)(t^2 + at + 1)$ is a decomposition of $f(t)$ into irreducible factors in $\mathbb{F}_4[t;\theta]$.

c) Let us consider the polynomial $f(t) = t^5 + at^4 + (1 + a)t^3 + at^2 + t + 1$. Its attached $[p]$-polynomial is $x^{31} + ax^{15} + (1 + a)x^7 + ax^3 + x + 1$. It is easy to remark that a is a root and we get $f(t) = q_1(t)(t + a)$ in $\mathbb{F}_4[t;\theta]$ where $q_1(t) = t^4 + (a + 1)(t^2 + t + 1)$. The $[p]$-polynomial attached to $q_1(t)$ is $x^{15} + (a + 1)(x^3 + x + 1)$. Again we get that a is a root and we obtain

that $q_1(t) = (q_2(t))(t+a)$ in $\mathbb{F}_4[t;\theta]$ where $q_2(t) = t^3 + (a+1)t^2 + at + a$. The $[p]$-polynomial attached to $q_2(t)$ is $x^7 + (a+1)x^3 + ax + a$. Once again a is a root and we have $q_2(t) = (t^2+t+1)(t+a)$. Since t^2+t+1 is easily seen to be irreducible in $\mathbb{F}_4[t;\theta]$, we have the following factorization of our original polynomial: $f(t) = (t^2+t+1)(t+a)^3$. We can also factorize $f(t)$ as follows: $f(t) = (t+a+1)(t+1)(t+a)(t^2+(a+1)t+1)$.

Remark 3.8. It is a natural question to try to find a good notion of a splitting field attached to a polynomial of an Ore extension. The above results justify that, in the case of a skew polynomial ring $\mathbb{F}_q[t;\theta]$ where $q = p^n$ and θ is the Frobenius automorphism, we define the splitting field of a polynomial $f(t) \in \mathbb{F}_q[t;\theta]$ to be the splitting of the polynomial $f^{\natural}(x)$ over $\mathbb{F}_q$.

Our next application of Theorem 3.1, is an easy proof of Hilbert 90 theorem. (Cf. [LL$_3$]) for more advanced results using also structure theory of an Ore extension $K[t;\sigma,\delta]$.

Proposition 3.9. *a) Let K be a division ring, σ an automorphism of K of finite order n and such that no power of σ of order strictly smaller than n is inner. Then $\Delta^\sigma(1)$ is algebraic and $t^n - 1 \in K[t;\sigma]$ is its minimal polynomial (i.e. $V(t^n-1) = \Delta(1)$).*

b) Let K be a division ring of characteristic p and δ a nilpotent derivation of K of order p^n satisfying no identity of smaller degree than p^n. Then $\Delta^\delta(0)$ is algebraic and t^{p^n} is its minimal polynomial ($V(t^{p^n}) = \Delta^\delta(0)$).

Proof. a) Since $T_1^n = \sigma^n = id.$, we have $\ker(T_1^n - id.) = K$. It is easy to check that $(t^n-1)(\sigma(x)x^{-1}) = 0$ for any $x \in K \setminus \{0\}$. We thus have $\Delta^\sigma(1) \subseteq V(t^n-1)$. Standard Galois theory of division rings implies that $[K : Fix(\sigma)]_r = n$. Moreover $C^\sigma(1) = Fix(\sigma)$, part two of Theorem 3.1 than quickly yields the result.
b) This is similar to the above proof noting that $K = \ker(\delta^{p^n}) = \ker(T_0^{p^n})$, $C^\delta(0) = \ker(\delta)$ and $[K : \ker(\delta)]_r = p^n$. □

Remark 3.10. We do get back the standard Hilbert 90 theorem remarking in particular that $\Delta^\sigma(1) = \{\sigma(x)x^{-1} \mid x \in K \setminus \{0\}\}$.

As another application, let us now give a quick proof of a generalized version of the Frobenius formula in characteristic $p > 0$. The proof of this formula is usually given for a field through long computations involving additive commutators (Cf. Jacobson [Ja$_2$], p. 190). Using the polynomial maps we give a quick proof.

Proposition 3.11. *Let K be a ring of characteristic $p > 0$, δ be a (usual) derivation of K and a any element in K. In $R = K[t; id., \delta]$ we have*

$$(t-a)^p = t^p - N_p(a).$$

Proof. Define d a derivation on R by $d|_K = 0$ and $d(t) = 1$. It is easy to check that this gives rise to a well defined derivation of R. Notice that $d(t-a) = 1$ commutes with $t-a$ hence $d((t-a)^p) = 0$. Let us write $(t-a)^p = \sum_{i=0}^{p} c_i t^i$. Applying d on both sides we quickly get that $c_i = 0$ for all $i = 1, \ldots, p-1$. We thus have $(t-a)^p = t^p - c_0$. Since a is a right root we have indeed that $c_0 = N_p(a)$. □

Let us now analyze the maps arising in a division process. The so called N_i maps of section 1 have been largely studied in previous works (e.g. [LL$_1$],[LL$_2$]). Here we will look at the quotient and get some formulas generalizing elementary ones. It doesn't seem that these maps have been introduced earlier in this setting.

Proposition 3.12. *Let A, σ, δ be a ring, an endomorphism and a σ-derivation of A. For $a \in A$ and $i \geq 0$, let us write $t^i = q_{i,a}(t)(t-a) + N_i(a)$ in $R = A[t; \sigma, \delta]$. We have:*

1) If $f(t) = \sum_{i=0}^{n} a_i t^i \in R$, then $f(t) = \sum_{i=0}^{n} a_i q_{i,a}(t)(t-a) + \sum_{i=0}^{n} a_i N_i(a)$.

2) $q_{0,a} = 0, q_{1,a} = 1$ and, for $i \geq 1$, $q_{i+1,a}(t) = t q_{i,a}(t) + \sigma(N_i(a))$.

3) $N_i(b) - N_i(a) = q_{i,a}(T_b)(b-a) = q_{i,b}(T_a)(b-a)$.

Proof. The elementary proofs are left to the reader. □

Remark 3.13. Even the case when $\sigma = id.$ and $\delta = 0$ is somewhat interesting. In this latter case the polynomials $q_{i,a}$ can be expressed easily: $q_{i,a}(t) = t^{i-1} + at^{i-1} + \cdots + a^{i-1}$. Of course, in this case we get some familiar formulas. For instance the last equation in 3.12 above gives the classical equality in a noncommutative ring A: $b^i - a^i = (b-a)b^{i-1} + a(b-a)b^{i-2} + \cdots + a^{i-1}(b-a)$.

We now present the last application which is slightly related to the case when the base ring is left duo.

Definition 3.14. We will say that two monic polynomials $f, g \in R = A[t; \sigma, \delta]$ have a monic left common multiple if there exists monic polynomials $f', g' \in R$ such that $f'g = g'f$.

We will use the notations from Theorem 2.12.

Proposition 3.15. *Two monic polynomial f, g have a monic left common multiple if and only if there exists a monic polynomial $g' \in R$ such that $(1, 0, \ldots, 0) \in \ker g' f(T_g)$. In particular, if $g = t - a$ then there exists a monic left common multiple of f, g if and only if there exists $c \in A$ such that $T_a(f(a)) = cf(a)$.*

The easy proof is left to the reader. We now look at the same problem from a slightly different perspective (a "down-up" approach, comparing to the "top down" mentioned above)

Proposition 3.16. *Let A, σ, δ be respectively, a ring, an endomorphism of A and a σ-derivation of A. The following are equivalent:*

(i) For $a, b \in A$, there exist $c, d \in A$ such that $(t-c)(t-a) = (t-d)(t-b)$ in $R = A[t; \sigma, \delta]$.

(ii) For any $a, b \in A$, there exists $c \in A$ such that $T_b(a) = ca = L_c(a)$

(iii) For any $a, b \in A$, there exists $c \in A$ such that $\sigma(a)b + \delta(a) = ca$.

In particular, when $\sigma = id.$ and $\delta = 0$, the above conditions are also equivalent to the ring A being left duo.

Proof. $(i) \Rightarrow (ii)$. Clearly (i) implies that b is a (right) root of $(t-c)(t-a)$. Hence for every $a, b \in A$ there exists $c \in A$ such that $(T_b - c)(b-a) = 0$. Since a, b are any elements of A this implies (ii)).
$(ii) \Rightarrow (iii)$. This is easily obtained using the definition of T_b.
$(iii) \Rightarrow (i)$. Let $a, b \in A$. Writing the condition (iii) for the elements $b-a$ and b we find an element $c \in A$ such that $\sigma(b-a)b + \delta(b-a) = c(b-a)$. We then check that $((t-c)(t-a))(b) = 0$. This shows that $(t-c)(t-a)$ is right divisible by $t-b$ and this proves statement (i).
The additional statement is clear from (iii) indeed in this case (iii) means that for any $a, b \in A$, $ab \in Aa$. Or in other words, that any left principal ideal Aa is in fact two sided. □

The last statement of the previous proposition 3.16 justifies the following definition:

Definition 3.17. A ring A is left (σ, δ)-duo if for any $a, b \in A$, there exists $c \in A$ such that $T_b(a) = ca$.

Proposition 3.16 was already given in the last section of [DL]. Here we stress the use of T_a. In fact the pseudo-linear map T_a enables us to show that in an Ore extension built on a left (σ, δ)-duo ring, the least left common multiple exists for any two monic polynomials as long as one of them can be factorized linearly. We state this more precisely in the following theorem. This theorem was also proved by M. Christofeul with a different, more computational, proof [C].

Theorem 3.18. *Let $a_1, \ldots, a_n$ be elements in a left (σ, δ)-duo ring A. Then for any monic polynomial $g(t) \in R = A[t; \sigma, \delta]$ there exists a monic least left common multiple of $g(t)$ and of $(t-a_n)\cdots(t-a_1)$ of degree $\leq n + \deg(g)$.*

Proof. We proceed by induction on n. If $n = 1$ the fact that A is (σ, δ)-left duo implies that there exists $c \in A$ such that $T_{a_1}(g(a_1)) = cg(a_1)$ and this shows that the polynomial $(t-c)g(t)$ is divisible on the right by $t - a_1$, as desired.

Assume $n > 1$. By the above paragraph, there exist a monic polynomial $g_1(t) \in R$ and an element $c \in A$ such that $g_1(t)(t-a_1) = (t-c)g(t)$. On the other hand, the induction hypothesis shows that there exist monic polynomials $h(t), p(t) \in R$ such that $h(t)(t-a_n)\cdots(t-a_2) = p(t)g_1(t)$ where $\deg(h)+n-1 \leq \deg(g_1)+n-1 = \deg(g)+n-1$. This implies that $h(t)(t-a_n)\cdots(t-a_2)(t-a_1) = p(t)g_1(t)(t-a_1) = p(t)(t-c)g(t)$. This shows that $g(t)$ and $(t-a_1)(t-a_2)\cdots(t-a_n)$ have a monic common multiple of degree $\leq \deg(g)+n$. □

References

[BGU] D. Boucher, W. Geiselmann and F. Ulmer: *Skew Cyclic Codes*, Applied Algebra in Engineering, Communication and Computing, **18** (2007), 379-389.

[BU] D. Boucher and F. Ulmer: *Coding with skew polynomial rings*, Journal of Symbolic Computation, **44** (2009), 1644-1656.

[Ca] G. Cauchon, Les T-anneaux et les anneaux à identités polynômiales noethériens, Thèse Orsay : Université Paris XI, (1977).

[C] M. Christofeul: Ph. D. Thesis, in preparation, Université d'Artois.

[Co] P. M. Cohn: *Skew Fields. Theory of General Division Rings*, Encyclopedia in Math., Vol. 57, Cambridge Univ. Press, Cambridge, 1995.

[DL] J. Delenclos and A. Leroy: *Symmetric functions and W-polynomials*, Journal of Algebra and its Applications, **6** (2007), 815-837.

[F] P. R. Fuchs, C. J. Maxson and G. F. Pilz, Rings with FZP, Transactions of the American Mathematical Society **349** (1997), 1269-1283.

[GR] I. Gelfand,R.L. Wilson Noncommutative Vieta Theroem and symmetric functions, The Gelfand Mathematical Seminars 1993-1995, Birkhauser, Boston, **1995** , 93-100

[GRW] I. Gelfand,V. Retakh,R.L. Wilson:*Quadratic linear algebras associated with factorizations of noncommutative polynomials and noncommutative differential polynomials*, Selecta Math., **7**,

[HR] D. E. Haile and L. H. Rowen: *Factorization of polynomials over division algebras*, Algebra Colloq. **2** (1995), 145-156.

[Ja_1] N. Jacobson: *Lectures in abstract algebra*, Vol. 3, Van Nostrand, 1964.

[Ja_2] N. Jacobson: *Pseudo linear transformations*, Annals of Math. **38** (1937), 484-507.

[La] T. Y. Lam: *A First Course in Noncommutative Rings*, Graduate Texts in Math., Vol. **131**, Springer-Verlag, Berlin-Heidelberg-New York, 1991.

[LL_1] T. Y. Lam and A. Leroy: *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), 308-336.

[LL_2] T. Y. Lam and A. Leroy: *Algebraic conjugacy classes and skew polynomial rings*, in: "Perspectives in Ring Theory", (F. van Oystaeyen and L. Le Bruyn, eds.), Proceedings of the Antwerp Conference in Ring Theory, pp. 153-203, Kluwer Academic Publishers, Dordrecht/Boston/London, 1988.

[LL_3] T. Y. Lam and A. Leroy: *Hilbert 90 Theorems for division rings*, Trans. A.M.S. **345** (1994), 595-622.

[LL_4] T. Y. Lam and A. Leroy: *Wedderburn polynomials over division rings,* I, Journal of Pure and Applied Algebra, **186** (2004), 43-76.

[LLLM] Lam, Leroy, Leung, Matczuk, Invariant and semi-invariant polynomials in skew polynomial rings, in "ring theory 1989" (in honour of S.A. Amitsur), ed. L. Rowen, Israel Mathematical conference proceedings, Kluwer Academic Publishers, pp. 153-203.

[LLO] T. Y. Lam, A. Leroy and A. Ozturk: *Wedderburn polynomials over division rings,* II, Proceedings of a conference held in Chennai at the Ramanujan Institute (India) Contemporary mathematics (456) 2008, pp. 73-98.

[LM] A. Leroy, J. Maczuk, The Extended Centroid and X-Inner Automorphisms of Ore Extensions, Journal Of Algebra (1992), 145, 143-177.

[L] A. Leroy: *Pseudo-linear transformations and evaluation in Ore extensions*, Bull. Belg. Math. Soc. **2** (1995), 321-347.

[LO] A. Leroy, A.Ozturk: *Algebraic and F-independent sets in* 2*-firs*,Com. in Algebra, Vol. **32** (5) (2004), 1763-1792.

[MB] B. Marinescu, H. Bourlès: *An intrinsic algebraic setting for poles and zeros of linear time-varying systems*, System & control letters, **58** (2009), 248-253.

[Or] O. Ore: *Theory of noncommutative polynomials*, Annals of Math., **34** (1933), 480-508.

[S] M. Slusky, Zeros of 2 2 Matrix Polynomials, preprint